ПЕРЕДМОВА

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

У публікації «Эндрю Ворланд: Проблема идентификации изначально-электронных документов» розглядаються проблеми ідентифікації (виявлення) спочатку-електронних документів з метою управління ними.

У публікації «Стратегическое управление информацией - дело скучное, но необходимое» розповідається, що таке стратегічне управління інформацією. Наведені приклади.

У публікації «Итак, какую же пользу приносит нам управление документами?» розповідається про переваги, які дає вашому підрозділу впровадження програми управління документами.

У публікації «Удалённая работа: Две трети опрошенных считает, что пути назад нет» розповідається, що віддалена робота стала новою нормою. Вісімдесят відсотків компаній впровадили або розширили можливості для своїх співробітників працювати віддалено.

У публікації «ИСО/МЭК: Опубликован новый стандарт ISO/IEC 23264-1 «Цензурирование аутентичных данных»» розповідається, що цей документ визначає властивості криптографічних механізмів, процеси, задіяні в цих механізмах, які сторони беруть участь і криптографічні властивості.

У публікації «Китай: Ускорение применения технологий искусственного интеллекта в управлении документами и архивном деле» розповідається, що Китай приділяє значну увагу розвитку технології штучного інтелекту, і країна сформулювала пов'язані зі штучним інтелектом політики на національному, галузевому та місцевому рівнях.

У публікації «ИСО: Стандарт по стратегическому управлению информацией вышел на стадию публичного обсуждения» наводиться проєкт даного міжнародного стандарту який пропонує членам органів стратегічного управління організаціями (в числі власникам, директорам, партнерам, керівникам робіт і та інш.) основні принципи для ефективного, продуктивного, відповідного законодавчо-нормативним та іншим вимогам, безпечного, прозорого і підзвітного створення, використання, зберігання, забезпечення довготривалого збереження і знищення / передачі на архівне зберігання інформації в їхніх організаціях.

У публікації «Евросоюз: Европейская комиссия собирается обеспечить для всех европейцев надежные и безопасные цифровые идентификационные профили (Digital Identity)» розповідається, що Європейські цифрові ідентифікаційні профілі дозволять нам в будь-якій державі-члені Євросоюзу діяти так само, як вдома, без будь-яких додаткових витрат і при меншій кількості перешкод.

У публікації «Прошло первое заседание нового технического комитета ТС 468 «Управление и обеспечение долговременной сохранности цифрового контента» Европейского комитета по стандартизации CEN» розповідається про перше засідання новоствореного технічного комітету, проведеному 28 травня 2021 року CEN / TC 468 «Управління та забезпечення довготривалого збереження цифрового контенту».

У публікації «Над чем сейчас работает целевая рабочая группа AHG2 «Уничтожение/передача документов» технического подкомитета ИСО TC46/SC11» розповідається про напрацювання групи AHG2 TC46 / SC11 / Міжнародної організації зі стандартизації, яка займається питаннями остаточного вирішення долі документів (знищення або передачі на архівне зберігання).

У публікації «Штат Виктория, Австралия: Проект проведения экспертизы ценности, уничтожения/передачи на архивное хранение и обеспечения долговременной сохранности электронной почты» розповідається про досвід Управління державними документами австралійського штату Вікторія з розробки нормативно-методичної бази в сфері управління документами для державних органів штату.

У публікації «Росстандарт: Как стандартизация перерастает в профанацию» розповідається про низку стандартів, викладених на сайті Росстандарта в травневому 2021 року розділі за надуманими питаннями.

У публікації «Искусственный интеллект: Беспокойство о последствиях «второго порядка»» розповідається про дослідження фірми Gartner, яка передбачає потенційно небажані «вторинні» наслідки впровадження технологій штучного інтелекту.

ЭНДРЮ ВОРЛАНД: ПРОБЛЕМА ИДЕНТИФИКАЦИИ ИЗНАЧАЛЬНО-ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

Источник: блог Эндрю Ворланда
https://andrewwarland.wordpress.com/2021/03/28/the-challenge-of-identifying-born-digital-records/

В опубликованном 30 января 2021 года отчёте по итогам проверки выполняемых функций и эффективности деятельности Национальных Архивов Австралии (см. https://www.ag.gov.au/rights-and-protections/publications/tune-review , также известном, как «Отчёт комиссии Тьюна» - Tune Review) отмечаются «стремительно возникающие и постоянно эволюционирующие проблемы электронно-цифрового мира».

В отчёте говорится, что «*определение понятия «документ» (record) должно соответствовать текущим международным стандартам, быть более непосредственно применимым в отношении цифровых технологий и более недвусмысленно предусматривать и поддерживать прямой захват тех документов, для которых велик риск уничтожения, таких, как электронные письма, текстовые или онлайн-сообщения*».

В данном документе также привлекается внимание к трудностям, связанным со вводом электронных документов в соответствующие архивные системы «с использованием интенсивных ручных операций (из-за отсутствия интеоперабельности между системами)», и предлагается новая модель, основанная на «непрерывной автоматизированной экспертизе ценности электронных документов [органа исполнительной власти центрального правительства], для реализации которой может потребоваться комбинация искусственного интеллекта и усилий опытных архивистов».

В отчёте подчеркнуты проблемы идентификации / выявления и управления изначально-электронными документами, а также потребность в более эффективных решениях.

В данном посте рассматриваются проблемы точной идентификации (выявления) изначально-электронных документов с целью управления ими.

Выявление и защита документов

Документы обычно являются свидетельствами / доказательствами того, что произошло - действия, деятельности или процесса, решения или текущего состояния (включая фото- и видеодокументы). Они могут иметь быть связаны с описательными метаданными (в том числе и в обязательном порядке), используемыми для описания контекста документов и для установления сроков их хранения.

Как и для любых других типов доказательств, следует защищать аутентичность, целостность и надежность документов в течение всего срока их хранения.

В бумажном мире этот результат достигался посредством хранения физических документов (включая распечатанные версии изначально-электронных документов) в бумажных делах или в физических хранилищах.

В течение последних двадцати или около лет подобный же результат достигался для (некоторых) электронных документов посредством (осуществляемого в основном вручную) копирования их с сетевого диска или из системы электронной почты (или через соединительный интерфейс) в специализированную систему управления электронными документами (electronic records management, ERM), с последующей «блокировкой» их в этой системе с целью предотвращения несанкционированного изменения или удаления. В состав большинства ERM-систем (ERMS – *к такому классу систем, в частности, относятся наши СЭД*) входили база данных для метаданных и взаимосвязанное с ней сетевое файловое хранилище для электронных объектов.

На рис. показано, что система управления электронными документами и контентом (EDRMS) получает документы из почтовой системы и с сетевых дисков

Основная проблема этой централизованной модели хранения заключается в том, что как бы хороша она ни была в плане защиты экземпляров хранящихся в ней документов – однако оригинальные версии этих документов, наряду со всеми прочими документами, которые либо не удалось выявить, либо невозможно было скопировать в ERMS-систему, остаются там, где они были созданы или захвачены.

В то же время документы, хранившиеся «внутри» ERMS-системы, фактически хранились в сетевой системе хранения файлов на сервере, которая (a) был доступна ИТ-специалистам, и (b) почти всегда имела резервные копии. Таким образом, существовало ещё больше копий.

Проблемы изначально-электронных документов

Имеется ряд ключевых проблем, связанных с изначально-электронными документами:

- Последовательная и точная **идентификация** (или «декларирование» - *речь идёт о признании электронного объекта подлежащим сохранению «полноценным» документом; на практике для этой цели обычно служит процесс регистрации*) всех документов вне зависимости от их вида и формата, созданных или сохранённых во всех возможных местах. Слишком долго основное внимание уделялось электронной почте и всему, что может

быть сохранено на сетевом диске, при этом обязанность идентифицировать документ возлагалась на конечных пользователей.

- Обеспечение **аутентичности, надежности и целостности** во времени. Для документов, хранящихся в ERMS-системе, это обычно делается посредством блокирования возможности их редактирования (в том числе в результате процесса «декларирования»), и предотвращения их удаления. Однако почти во всех случаях исходную версию документа (в почтовой системе или на сетевом диске) по-прежнему можно модифицировать. Прочие документы, которые не были идентифицированы и/или сохранены в ERMS, могут быть удалены.
- Обеспечение **доступности** изначально-электронных документов до тех пор, пока в них сохраняется потребность.

Вручную (или даже автоматически) невозможно последовательно и точно идентифицировать каждый изначально-электронный документ, который организация создаёт или захватывает, с тем, чтобы обеспечить аутентичность, надёжность, целостность и доступность этих документов с течением времени. Лишь небольшой процент изначально-электронных документов копируется в ERMS-системы.

Документы скрываются в личных почтовых ящиках, на личных дисках и в решениях, поддерживаемых третьими сторонами (использование которых часто неавторизованно). Документы могут существовать в различных формах и форматах; иногда они создаются или хранятся в «частных» системах или на платформах социальных сетей. Документы могут быть представлены в виде текстов, мгновенных сообщений, постов и цепочек сообщений в социальных сетях. Это могут быть рисунки, графические изображения, голосовые или видеозаписи.

Даже если документ идентифицирован, не всегда возможно сохранить его в ERMS-системе. Текстовые или мгновенные сообщения на мобильных устройствах - это пример, проблемы, существующей, по крайней мере, уже два десятилетия. В качестве более свежих примеров можно назвать сообщения в чате, реакции (смайлики, комментарии) и записи онлайн-совещаний.

И даже если бы в ERMS-системах удалось сохранять больший процент изначально-электронных документов, - исходные их версии практически всегда останутся там, где они были созданы или **документов?**

Один из подходов к решению проблемы - признать, что не все документы имеют одинаковую ценность, т.е. что не всеми документами нужно управлять одинаково.акой-то степени такой образ мышления уже нашёл отражение в рубриках в структуре перечней видов документов с указанием сроков хранения, и в том внимании, которое уделяется:

- Документам, имеющим постоянную или архивную ценность и подлежащим передаче на хранение в архивные учреждения;
- Специфическим видам документов, которые должны создаваться и/или сохраняться организацией в течение установленных минимальных сроков (иногда довольно долго, но не «вечно»), в юридических целях, во исполнение законодательно-нормативных требований или в целях аудита;

- Документам, которые не подпадают под законодательные-нормативные или иные обязательные требования, но которые организация сама решает хранить в течение определённых минимальных сроков;
- Всему остальному.

Дифференциация (triaging *это один из видов экспертизы ценности документов*) означает, что документами можно управлять так, как это требуется на соответствующем уровне, при этом ничего не упускается. Здесь требуется подход на основе менеджмента риска.

Для документов, имеющих постоянную ценность или подпадающих под законодательно-нормативные или иные обязательные требования, это означает уделение данным документам наибольшего внимания, а также то, что предпринимаются все возможные усилия для обеспечения того, чтобы они могли быть и были идентифицированы (декларированы) и управлялись соответствующим образом. Сюда входит обеспечение возможности идентифицировать и захватить эти документы в системах, используемых для их создания или захвата (например, ключевые по важности сообщения электронной почты).

Аналогичный подход будет применяться к документам, которые необходимо хранить в юридических целях, в целях исполнения законодательно-нормативных и иных требований или в целях аудита, - но с пониманием того, что некоторые из этих документов (например, электронные письма) могут оставаться в исходной системе, в которой они были созданы или захвачены. Технологические решения могут использоваться для идентификации или тегирования (маркировки) этих документов. Уничтожение таких документов должно осуществлять только после проведения в какой-то форме экспертизы ценности, и следует сохранять документы, отражающие принятие решения об уничтожении, а также что именно было уничтожено.

Все другие документы могут оставаться на хранении там, где они были созданы или захвачены, и им могут быть установлены минимальные сроки хранения, по истечении которых они могут быть уничтожены без проведения дополнительной экспертизы - но при этом следует вести документацию, отражающую основные метаданные каждого документа (включая сведения об исходном место хранения).

Защита - или доказательство - аутентичности, целостности и надёжности документов

При обеспечении защиты документов предполагается, что документы не должны быть изменены или удалены.

Если говорить более точно, то не должно быть ***несанкционированного*** *изменения или уничтожения документов. Санкционированные изменения, осуществляемые в соответствии с установленными регламентами, могут быть желательны и даже необходимы – особенно тогда, когда речь идёт о выполняющих функции документов базах данных.*

Реальность при использовании электронных документов такова, что они могут быть изменены в любое время посредством появления новых цепочек,

новых редакций, новых чатов - или даже с помощью редактирования графических образов (фотошопа).

Более реалистичный подход может заключаться в использовании информации о том, что было изменено, кем и когда - не для защиты документа, а для обеспечения доказательственного «следа», подтверждающего, чем документ был или стал. «Явной уликой» (smoking gun evidence) при работе с большинством изначально-электронных документов являются метаданные, которые фиксируются их захвате или модификации документов, а не (обязательно) добавленные описательные метаданные.

Ситуации могут быть разными в зависимости от роли документов и их ценности. Иногда достаточно контролировать неизменность документа (например, используя хеши) – когда утрата документа влечёт не слишком большие последствия, и/или вредит в первую очередь самому предъявителю документа.

В других ситуациях абсолютно необходимо сохранить именно сам документ в т.ч. его содержание. Например, в банковской сфере по этой причине существуют нормативные требования к хранению определенных документов на физически неизменяемых носителях. Во многих отраслях есть требования к сохранению многочисленных экземпляров, в том числе записанных на носителях разных видов, размещённых в автономных системах, в облачных или территориально-разнесённых хранилищах – чтобы максимально затруднить одновременную модификацию или уничтожение сразу всех экземпляров.

Например:

- Кто-то может создать документ (метаданные документируют каждую редакцию, и каждую такую редакцию можно просмотреть);
- Документ может быть утверждён в электронном виде (что фиксируется в метаданных);
- Затем кто-то модифицирует утвержденную версию;
- Всё вышеперечисленное документируется в полях метаданных «когда изменено» (modified), «кем изменено» (modified by) и в метаданных об утверждении документа;
- Следует (или можно) также фиксировать, кто и когда просматривал документ.

Записанные в файлах графических образов EXIF-метаданные (*набор метаданных для графических образов*) предоставляют собой аналогичный вид доказательств (и могут даже включать GPS-информацию).

Какой документ с большей вероятностью будет принят в качестве надлежащего доказательства?

- Документ, хранящийся в EDRMS-системе, версии или редакции которого могут существовать во многих других местах, включая сетевые файловые ресурсы, систему электронной почты и даже ленты с резервными копиями;

- Документ, хранящийся в системе, в которой имеется полный набор метаданных о доступе и изменениях, или же имеется самая последняя «ветка» проводимых по электронной почте дискуссии?

Что юрист, что профессиональный консультант по вопросам управления документами на вопросы такого рода всегда отвечает «Это зависит от конкретных обстоятельств».

Выводы

В конечном итоге, должна иметься возможность подтвердить аутентичность, надёжность и целостность документов на основе информации / метаданных, которые являются составной частью изначально-электронного документа: кем и когда он был создан; контекст, в котором он была создан; и как он взаимосвязан с другими документами.

Возможно, вместо того, чтобы сосредотачивать внимание на попытках идентифицировать и захватить все изначально-электронные объекты, которые потенциально могут быть документами, и затем «защищать» версию этого документа, - более практичным и простым будет оставить большинство документов там, где они были созданы или захвачены (и сохраняются в соответствии с политиками установления и отслеживания сроков хранения), и использовать метаданные об изменениях и версиях для подтверждения их аутентичности.

В конце концов, такой способ обеспечения защиты аутентичности документов может оказаться гораздо более простым, чем полагаться на ручную идентификацию или декларацию документов.

СТРАТЕГИЧЕСКОЕ УПРАВЛЕНИЕ ИНФОРМАЦИЕЙ - ДЕЛО СКУЧНОЕ, НО НЕОБХОДИМОЕ

Источник: сайт CMSWire.com https://www.cmswire.com/information-management/information-governance-is-boring-but-necessary/

Стратегическое управление информацией – скучное дело. Ну вот, я сказал это вслух. И хотя вроде бы все должны быть в нём заинтересованы, это, как правило, не так.

Я помню бум в сфере управления документами после 11 сентября 2001 года (*тогда в результате террористической атаки были уничтожены две башни Всемирного торгового центра в Нью-Йорке*). Год спустя интерес снова улетучился. Так же, как мало кто хочет заниматься домашним хозяйством, лишь немногие готовы взять на себя задачи, связанные со стратегическим управлением информацией - Вы прибираетесь и раскладываете вещи по местам только для того, чтобы другие люди снова навели беспорядок. Поэтому было бы нечестно говорить, что мы когда-либо сможем сделать

стратегическое управление привлекательным занятием; однако мы можем, по крайней мере, сделать его менее скучным и гораздо более эффективным, чем сегодня.

Что такое «стратегическое/полномасштабное управление информацией» (Information Governance)

Давайте начнем с того, что разберёмся – что же такое «стратегическое управление». Стратегическое управление информацией - это применение правил, процессов, процедур и наведение порядка в управлении и хранении информации. Исторически оно полагалось на сотрудников в целом и на специализированный персонал, которые определяли, применяли и контролировали деятельность по стратегическому управлению. Но технологии быстро меняются, и объемы, разнообразие и скорость создания и обработки корпоративной информации также быстро растут.

Поскольку стратегическое управление, по определению, включает создание и соблюдение правил, не стоит ли в большей степени использовать в помощь себе такие технологии, как машинное обучение (machine learning, ML)? Не поймите меня неправильно - такие системы на основе машинного обучения существуют, но в данной области применяются они всё ещё относительно редко. Решения на основе машинного обучения могут интерпретировать и применять правила и адаптироваться к сложным изменениям правил со скоростью и в объёмах, невозможных для человека. Так что, хотя системы стратегического управления информацией на основе машинного обучения доступны, - профессионалы в области стратегического управления информацией, похоже, не слишком заинтересованы в том, чтобы их использовать.

Уроки практического примера стратегического управления с использованием технологии машинного обучения

Недавно я беседовал с представителями компании, которая широко использует машинное обучение в своей системе управления документами. Хотя сама технология была увлекательной с точки зрения любителя новинок такого рода, еще более увлекательным оказался их опыт её применения в рамках «боевой» системы.

Изначально проектная группа представила свой проект как связанный с документами. Это не вызвало абсолютно никакого интереса. Год спустя, после исключения термина «документ» из всей документации и замены его словом «файл», результатом стала немедленная заинтересованность со стороны высшего руководства, обеспокоенного рисками. Это была несколько упрощенная семантическая подмена, но результаты говорят сами за себя.

Точно так же, когда проект был представлен группе управления документами, сразу было сильнейшее отторжение, поскольку эта группа восприняла его как автоматизацию их работы. Год спустя, когда сразу же была сделана оговорка о том, что машинное обучение (от первоначально использовавшегося термина «искусственный интеллект» отказались) будет

бесполезно без их опыта, - проект был с энтузиазмом воспринят как нечто, за что специалисты по управлению документами могли ухватиться, чтобы сохранить свои рабочие места и поднять свой статус.

Итак, проект стратегического управления предлагался дважды. В первый раз к нему не было никакого интереса. Во второй раз, когда тот же самый проект был представлен с небольшими изменениями в его подаче, все его приняли. Проект стратегического управления, с которым никто не хотел иметь ничего общего, стал чем-то захватывающим и вдохновляющим.

И вот что важно: это не разовая ситуация. То, что происходило в этой компании, происходило за последние несколько лет с небольшими вариациями множество раз, и есть пара ключевых уроков, которые нужно усвоить любому, кто попытается продвигать или «продавать» стратегическое управление в своей организации.

Чему могут научиться специалисты по управлению документами

Первый урок заключается в том, что никому нет дела до управления документами. Пусть меня за эти слова возненавидят, - но это правда. И в то же время, это печально. Специалистов по управлению документами недооценивают и часто неправильно понимают. Они обеспечивают чрезвычайно важный сервис, которая редко получает должное признание. Но реальность такова, что по мере того, как объемы, разнообразие и скорость данных и информации росли в геометрической прогрессии, традиционные практики управления документами так и не сумели адаптироваться с тем, чтобы как-то решить эту проблему.

Как отраслевой аналитик, я общаюсь с бесчисленным множеством покупателей и продавцов технологий управления документами. Все они без исключения говорят мне, что борьба за внимание, бюджет и поддержку со стороны высшего руководства становятся всё более трудным делом. Но всё совсем иначе, когда речь заходит об управлении рисками и обеспечении исполнения законодательно-нормативных требований. Или, говоря более точно, о смягчении рисков и борьбе с несоблюдением требований, поскольку именно эти темы действительно привлекают внимание руководства. И если усилия по уменьшению риск и степени неисполнения установленных требований удастся автоматизировать с помощью машинного обучения, тем лучше! Таким образом, простая игра с терминологией, когда «документы» заменяются на «файлы» (или «данные») может заставить сработать «включатель внимания». В этом нет ничего удивительного, поскольку такие законодательно-нормативные акты, как HIPAA (*американский «Закон о переносимости и подотчётности медицинского страхования», содержащий довольно жёсткие требования по защите медицинских персональных данных*) и GDPR (*закон о защите персональных данных Евросоюза*) сегодня становятся лишь верхушкой растущего нормативного айсберга, - и соблюдение соответствующих требований будет обеспечиваться гораздо более строго, чем в прошлом.

Аналогичным образом, если заявлять специалистам по управлению документами, что искусственный интеллект может и будет делать их работу так же хорошо, если не лучше, как они сами, это вряд ли будет воспринято позитивно. Поверьте, я знаю. Пару лет назад я выступал с пленарным докладом в Нэшвилле (Nashville) перед членами международной ассоциации специалистов по управлению документами и информацией ARMA International, и, скажем так, отклик на мои идеи был неоднозначным, хотя факты были вполне точными: принципы управления документами основаны на правилах, а решения на основе технологии машинного обучения способны применять правила быстрее и точнее, чем люди. Никто не хочет слышать разговоры о том, что их работа будет автоматизирована.

В свою защиту скажу, что, хотя аудитория могли воспринять мой доклад именно так, в тех идеях, которые я хотел донести до публики, было куда больше нюансов. Технология машинного обучения автоматизирует большую часть работы специалистов по управлению документами, однако без руководства со стороны настоящих экспертов инструменты машинного обучения ничего не могут сделать.

В конце концов, мир искусственного интеллекта и машинного обучения - это не что иное, как множество инструментов и гора данных, которые позволяют предсказывать вероятности. Эти технологии максимально эффективны, когда их дополняет человеческий опыт, который может направлять их и работать совместно с ними. Специалисты по управлению документами никогда не смогут даже надеяться на то, чтобы справиться с информационным половодьем, захлёстывающим их организации. Просто отсеять пшеницу от плевел практически невозможно. Но адаптируясь к технологиям машинного обучения и работая с ними рука об руку, специалисты-люди смогут свою работу лучше, чем когда-либо прежде.

Стратегическое управление никогда не будет увлекательным, но оно всегда будет востребованным

Стратегическое управление информацией, возможно, никогда не станет самой интересной темой, однако модернизация практик, процедур и инструментов поможет решить сегодняшние проблемы реального мира. Смягчение рисков и использование существующих возможностей для продвижения своей карьеры создает «момент времени» для роста и развития. Такие возможности предоставляются не столь уж и часто, так что хватайтесь за них, пока можете. Перефразируйте и обновите аргументацию, которую Вы используете в Вашей организации, и реакция на это может Вас приятно удивить.

ИТАК, КАКУЮ ЖЕ ПОЛЬЗУ ПРИНОСИТ НАМ УПРАВЛЕНИЕ ДОКУМЕНТАМИ?

Источник: сайт TSLAC
https://www.tsl.texas.gov/slrm/blog/2021/04/how-does-records-management-benefit-us-anyway/ , Брианна Кокран

К настоящему моменту Вы, вероятно, уже знаете, что Ваши органы государственной власти по закону обязаны соблюдать законы об управлении документами. Однако часто бывает сложно мотивировать себя, коллег и руководство внедрять что-либо только потому, что это «требуется». В природе человека сопротивляться всему тому, что мы воспринимаем как трудное, трудозатратное и/или навязанное.

Группа поддержки управления документами RMA (records management assistance) при Комиссии по вопросам библиотечного и архивного дела штата Техас (TSLAC) хотела бы, чтобы управление документами было как можно более увлекательным! Конечно, соблюдение требований законодательства к управлению документами обязательно, – однако внедрение разумной программы управления документами не обязательно должны быть сложными, трудоёмкими или восприниматься как некое насилие. В конце концов, наличие сильной программы управления документами дает Вашему подразделению много преимуществ, в числе которых правовая защита, повышение эффективности, сокращение затрат, улучшение общественного мнения о Вашей структуре и защита важнейших документов.

В этой статье мы подробнее рассмотрим упомянутые выше преимущества хороших практик управления документами. Мы надеемся, что статья станет полезным ресурсом для государственных и муниципальных служащих, помогая стимулировать хорошие практики управления документами в Ваших органах и организациях.

Пять преимуществ управления документами

1. Обеспечение правовой защиты

Соблюдение правовых требований, сформулированных в наших опубликованных законах и нормативных актах, обеспечивает правовую защиту Вашего подразделения. Например, избыточно или недостаточно длительное хранение документов представляет собой правовой риск. В случае судебного разбирательства или аудита Вашему подразделению, возможно, придется раскрыть документы, которые могли быть уничтожены много лет назад, или

же, что ещё хуже, Вы не сможете представить документы, которые были уничтожены слишком рано. Соблюдение опубликованных Комиссией TSLAC указаний по срокам хранения документов и действиям по их истечении (*аналог наших Перечней*) и уничтожение документов в строгом соответствии с ними помогает снизить этот правовой риск.

2. ***Повышение эффективность (высвобождение времени и пространства)***

Хорошая программа управления документами также поможет Вашему подразделению работать более эффективно, потому что сотрудники не будут зря тратить время и силы на поиски информации. Люди будут тратить больше времени на поиск документов, если их хранится много, - а это влияет на общую эффективность Вашего подразделения. Своевременное уничтожение документов по истечении установленных сроков хранения высвободит место для хранения и упростит доступ к тем документам, которые Вам действительно необходимы.

3. Снижение затрат

Хорошее управление документами также экономит деньги! Когда Вы освобождаете место для хранения и повышаете свою эффективность, это также снижает Ваши расходы. Хранение слишком большого количества документов сверх сроков хранения может привести к увеличению затрат на хранение и обслуживание. Расходы в этом случае на дополнительные физические шкафы для хранения документов или на дополнительное пространство на сервере – зря потраченные деньги.

4. Улучшение общественного мнения

Государственным и муниципальным органам власти, которые используют передовые методы управления документами, также проще поддерживать свою

хорошую репутацию в глазах общественности. И наоборот – следствием плохой практики управления документами часто является появление в обществе негативных настроений. Даже проведенное с самыми лучшими намерениями уничтожение огромного количества документов может показаться подозрительным – если Вы до этого долгое время уничтожением не занимались. Уничтожение документов лучше всего проводить регулярно и в соответствии со сроками хранения, чтобы избежать негативного восприятия.

5. ***Защита важнейших документов***

Активно выполняемая программа управления документами также поможет защитить важнейшие (*т.е. необходимые для обеспечения непрерывности деловой деятельности в случае ЧП и для восстановления после ЧП*), исторически ценные и имеющие постоянную ценность документы органа власти от таких вещей, как вредители, плесень, кража или нарушения безопасности. Неспособность защитить эти документы потенциально может привести к уголовным наказаниям и штрафам. Например, преднамеренное уничтожение документа до истечения установленного ему срока хранения может классифицироваться как проступок класса А (Class A misdemeanor), за который предусмотрено максимальное наказание в виде одного года тюремного заключения и штрафа в размере до 4 тысяч долларов.

Комментарий: Всё сказанное верно, - но самые «сладкие» преимущества хорошего управления документами все-таки другие! Можно назвать следующие:

- Создание совершенно новых возможностей для ведения деловой деятельности государственного или муниципального органа. Обычно это подразумевает активное участие службы управления документами во внедрении инновационных технологий, поддерживающих основную деловую деятельность этого органа (в отличие от автоматизации деятельности самой этой службы) – а также взятие «под своё крыло» значительно более широкого круга документов и информации.

В эпоху активного внедрения искусственного интеллекта и больших данных, именно служба управления документами обладает многими знаниями и навыками, необходимыми для поддержки законного, прозрачного и эффективного использования этих технологий.

Именно служба управления документами (вместе с юристами) обычно лучше всех в организации разбирается в вопросах защиты персональных данных и в обеспечении долговременной сохранности ценных информационных активов.

- В США очень большое значение имеют деятельность по раскрытию электронных документов и информации в случае судебных споров,

расследований и аудита; по выполнению запросов на основании закона о свободе доступа к государственной информации; а также по обеспечению непрерывности деловой деятельности в случае катастроф. Популярными направлениями работы становятся стратегическое управление данными и информацией, включая управление электронной почтой, социальными сетями и веб-сайтами. Всё это служба управления документами может полностью или частично взять на себя – получив, конечно, немалую дополнительную нагрузку, но также и дополнительные ресурсы и более высокий статус.

Защитить себя любимого от «сумы и тюрьмы» очень важно – тут спора нет. Бесценно, однако, когда удаётся от того же самого защитить своё высшее руководство, и оно об этом знает!

УДАЛЁННАЯ РАБОТА: ДВЕ ТРЕТИ ОПРОШЕННЫХ СЧИТАЕТ, ЧТО ПУТИ НАЗАД НЕТ

Источник: блог компании Formtek https://formtek.com/blog/telework-two-thirds-say-that-theres-no-going-back/

Удалённая работа стала новой нормой. В ходе опроса, проведенного компанией 451 Research (см.https://go.451research.com/2020-mi-covid19-remote-work-influence-unified-communications-and-collaboration.html), было установлено, что 80 процентов компаний внедрили или расширили возможности для своих сотрудников работать удалённо. Примерно две трети компаний сообщило о том, что они ожидают, что некоторые из этих политик останутся в силе после того, как мы полностью преодолеем пандемию Covid-19. Согласно опросу Flexjobs (https://www.flexjobs.com/blog/post/survey-productivity-balance-improve-during-pandemic-remote-work), две трети сотрудников, перешедших на удалённую работу во время пандемии, сказали, что не хотят возвращаться к прежнему режиму работы.

Вице-президент фирмы Forrester Мэтью Гуарини (Matthew Guarini, https://www.forrester.com/Matthew-Guarini) полагает, что когда пандемия закончится, в организациях будет в среднем в три раза больше дистанционно работающих сотрудников, чем до пандемии. Инструменты для виртуальной и коллективной работы будут приобретать всё большее значение для поддержки деятельности разрозненных сотрудников. «ИТ-директора, которые обеспечат сотрудникам удобные условия, станут маяками» (см.https://www.informationweek.com/strategic-cio/remote-reshapes-the-future-of-work/d/d-id/1339886).

Даррен Мерф (Darren Murph), руководитель отдела удаленной работы в GitLab, отметил, что «для многих переход на удаленную работу стал действительно сложной задачей, потому что это был не их выбор, и по большей части их компании были к этому не готовы. Теперь люди становятся лучше в

этом, поэтому я надеюсь, что в предстоящем году удалённая работа станет более привычным для них делом».

Генеральный директор еомпании Sophya Вишал Пунвани (Vishal Punwani, https://www.linkedin.com/in/vishal-punwani-md/) говорит, что «полного возвращения к прежней норме не будет. И преуспеют те компании, которые быстрее это осознают» (https://www.informationweek.com/strategic-cio/remote-reshapes-the-future-of-work/d/d-id/1339886).

ИСО/МЭК: ОПУБЛИКОВАН НОВЫЙ СТАНДАРТ ISO/IEC 23264-1 «ЦЕНЗУРИРОВАНИЕ АУТЕНТИЧНЫХ ДАННЫХ»

Источник: сайт ИСО https://www.iso.org/standard/78341.html https://www.iso.org/obp/ui/#!iso:std:78341:en

Как сообщил сайт международной организации по стандартизации, в марте 2021 года был опубликован стандарт **ISO/IEC 23264-1:2021 «Информационные технологии – Цензурирование аутентичных данных – Часть 1: Общие положения»** (Information security - Redaction of authentic data - Part 1: General) объёмом 20 страниц, см. https://www.iso.org/standard/78341.html и https://www.iso.org/obp/ui/#!iso:std:78341:en .

Стандарт разработан подкомитетом SC27 «Информационная безопасность, кибербезопасность и защита неприкосновенности частной

жизни» (Information security, cybersecurity and privacy protection) Объединенного технического комитета ИСО/МЭК JTC1 «Информационные технологии» (Information technology).

В аннотации на документ сказано:

«Схемы цифрового удостоверения (attestation schemes), - в частности, схемы подписания усиленными электронными подписями и коды аутентификации сообщений, - могут использоваться для обеспечения целостности данных и аутентификации источника данных.

Схема удостоверения с поддержкой цензурирования (redactable attestation scheme) делает возможным удостоверение сообщения таким образом, что если определенные части удостоверенного сообщения (известные как «поля») будут отцензурированы (стёрты, вымараны или безвозвратно удалены), то, несмотря на это, действительность удостоверения отцензурированного сообщения по-прежнему может быть проверена.

Говоря точнее, после удостоверения сообщения удостоверяющее лицо, владеющее закрытым ключом удостоверения (private attestation key), может выделить части сообщения, которые впоследствии могут быть отцензурированы (в смысле стандарта ISO/IEC 27038:2014) любой третьей стороной, располагающей только самим сообщением, его электронным удостоверением и ключом цензурирования удостоверяющего лица (*речь идёт об открытом ключе, парном закрытому ключу удостоверения – Н.Х.*). Любая иная модификация удостоверенного сообщения (например, цензурирование других частей сообщения или вставка / изменение любых частей) делает удостоверение недействительным.

Схемы удостоверения с поддержкой цензурирования являются базовыми строительными блоками во многих приложениях, обеспечивающих защиту неприкосновенности частной жизни, таких, как сохраняющий неприкосновенность частной жизни обмен информацией или аутентификация, в рамках которых сторона может принять решение раскрывать только ту информацию, которую абсолютно необходимо передать получателю, в то время как получатель информации по-прежнему сможет убедиться, что полученная информация была ранее удостоверена - например, государственным органом.

Цель стандартов серии ISO/IEC 23264 заключается в том, чтобы скорректировать имеющие место нестыковки и непоследовательность в определении свойств в существующих спецификациях подобных схем, и облегчить внедрение этой технологии на практике. В частности, документ ставит своей целью заложить фундамент для последующих частей стандарта (например, фокусируя внимание на конкретных алгоритмах сохраняющего аутентичность цензурирования определенных форматов документов - текста, изображений, видео и т.д.) путем установления и определения единой терминологии и свойств подобных схем.

Состоящий из нескольких частей стандарт ISO/IEC 23264 будет дополнять стандарт ISO/IEC 27038:2014 «Информационные технологии – Методы и средства обеспечения безопасности – Требования к электронному цензурированию» (Information technology - Security techniques - Specification for

digital redaction, *в России адаптирован как ГОСТ Р ИСО/МЭК 27038-2016 «Информационные технологии. Методы обеспечения безопасности. Требования и методы электронного цензурирования»,* http://protect.gost.ru/v.aspx?control=8&baseC=6&id=196572), который регламентирует цензурирование электронных документов, не рассматривая специально вопрос сохранения аутентичности данных».

«… Настоящий документ определяет свойства криптографических механизмов для цензурирования данных с сохранением их аутентичности. В частности, он определяет процессы, задействованные в этих механизмах, участвующие стороны и криптографические свойства».

Содержание документа:

Предисловие

Введение

1. Область определения
2. Нормативные ссылки
3. Термины и определения
4. Сокращения и обозначения
5. Общая модель и процессы
6. Криптографические свойства схем удостоверения с поддержкой цензурирования

Библиография

КИТАЙ: УСКОРЕНИЕ ПРИМЕНЕНИЯ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В УПРАВЛЕНИИ ДОКУМЕНТАМИ И АРХИВНОМ ДЕЛЕ

Источник: Сеть подготовки специалистов в области архивного дела и управления документами http://www.dapx.org/shownews.asp?ID=528 http://www.zgdazxw.com.cn/news/2021-01/15/content_316467.htm

В последние годы технология искусственного интеллекта стремительно развивалась, вызывая изменения во многих областях. Она стала национальной стратегической технологией, за которой гоняются правительства, отрасли, научно-исследовательские институты и потребительские рынки. Эта технология проникла во все аспекты работы и жизни людей, и играет огромную роль в улучшении качестве жизни, в повышении эффективности труда и в содействии социальному развитию.

Китай придаёт большое значение развитию технологии искусственного интеллекта, и страна сформулировала связанные с искусственным интеллектом политики на национальном, отраслевом и местном уровнях, с тем, чтобы

активно содействовать развитию и применению данной технологии. В процессе своей стратегической трансформации архивная отрасль также активно осваивает технологию искусственного интеллекта. В настоящее время ряд архивных учреждений взял на себя лидирующую роль во внедрении и проведении исследовательских работ на основе технологии искусственного интеллекта, и уже удалось достичь определенных результатов.

С точки зрения текущей ситуации с развитием технологии искусственного интеллекта и насущных потребностей архивной отрасли, данная технология в основном может использоваться в четырех типовых вариантах применения, а именно:

- Оцифровка архивных материалов;
- Классификация и контроль;
- Повышение качества и восстановление цвета архивных изображений;
- «Умная» безопасность.

Первый вариант применения - это работа по оцифровке архивных материалов. «Оцифровка» - это популярный термин, который в последние годы получил широкое распространение в архивной отрасли. Целью оцифровки архивных материалов является распознавание содержимого графических изображений, аудиовизуальных записей и иных материалов и преобразование их в информацию, которую можно редактировать, обрабатывать, анализировать и искать с помощью компьютера. Оцифровку архивных материалов можно разделить на четыре типа: распознавание текста (OCR) в электронных копиях бумажных документов; оцифровка фотографий; оцифровка аудиозаписей и оцифровка видеоматериалов.

На фоне энергичных усилий Государственного архивного управления Китая (далее Госархив) по реализации стратегии «оцифровки и повышения качества архивных фондов», оцифровка по всему Китаю архивных фондов на всех уровнях архивов дала замечательные результаты. По состоянию на конец 2019 года, суммарный объём электронных копий архивных документов, созданных китайскими архивами всех уровней, достиг в масштабах страны 14 миллионов гигабайт. Некоторые региональные архивные управления приступили к полнотекстовому распознаванию отсканированных бумажных документов.

Исходя из текущей ситуации, Госархив в декабре 2019 года выпустил стандарт DA/T 77-2019 «Требования к распознаванию текста в электронных копиях бумажных документов» (纸质档案数字复制件光学字符识别（OCR）工作规范 , самоназвание на английском языке: Specification for optical character recognition (OCR) of digital copies of paper-based records), что указывает на то, что данный вид работ повсеместно осуществляется в архивной отрасли.

Качество OCR-распознавания на основе технологии искусственного интеллекта, в случае упрощённого печатного текста (*не будем забывать, речь идёт о китайских иероглифах, распознавать которые намного сложнее, чем*

фонетические алфавиты) превысило 98% (*это примерно тот уровень качества, когда обеспечение 100% точности итогового текста, когда в этом есть необходимость, уже не требует колоссальных дополнительных трудозатрат*), что обеспечивает техническую поддержку непрерывных усилий архивов по выполнению такого вида работ.

В последние годы быстро развивалась технология распознавания речи, и качество распознавания речи на стандартном диалекте китайского языка превысило 97%. Технология распознавания лиц также становится более зрелой, и она начала широко использоваться в сфере безопасности, аутентификации при выполнении финансовых транзакций и в других областях.

В то же время, по мере постоянного развития технологий обработки изображений и снижения затрат на хранение, объёмы цифровых аудио- и видеоархивов продолжают расти. Архивные учреждения и службы также активно изучают возможности «полной оцифровки» цифровых аудиовидеоархивов и проводят соответствующие исследования на основе технологий искусственного интеллекта, в ходе которых достигнуты большие успехи. Так, Архивы провинции Чжэцзян (浙江省档案馆) и компания iFlytek (科大讯飞 - *частично государственная компания, известная своими решениями для распознавания речи и работами в области искусственного интеллекта*) совместно выполнили научно-технический проект Госархива «Исследование приложений технологии искусственного интеллекта для упорядочения и использования аудиовизуальных архивных материалов». В проекте, посредством комплексного использования распознавания голоса, распознавания лиц и иных технологий, речь преобразуется в текст, обеспечивается «умная» группировка по людям и т.д. Результаты проекта были официально опубликованы 3 сентября 2020 года.

Вторая область применения - это область классификации и рассекречивания. Классификация документов и вопросы определения степени их секретности (конфиденциальности) - это два различных вида работ, но с технической точки зрения между ними есть общие черты, поэтому автор объединяет их в одну категорию для целей анализа.

Классификация и установление сроков хранения всегда были основными задачами в сфере управления документами, однако из-за недостаточного внимания и отсутствия специалистов эта работа всегда для ряда архивных учреждений и служб низших уровней создавала непростые проблемы. Использование технологии искусственного интеллекта для содействия недостаточно опытному персоналу архивно-документационных в выполнении работы по классификации документов может решить сложные проблемы управления документами в организациях, поможет повысить эффективность и точность упорядочения документов и, таким образом, определенно имеет практическую ценность.

Сложность, высокий риск и высокая ответственность за результаты рассекречивания; ограниченное количество экспертов соответствующей квалификации и несогласованные друг с другом стандарты в определенной

степени препятствовали раскрытию архивных документов для общественности. Недавно пересмотренный Закон об архивах официально вступил в силу, и одним из основных нововведений стало сокращение периода ограничения доступа к архивным материалам, расширение состава раскрываемых документов, расширение спектра каналов и методов раскрытия, а также появление конкретных положений об ответственности должностных лиц, не обеспечивающих раскрытие архивных документов в соответствии с законом. Данный шаг, несомненно, будет способствовать дальнейшему увеличению доступности архивов.

В настоящее время некоторые архивные учреждения и службы берут на себя ведущую роль в проведении исследований и прикладных работ на основе технологии искусственного интеллекта. Так, например, компания China Mobile Communications Group Jiangsu Co. Ltd. (中国移动通信集团江苏有限公司) на основе ИИ-алгоритма TextCNN (Text Classification Using a Convolutional Neural Network – «классификация текста с использованием свёрточной нейросети»; это алгоритм, использующий свёрточную нейронную сеть для классификации текста) проводит работу по определению сроков хранения документов.

Архивное управление провинции Аньхой (安徽省档案局) и компания iFlytek совместно выполнили научно-технический проект Госархива «Применение технологии искусственного интеллекта для контроля над документами» (人工智能技术在档案划控上的应用), помогая управляющему документами персоналу определять конфиденциальность документов и выбирать надлежащие меры контроля и управления.

Третья область применения – повышение качества и восстановление цвета архивных изображений. К 70-летию основания Китайской Народной Республики Центральный архив выпустил самую длительную и полную цветную видеозапись церемонии основания КНР, вызвавшую огромную сенсацию в Интернете. Эта видеозапись была показана или перевыложена крупными СМИ, и уже за первые 24 часа. количество просмотров достигло 320 миллионов.

При создании примерно тогда же вышедшего в прокат фильма «Решающий момент» (《决战时刻》) много средств было потрачено на восстановление цвета черно-белых фотографий церемонии основания КНР и повышение их разрешения до 4K, что также вызвало больший общественный резонанс.

Архивные изображения после улучшения качества и восстановления цвета в определенной степени изменили свой первоначальный вид, и их больше нельзя рассматривать и использовать как «архивные» документы. Однако в нашу информационную эпоху чёткие и красочные исторические изображения могут не только разжечь любопытство людей и повысить их интерес к истории, стимулировать чувство национальной гордости – они также позволяют в полной мере продемонстрировать роль архивов в патриотической пропаганде и воспитании.

Источник: https://kknews.cc/zh-my/entertainment/y34roza.html

В этой связи усилия по восстановлению цвета и повышению качества архивных изображений имеют определенное социальное значение. Второй исследовательский отдел Института архивной науки и технологий Госархива провёл соответствующие эксперименты в этой области и подало заявку на выполнение проекта по данной теме. Следующим шагом будет продолжение прикладных исследований в области повышения качества и восстановления цвета архивных изображений на основе технологии искусственного интеллекта.

Четвертая область применения – «умные» подходы к обеспечению безопасности. К настоящему времени интеллектуальные технологии обеспечения безопасности достигли очень высокого уровня зрелости. Начиная от строительства безопасного города в 2005 году до строительства «умного» города, начатого в 2011 году, а также включая такие ключевые проекты в сфере безопасности, как «проект Skynet» (天网工程 – *масштабная китайская система видеонаблюдения, обеспечивающая идентификацию пешеходов в реальном времени*), «проекта Xueliang» (雪亮工程 – *проект наблюдения и мониторинга, ставящий задачу обеспечит покрытие всех общественных мест и территорий в стране*), тень технологии искусственного интеллекта можно увидеть повсюду.

В рамках создания «умных» (интеллектуальных) архивов, многие архивные учреждения и службы включили интеллектуальные системы безопасности в свои планы и программы внедрения. В настоящее время передовые интеллектуальные системы безопасности в основном используют

технологии мультимодального распознавания, которая объединяет распознавание лиц, походки, характерных особенностей и голоса человека, что дополнительно повышает уровень безопасности, поддерживаемый такой системой, и обеспечивает более качественную техническую поддержку безопасности деятельности архивов.

В настоящее время технология искусственного интеллекта становится всё более зрелой, и такие функции, как распознавание текста, содержащего упрощённые китайские иероглифы (*применяются в КНР, в отличие от Тайваня и некоторых других стран и регионов*), и речи на официальном северокитайском диалекте, уже могут напрямую применяться при работе с документами.

На данном этапе развития технологии искусственного интеллекта, чтобы расширить спектр вариантов её применения, необходимо продолжить работу по оптимизации алгоритмов, по разработке моделей и обучению, другие работы по внедрению ИИ-технологий, - а также инвестировать определенные средства.

Чтобы идти в ногу со временем, нам необходимо продолжить изучение вариантов применения технологий искусственного интеллекта в управлении документами и архивном деле, активизировать исследования и усилия по внедрению этих технологий, как можно скорее разработать и улучшить соответствующие стандарты. Нужно стремиться к тому, чтобы сформировать междисциплинарные группы специалистов, которые обладают знаниями как в сфере технологий, так и в архивном деле, а также научно обоснованно использовать информационные технологии нового поколения для ускорения стратегической трансформации деятельности архивов.

ИСО: СТАНДАРТ ПО СТРАТЕГИЧЕСКОМУ УПРАВЛЕНИЮ ИНФОРМАЦИЕЙ ВЫШЕЛ НА СТАДИЮ ПУБЛИЧНОГО ОБСУЖДЕНИЯ

Источники: сайт igguru.net / сайт ИСО https://igguru.net/2021/05/04/iso-standard-for-information-governance-enters-enquiry-stage/
https://www.iso.org/standard/77915.html
https://www.iso.org/obp/ui/#!iso:std:77915:en

4 мая 2021 года сайт IGGuru.net опубликовал коротенькую, буквально в одну строку новость о том, что разрабатываемый техническим комитетом Международной организации по стандартизации (ИСО) ТС46 «Информация и документация» первый стандарт по стратегическому управлению информацией вышел на стадию публичного обсуждения (DIS). Это завершающий этап

работы, в случае более-менее успешного прохождения которого стандарт может быть официально опубликован уже в этом году.

Чуть позднее сайт ИСО также сообщил о выходе на стадию DIS проекта международного стандарта I**SO/DIS 24143 «Информация и документация - Стратегическое управление информацией - Концепция и принципы»** (Information and documentation - Information Governance - Concept and principles) объёмом 10 страниц основного текста, см.https://www.iso.org/standard/77915.html и https://www.iso.org/obp/ui/#!iso:std:77915:en .


DRAFT INTERNATIONAL STANDARD
ISO/DIS 24143

Information and documentation — Information Governance — Concept and principles

ISO

В международном сообществе нет единого мнения о том, что же такое «стратегическое / полномасштабное управление информацией» (Information Governance, IG). Одни видят в этом не более чем новое название для доброй старой дисциплины управления документами, другие – «зонтичную» концепцию объединения усилий специалистов различных дисциплин с целью всестороннего управления всей информацией организации по единым принципам, а третьи – что-то ещё. Посмотрим, удастся ли новому стандарту ИСО внести какую-то ясность в этот вопрос... же, наоборот, запутать его ещё сильнее).

Во вводной части документа отмечается следующее:

«Информация является критически-важным активом, который абсолютно необходим для поддержки деловых процессов и, таким образом, служит фундаментом успеха любой деловой деятельности. Из-за многочисленных существующих и появляющихся форм и вариантов использования информации и из-за связанных с информацией рисков организации часто испытывают трудности с внедрением согласованных и всеобъемлющих систем для хранения, поиска, распространения и анализа информации. Идущая в настоящее время глобальная цифровая трансформация и общая эволюция общества всё больше требуют большей прозрачности, подотчетности, защиты

персональных данных, безопасности, интероперабельности и обмена информацией внутри и между организациями. Эта тенденция требует основательной стратегии стратегического управления информацией, которая поддерживает деловые процессы на стратегическом уровне. Существует потребность в более стратегическом видении, известном как «стратегическое управление информацией» (Information Governance), которое предстоит сыграть ключевую роль в поддержке инициатив цифровой трансформации. Многие государственные и неправительственные органы и организации во всём мире уже осознают необходимость и понимают преимущества координации на стратегическом уровне усилий множества дисциплин, связанных с информацией, данными и знаниями.

Настоящий международный стандарт определяет понятия и принципы стратегического управления информацией.

Данный международный стандарт предлагает членам органов стратегического управления организациями (в числе которых могут быть владельцы, директора, партнеры, руководители работ и т.д.) основные принципы для эффективного, продуктивного, соответствующего законодательно-нормативным и иным требованиям, безопасного, прозрачного и подотчетного создания, использования, хранения, обеспечения долговременной сохранности и уничтожения / передачи на архивное хранение информации в их организациях.

Стратегическое управление информацией является неотъемлемой частью общего стратегического управления организацией (governance). Оно определяет общие высокоуровневые принципы и обеспечивает рамки для эффективного и продуктивного сотрудничества всех специалистов информационных профессий в интересах поддержки миссии организации и достижения её стратегических целей. Области сотрудничества включают, но не ограничиваются следующими:

- Управление данными,
- Управление информацией,
- Управление документами,
- Управление знаниями,
- Обеспечение исполнения законодательно-нормативных требований,
- Электронная сохранность,
- Информационная безопасность,
- Корпоративная архитектура,
- Защита персональных данных,
- Открытые данные,
- Большие данные,
- Деловые процессы,
- Менеджмент качества.

Стратегическое управление информацией требует согласованности и интеграции с соответствующими стандартами систем менеджмента, такими, как стандарты серий ISO 9000, ISO 27000 и ISO 30300 (*это системы менеджмента качества, информационной безопасности и менеджмента*

документов соответственно. Подразумевается, что то же самое относится и ко всем прочим системам менеджмента ИСО, которые может использовать организация).

Стратегическое управление информацией - это стратегическая концепция (strategic framework) управления информационными активами в масштабе всей организации с целью поддержки достижения желаемых результатов её деловой деятельности и обеспечения уверенности в том, что риски для её информации и, следовательно, для возможности ведения ею оперативной деятельности и для целостности организации, адекватно определены и управляются. Стратегическое управление информацией включает в себя (но не ограничивается этим) определение и внедрение политик, процедур, ролей и мер контроля и управления для обеспечения исполнения законодательно-нормативных требований, менеджмента рисков и удовлетворения потребностей оперативной деятельности. Стратегическое управление информацией обеспечивает всеобъемлющую высокоуровневую концепцию, которая:

- Обеспечивает согласованность всей связанной с информацией деятельности с миссией и целями организации, а также с её деловыми, правовыми и общественными обязательствами;
- Обеспечивает всеобъемлющий и систематический подход к информации за счет интеграции управления документами и информацией, информационной безопасности и защиты персональных данных, обеспечения соответствия законодательно-нормативным требованиям, обеспечения непрерывности деловой деятельности и восстановления после катастроф, э-раскрытия и иных аспектов, относящихся к управлению и контролю над информацией;
- Поддерживает сотрудничество между представителями различных профессий; и
- Создаёт высокоуровневую основу для управления информацией вне зависимости от её формы, типа и формата; оказывает влияние на образование и повышение квалификации персонала и на осведомленность о связанных с информацией обязательствах, рисках и возможностях.»

Ключевое определение сформулировано следующим образом:

3.2.6. Стратегическое управление информацией (information governance) - стратегическая основа для стратегического управления информационными активами в масштабе всей организации с целью усиления скоординированной поддержки достижения результатов её деловой деятельности и обеспечения уверенности в том, что что риски для её информации и, следовательно, для возможности ведения ею оперативной деятельности и для целостности организации, адекватно определены и управляются.

Примечание 1: Стратегическое управление информацией включает в себя (но не ограничивается этим) определение и внедрение политик, процедур, ролей и мер контроля и управления для обеспечения исполнения

законодательно-нормативных требований, менеджмента рисков и удовлетворения потребностей оперативной деятельности.

Примечание 2: Данные являются частью информационного актива.

Содержание документа следующее:

Предисловие

Введение

1. Область применения

2. Нормативные ссылки

3. Термины и определения

4. Преимущества стратегического управления информацией

5. Принципы стратегического управления информацией

5.1. Признание информации стратегическим корпоративным активом

5.2. Реализация стратегического управления информацией на основе кооперации и сотрудничества

5.3. Проектирование стратегического управления информацией в качестве ключевого элемента корпоративной стратегии

5.4. Интеграция стратегического управления информацией в структуры стратегического управления организацией

5.5. Обеспечение лидерства и поддержки со стороны высшего руководства

5.6. Обеспечение поддержки в рамках стратегического управления информацией исполнения законодательно-нормативных требований и выполнения иных обязательных требований

5.7. Согласованность стратегического управления информацией с целями деловой деятельности

5.8. Обеспечение поддержки в рамках стратегического управления информацией информационной безопасности и защиты персональных данных

5.9. Обеспечение поддержки в рамках стратегического управления информацией качества и целостности информации

5.10. Способствование развития культуры сотрудничества и обмена знаниями

5.11. Внедрение подходов на основе менеджмента рисков

5.12. Повышение эффективности деятельности организации

5.13. Стратегическое управление информацией на протяжении всего её жизненного цикла

5.14. Поддержка корпоративной культуры

5.15. Поддержка жизнестойкости, устойчивого развития и экологической рациональности (sustainability)

Приложение А: Диаграммы взаимосвязи понятий

Библиография

ЕВРОСОЮЗ: ЕВРОПЕЙСКАЯ КОМИССИЯ СОБИРАЕТСЯ ОБЕСПЕЧИТЬ ДЛЯ ВСЕХ ЕВРОПЕЙЦЕВ НАДЕЖНЫЕ И БЕЗОПАСНЫЕ ЦИФРОВЫЕ ИДЕНТИФИКАЦИОННЫЕ ПРОФИЛИ (DIGITAL IDENTITY)

Источник: сайт Еврокомиссии
https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663

3 июня 2021 года Еврокомиссия предложила концепцию европейских цифровых идентификационных профилей (European Digital Identity, EDI), которые будут доступны всем гражданам Евросоюза, резидентам и деловым организациям в Евросоюзе. Граждане смогут подтверждать свою личность и обмениваться электронными документами из своих EDI-кошельков (wallets) одним нажатием кнопки на своем телефоне. Они смогут получить доступ к онлайн-сервисам с использованием своей национальной цифровой идентификации, которая будет признаваться во всей Европе. Очень крупные платформы будут обязаны поддерживать использование EDI-кошельков по запросу пользователя, например, для подтверждения своего возраста. Использование EDI-кошелька всегда будет по выбору пользователя.

По мнению исполнительного вице-президента организации «Европа, соответствующая цифровой эпохе» (Europe Fit for the Digital Age) Маргрет Вестагер (Margrethe Vestager), «Европейские цифровые идентификационные профили позволят нам в любом государстве-члене Евросоюза действовать так же, как дома, без каких-либо дополнительных затрат и при меньшем количестве препятствий - будь то аренда квартиры или открытие банковского счета за пределами собственной страны – и они позволят делать это безопасным и прозрачным способом, так что мы сами будем решать, каким объемом информации о себе мы хотим поделиться, с кем и с какой целью. Это уникальная возможность дань нам на практике ещё раз почувствовать, что значит жить в Европе и быть европейцем».

Еврокомиссар по внутреннему рынку Тьерри Бретон (Thierry Breton) отмечает: «Граждане Евросоюза ожидают не только высокого уровня безопасности, но и удобства, независимо от того, имеют ли они дело с национальными администрациями, например, при подаче налоговой декларации, или при поступлении в европейский университет, где им требуется официальное удостоверение личности. EDI-кошельки дают им новую возможность хранить и использовать данные для получения всех видов услуг, от регистрации в аэропорту до аренды автомобиля. Речь идет о предоставлении потребителям выбора, европейского выбора. Наши европейские компании, большие и малые, также получат выгоду от этой цифровой идентификации, поскольку они смогут предлагать широкий спектр новых услуг - ведь Еврокомиссия предлагает решение для предоставления безопасных и надежных услуг идентификации».

Европейская концепция цифровых идентификационных профилей

В соответствии с предлагаемым Регламентом (*в Евросоюзе Регламенты – это законы прямого действия*) государства-члены будут предлагать гражданам и коммерческим организациям цифровые кошельки, которые смогут связать их национальные цифровые идентификационные профили (digital identities) с подтверждениями других личных атрибутов (таких, например, как водительские права, дипломы, банковский счет). Эти кошельки могут быть предоставлены как государственными органами, так и частными организациями при условии, что они признаны государством-членом Евросоюза.

Новые EID-кошельки дадут всем европейцам возможность получать доступ к онлайн-сервисам без необходимости использовать частные методы идентификации и/или не делясь без необходимости персональными данными. С помощью этого решения они будут иметь полный контроль над теми данными, которыми они делятся.

Европейские цифровые идентификационные профили:

- **Будут доступны для всех, кто хочет их использовать:** Любой гражданин Евросоюза, любой резидент или коммерческая организация в Евроюзе, жедающие использовать европейскую цифровую идентификацию, смогут это сделать;

- **Будут широко использоваться:** EDI-кошельки будут широко использоваться как способ либо идентификации личности пользователей, либо подтверждения определенных персональных атрибутов, с целью доступа к государственным и частным электронным услугам в рамках всего Евросоюза;
- **Обеспечат пользователям контроль над своими данными:** EID-кошельки дадут людям возможность выбирать, какими атрибутами из своего идентификационного профиля, какими данными и сертификатами они будут делиться с третьими сторонами, и отслеживать такой обмен данными. Пользовательский контроль обеспечит то, что будет передана только та информация, которой необходимо поделиться.

Чтобы всё это стало реальностью как можно скорее, к предложению прилагается Рекомендация. Еврокомиссия предлагает государствам-членам Евросоюза к сентябрю 2022 года сформировать общий набор инструментов и немедленно начать необходимую подготовительную работу. Такой набор инструментов должен включать техническую архитектуру, стандарты и рекомендации по передовой практике.

Последующие шаги

Параллельно с процессом законотворчества, Еврокомиссия будет работать с государствами-членами Евросоюза и частным сектором над техническими аспектами европейских цифровых идентификационных профилей. В рамках программы «Цифровая Европа» (Digital Europe) Еврокомиссия будет поддерживать реализацию концепции европейских цифровых идентификационных профилей, и многие государства-члены Евросоюза уже предусмотрели включение проектов по внедрению решений электронного правительства, включая европейские цифровые идентификационные профили, в своих национальные планы в рамках Программы обеспечения жизнестойкости и восстановления после катастроф (Recovery and Resilience Facility, см.https://ec.europa.eu/info/business-economy-euro/recovery-coronavirus/recovery-and-resilience-facility_en).

Общая картина

В «Цифровом компасе» Еврокомиссии на период до 2030 года (2030 Digital Compass, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en) сформулирован ряд целей и этапов, в достижении которых помогут европейские цифровые идентификационные профили. Например, к 2030 году все ключевые государственные услуги должны быть доступны онлайн, все граждане должны будут иметь доступ к электронным медицинским документам; и 80% граждан должны будут использовать eID-решение для цифровой идентификации и аутентификации.

В рамках этой инициативы Еврокомиссия опирается на существующую трансграничную правовую базу для доверенных цифровых удостоверений личности - европейскую инициативу по электронной идентификации и услугам доверия (закон eIDAS). Этот закон, принятый в 2014 году, обеспечивает основу для трансграничной электронной идентификации, аутентификации и

сертификации веб-сайтов в Евросоюзе. Уже около 60% европейцев могут воспользоваться существующей системой.

Государства-члены Евросоюза, однако, не обязаны разрабатывать национальные цифровые удостоверения личности и обеспечивать их совместимость с цифровыми удостоверениями личности других государств-членов, что приводит к большим различиям между странами. Нынешнее предложение Еврокомиссии позволит устранить эти недостатки за счет повышения эффективности рамочной структуры и распространения её преимуществ на частный сектор и на среду мобильного использования.

Дополнительная информация:

- «Европейские цифровые идентификационные профили - вопросы и ответы» (European Digital Identity – Questions and Answers), https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_2664
- «Европейские цифровые идентификационные профили – Факты» (European Digital Identity – Facts Page)
- Европейский Регламент для цифровых идентификационных профилей (European Digital Identity Regulation) https://ec.europa.eu/newsroom/dae/redirection/item/712464/en
- «Рекомендации в отношении европейских цифровых идентификационных профилей» (European Digital Identity Recommendation)
- Веб-страница о законе eIDAS, https://digital-strategy.ec.europa.eu/en/policies/trust-services-and-eid
- Отчет об оценке закона eIDAS, https://ec.europa.eu/newsroom/dae/redirection/item/712467/en
- Пресс-релиз «Цифровое десятилетие», https://ec.europa.eu/commission/presscorner/detail/en/IP_21_983

ПРОШЛО ПЕРВОЕ ЗАСЕДАНИЕ НОВОГО ТЕХНИЧЕСКОГО КОМИТЕТА ТС 468 «УПРАВЛЕНИЕ И ОБЕСПЕЧЕНИЕ ДОЛГОВРЕМЕННОЙ СОХРАННОСТИ ЦИФРОВОГО КОНТЕНТА» ЕВРОПЕЙСКОГО КОМИТЕТА ПО СТАНДАРТИЗАЦИИ CEN

Источник: сайт LinkedIn
https://www.linkedin.com/feed/update/urn:li:activity:6808292049595465728

На своём первом заседании, проведенном 28 мая 2021 года, технический комитет CEN/TC 468 «Управление и обеспечение долговременной сохранности

цифрового контента» (Management and preservation of digital content) утвердил своё название и круг вопросов.

Название: «Обеспечение долговременной сохранности цифровой информации» (Preservation of digital information / Conservation de l'information numérique).

Круг вопросов:

Стандартизация функциональных и технических аспектов деятельности по обеспечению долговременной сохранности цифровой информации. В этой области комитет разработает структурированный набор стандартов, спецификаций и отчетов, отвечающих потребностям деловой деятельности, включая соответствие европейской законодательно-нормативной базе (например, законам GDPR и eIDAS), по следующим вопросам:

- Поддержание характеристик (таких, как целостность, аутентичность, надежность, пригодность к использованию и т.д.) цифровой информации на протяжении её жизненного цикла;
- Разработка, внедрение и управление процессами систем обеспечения долговременной сохранности (доступность, конфиденциальность и т.д.);
- Процедуры аудита и контроля качества в области обеспечения долговременной сохранности цифровой информации;
- Интероперабельность и обмен информацией между системами и сервисами;
- Процедуры и процессы, способствующие допустимости в качестве доказательств в суде.

Комитет не будет разрабатывать какие-либо документы, которые бы дублировали или заменяли опубликованные международные или европейские стандарты, разработанные, например, ISO/TC46, ISO/TC171, ISO/TC20/SC13 и ETSI. Технический комитет CEN/TC 468 будет поддерживать партнерские отношения с этими комитетами во избежание дублирования усилий в будущем.

Темы, попадающие в сферу деятельности комитета CEN/TC 457 «Электронная сохранность кинематографических произведений» (Digital preservation of cinematographic works) исключаются из сферы деятельности технического комитета CEN/TC 468.

НАД ЧЕМ СЕЙЧАС РАБОТАЕТ ЦЕЛЕВАЯ РАБОЧАЯ ГРУППА AHG2 «УНИЧТОЖЕНИЕ/ПЕРЕДАЧА ДОКУМЕНТОВ» ТЕХНИЧЕСКОГО ПОДКОМИТЕТА ИСО TC46/SC11

Источник: сайт IRMS https://irms.org.uk/news/565660/ Роджер Пул

TC46/SC11/AHG2 Международной организации по стандартизации (ИСО), занимается вопросами окончательного решения судьбы документов (уничтожения или передачи на архивное хранение - disposition) по истечении срока их хранения.

После пленарной встречи членов подкомитета TC46/SC11 «Управление документами» в ноябре 2020 года, группа AHG2 собиралась 7 раз. Группа занималась анализом пробелов в стандартизации по своему профилю, определением целевой аудитории и потенциальных заинтересованных сторон (я потратил на это более 18 часов!).

В рамках работы по анализу пробелов в стандартизации, группа AHG2 рассмотрела существующие рекомендации и руководства по вопросам уничтожения / передачи. Существует достаточно много материалов по данному вопросу, подготовленных национальными и местными органами государственной власти и Национальными Архивами различных стран мира. Эти документы содержат рекомендации / руководства / процедуры для реализации на практике положений нормативно-правовых документов, регламентирующих сроки хранения и действия по их истечении, а также для организации передачи имеющих непреходящую ценность документов на архивное хранение. Поскольку эти разнородные материалы были в массе своей подготовлены местными органами власти для решения их специфических проблем, в них имеются различия в терминологии и рекомендуемых процедурах. Естественно предположить, что не все государственные органы и учреждения по всему миру разработали свои руководства по уничтожению/передаче документов.

Предварительный анализ пробелов в стандартизации, проведенный группой AHG2, показал, что в настоящее время не существует единого стандарта, который мог бы использоваться в качестве основного различными заинтересованными сторонами. Группа AHG2 проанализировала существующие стандарты ИСО с точки зрения их актуальности для процессов уничтожения/передачи. Требования по уничтожению/передаче включены в несколько стандартов ИСО, в том числе ISO 15489 (*в России адаптирован как ГОСТ Р ИСО 15489-1:2019 «Система стандартов по информации, библиотечному и издательскому делу. Информация и документация. Управление документами. Часть 1. Понятия и принципы»,* http://protect.gost.ru/v.aspx?control=8&baseC=6&id=224713 .) и ISO 16175 «Информация и документация – Процессы и функциональные требования к программному обеспечению для управления документами» *см.*http://rusrim.blogspot.com/2020/10/iso-16175-1-ica-req.html). На основании результатов предварительного анализа пробелов стандартизации можно сказать, что имеющиеся стандарты ИСО не в полной мере решают задачу предоставления рекомендаций по вопросам уничтожения/передачи документов.

Исходя из наших выводов, на очередном пленарном заседании в мае 2021 года мы будем рекомендовать новый предварительный рабочий проект (preliminary work item, PWI) по разработке продукта, решающего проблемы, которые мы установили.

ШТАТ ВИКТОРИЯ, АВСТРАЛИЯ: ПРОЕКТ ПРОВЕДЕНИЯ ЭКСПЕРТИЗЫ ЦЕННОСТИ, УНИЧТОЖЕНИЯ/ПЕРЕДАЧИ НА АРХИВНОЕ ХРАНЕНИЕ И ОБЕСПЕЧЕНИЯ ДОЛГОВРЕМЕННОЙ СОХРАННОСТИ ЭЛЕКТРОННОЙ ПОЧТЫ

Источник: сайт PROV https://prov.vic.gov.au/recordkeeping-government/research-projects/email-appraisal-disposal-preservation-project

Я регулярно рассказываю об опыте Управления государственных документов австралийского штата Виктория (Public Record Office Victoria, PROV) по разработке нормативно-методической базы в сфере управления документами для государственных органов штата. Ниже приведен перевод материала, размещенного в соответствующем разделе веб-сайте Управления (последний раз обновлён в ноябре 2020 года).

Разработка решений для управления государственной электронной почтой в системе Lotus Notes: инициатива VERS

Предыстория

Электронная почта является жизненно важным элементом ведения деловой деятельности, и электронные письма признаются государственными документами в соответствии с Законом о государственных документах 1973 года (Public Records Act 1973). Электронная почта позволяет обмениваться идеями и принимать решения, а также поддерживает взаимодействие между всё более рассредоточенными сотрудниками. В государственной среде некоторые электронные письма также являются доказательствами, играющими ключевую роль для обеспечения подотчетности, и их следует сохранять во времени в качестве государственных документов.

С конца 1990-х годов правительство австралийского штата Виктория использовало почтовое приложение Lotus Notes в качестве основного средства обмена информацией как во внутренней работе, так и во внешнем общении. Ключевые действия и решения государственных служащих фиксируются в электронной переписке, которая является основным хранилищем документов правительства штата.

Учитывая проприетарный формат почтовых сообщений Lotus Notes и накопленные объемы хранения (хранение осуществляется онлайн и на LTO-лентах), доступ и извлечение электронных писем с целью анализа и в качестве свидетельств принятых решений может оказаться трудным, дорогостоящим и трудоёмким делом. Это означает, что ценность электронной переписки как источника информации не может быть в полной мере реализована.

Это ставит под угрозу репутацию правительства штата в плане обеспечения прозрачности и подотчётности, создает риски для текущей

деятельности по государственному управлению, а также потенциальный риск появления пробелов в документированной памяти штата Виктория.

О проекте

Управление государственных документов австралийского штата Виктория (Public Record Office Victoria, PROV) выполняет проект разработки и тестирования решений для надлежащего захвата, хранения, проведения экспертизы ценности и уничтожения/передачи на постоянное архивное хранение электронной почты, накоплений в системе Lotus Notes.

Проект выполняется в виде ряда описанных ниже этапов.

Этап 1: Проверка работоспособности концепции (Proof of Concept, PoC), 2017-2018 годы

На первом этапе Управление провела, совместно с компанией CenITex, проверку работоспособности концепции, с целью тестирования инструмента электронного раскрытия (eDiscovery – э-раскрытие) на выборке из 4,6 миллионов электронных писем из системы Lotus Notes, принадлежащих одному из министерств штата.

В рамках проверки концепции усилия были сосредоточены на результатах процесса уничтожения/передачи, и включали выполнение следующих задач:

- Проведение первоначальной количественной и качественной оценки тестового набора сообщений электронной почты;
- Выявление дубликатов в наборе данных (мы обнаружили, что **43% электронных писем были дубликатами**);
- Выявление в наборе данных малоценных документов, а также материалов, не являющихся государственными документами, посредством анализа доменных имен;
- Ручная проверка результатов с целью определения точности.

Для получения дополнительной информации, скачайте наш итоговый отчёт по первому этапу здесь:https://prov.vic.gov.au/sites/default/files/files/Blog/Government%20recordkeeping/Victoria%20Government%20Email%20Machine%20Assisted%20Appraisal%20Final.pdf

Этап 2: 2019-2020 годы

На втором этапе мы использовали коллекцию наших собственных электронных писем в системе Lotus Notes (это около 1,2 миллиона писем), и провели изучение методов для:

- Удаления дубликатов электронных писем (как и на этапе проверки концепции, мы обнаружили, что более 40% писем в выборке были дубликатами);
- Объединения писем в цепочки (threading) для сохранения проводимых с использованием электронной почты обсуждений, а также для уменьшения общего количества документов в электронной почте;
- Выявления не являющихся государственными документами писем с помощью анализа заголовков электронной почты и доменных имён;

- Преобразования электронной почты в инкапсулированные объекты VERS (VERS Encapsulated Objects, VEO – *это формат сдаточного информационного пакета, который ведомства обязаны использовать при передаче электронных документов на постоянное архивное хранение в Управление PROV*).

Ключевым результатом второго этапа стало подтверждение того, что используемый в Lotus Notes формат хранения - Lotus Notes Storage Format (NSF), не является жизнеспособным форматом для документов в электронной почте. Это означает, что с накопленной в Lotus Notes электронной перепиской органов правительства штата необходимо будет в ближайшее время что-то делать, прежде чем эти материалы не станут полностью морально устаревшими.

Для получения дополнительной информации, скачайте наш итоговый отчёт по второму этапу здесь: https://prov.vic.gov.au/sites/default/files/files/Govt%20Services%20General/Email-Stage2-Project-Summary-Report-2020.pdf .

РОССТАНДАРТ: КАК СТАНДАРТИЗАЦИЯ ПЕРЕРАСТАЕТ В ПРОФАНАЦИЮ

Источник: сайт Росстандарта
http://protect.gost.ru/default.aspx?control=6&month=5&year=2021

Кто не завидует Элону Маску, кому не хочется самому единым махом вывести полсотни спутников на орбиту – пусть даже основным результатом будет замусоривание ближнего космоса? Росстандарт в лучших традициях Эллочки Щукиной дал достойный ответ новоявленной американской Вандербильдихе – уж как сумел.

На сайте Росстандарта в майском 2021 года разделе (см.http://protect.gost.ru/default.aspx?control=6&month=5&year=2021) была выложена целая пачка стандартов на тему «Системная инженерия – Защита информации в процессе <*сюда впишите что придёт в голову*> [системы]»:

- ГОСТ Р 59329-2021 «Системная инженерия. Защита информации в процессах *приобретения и поставки продукции и услуг для* системы»
- ГОСТ Р 59330-2021 «Системная инженерия. Защита информации в процессе *управления моделью жизненного цикла* системы» (заметьте, в названии говорится об управлении моделью жизненного цикла, а не самим жизненным циклом!)
- ГОСТ Р 59331-2021 «Системная инженерия. Защита информации в процессе *управления инфраструктурой* системы»

- ГОСТ Р 59332-2021 «Системная инженерия. Защита информации в процессе *управления портфелем проектов*»
- ГОСТ Р 59334-2021 «Системная инженерия. Защита информации в процессе *управления качеством* системы»
- ГОСТ Р 59335-2021 «Системная инженерия. Защита информации в процессе *управления знаниями о* системе»
- ГОСТ Р 59336-2021 «Системная инженерия. Защита информации в процессе *планирования проекта*»
- ГОСТ Р 59337-2021 «Системная инженерия. Защита информации в процессе *оценки и контроля проекта*»
- ГОСТ Р 59338-2021 «Системная инженерия. Защита информации в процессе *управления решениями*»
- ГОСТ Р 59339-2021 «Системная инженерия. Защита информации в процессе *управления рисками для* системы»
- ГОСТ Р 59340-2021 «Системная инженерия. Защита информации в процессе *управления конфигурацией* системы»
- ГОСТ Р 59342-2021 «Системная инженерия. Защита информации в процессе *измерений* системы»
- ГОСТ Р 59344-2021 «Системная инженерия. Защита информации в процессе *анализа бизнеса или назначения* системы» (то есть, судя по названию, имеется некая система, что она делает – непонятно, так что будем её анализировать)
- ГОСТ Р 59345-2021 «Системная инженерия. Защита информации в процессе *определения потребностей и требований заинтересованной стороны для* системы»
- ГОСТ Р 59348-2021 «Системная инженерия. Защита информации в процессе *определения проекта*»
- ГОСТ Р 59350-2021 «Системная инженерия. Защита информации в процессе *реализации* системы»
- ГОСТ Р 59353-2021 «Системная инженерия. Защита информации в процессе *передачи* системы»
- ГОСТ Р 59354-2021 «Системная инженерия. Защита информации в процессе *аттестации* системы»
- ГОСТ Р 59355-2021 «Системная инженерия. Защита информации в процессе *функционирования* системы»
- ГОСТ Р 59357-2021 «Системная инженерия. Защита информации в процессе *изъятия и списания* системы»

Документы разработаны Федеральным исследовательским центром «Информатика и управление» Российской академии наук (ФГУ ФИЦ ИУ РАН), Государственным научно-исследовательским испытательным институтом проблем технической защиты информации Федеральной службы по техническому и экспортному контролю (ФАУ ГНИИИ ПТЗИ ФСТЭК России), Научно-техническим центром «Энергобезопасность» (ФБУ «НТЦ Энергобезопасность»), 4-м Центральный научно-исследовательским институтом Министерства обороны Российской Федерации (ФГБУ «4 ЦНИИ»

Минобороны России) и Научно-исследовательским институтом прикладной математики и сертификации» (ООО НИИПМС), под эгидой Технического комитета по стандартизации ТК022 «Информационные технологии» (не обижайтесь, если кого забыла!).

Объём этих шедевров научной мысли – от 28 до 46 страниц каждый, в совокупности порядка 600 страниц! И страшно даже подумать, сколько подобных стандартов можно ещё «настрогать»!

Между тем, не нужно быть узким специалистом, чтобы понимать – защита информации во всех этих случаях организуется более-менее по единым принципам, и различия носят столь специфический и детальный характер, что их можно было бы исчерпывающе описать в 1-2-страничной брошюре.

Думаю, немаловажно и то, что на разработку каждого стандарта выделяется пусть небольшая, но денежка из бюджета – и, как мудро отвечал Раскольников, когда его обвиняли в том, что он убил старушку за жалкие 10 копеек, - «Десять старушек - рубль!».

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ: БЕСПОКОЙСТВО О ПОСЛЕДСТВИЯХ «ВТОРОГО ПОРЯДКА»

Источник: блог компании Formtek https://formtek.com/blog/artificial-intelligence-the-worry-of-second-order-consequences/ Дик Вейсингер

Внедрение технологий искусственного интеллекта (ИИ) идёт очень быстро, и, хотя у ИИ есть много преимуществ, у него есть и обратная сторона потенциальных проблем, особенно в вопросах этики, злоупотребления ИИ и вторжения в частную жизнь.

В недавно опубликованном исследовании фирмы Gartner (https://www.techrepublic.com/article/gartner-the-future-of-ai-is-not-as-rosy-as-some-might-think/) предсказываются потенциально нежелательные «вторичные» последствия внедрения технологий искусственного интеллекта:

- К 2023 году в пятой части атак с использованием социальной инженерии (social engineering) будут применяться высокотехнологические фальшивки (дипфейки, deepfakes – *обычно создаваемые с использованием технологии ИИ*);
- К 2024 году 60% поставщиков программного обеспечения для искусственного интеллекта включат в своё программное обеспечение защитные меры для предотвращения злоупотреблений его возможностями;
- В 2025 году только 1% поставщиков будет использовать крупные предварительно обученные модели ИИ. Эти поставщики смогут контролировать то, как ИИ применяется;

- К 2025 году 75% разговоров на рабочем месте будет анализироваться с целью извлечения полезной для организации информации и оценки потенциальных рисков.

В ходе исследования, проведенное Вансоном Борном (Vanson Bourne) для компании SnapLogic (https://www.businesswire.com/news/home/20190326005362/en/The-AI-Ethics-Deficit-%E2%80%94-94-of-IT-Leaders-Call-for-More-Attention-to-Responsible-and-Ethical-AI-Development), выяснилось, что 89% ИТ-руководителей считают, что необходим централизованное регулирование и контроль применения ИИ, даже если такое регулирование замедлит темпы развития и эволюции ИИ.

Бывший декан Гарвардской школы бизнеса Нитин Нория (Nitin Nohria, https://www.hbs.edu/about/leadership/dean/Pages/default.aspx), и управляющий директор компании General Catalyst Хемант Танежа (Hemant Taneja, https://www.generalcatalyst.com/team/hemant-taneja/) пишут в статье для «Гарвардского делового обозрения» (Harvard Business Review), что «мы приветствовали появление трансформационных, «прорывных» компаний, но не указали на непреднамеренные сбои и преобразования, которые они могут вызвать. Результатом стало формирование компаний, присутствие которых в нашей жизни стало повсеместным, но также привело к целому ряду вредных непредвиденных последствий. Мы выступаем за новую этику инноваций, при которой возможные непредвиденные последствия тщательно рассматриваются с самого начала, и проводится их мониторинг во времени с целью их значительного смягчения. Мы считаем, что сможем добиться этого, если новаторы в области технологий будут создавать программные алгоритмы, способными могут послужить «канарейками», предупреждающими о нарождающихся вредных последствиях (*когда-то шахтёры использовали канареек, чтобы вовремя заметить появление опасных газов*), если предоставляющие капитал стороны будут настаивать на оценке и стратегическом управлении непредвиденными последствиями, а определяющие политику лица будут оценивают непредвиденные последствия в рамках обеспечения исполнения законодательно-нормативных требований. Это совершенно другая этика, другой менталитет, но их необходимо принять, если мы не хотим жить в мире антиутопии» (https://hbr.org/2021/01/managing-the-unintended-consequences-of-your-innovations).

ЗМІСТ