



## ПЕРЕДМОВА

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

У публікації «Европейский комитет по стандартизации CEN думает о создании технического комитета по управлению и обеспечению долговременной сохранности цифрового контента» повідомляється, що у відповідності до цінностей, принципів і правил електронного збереження Європейський комітет зі стандартизації CEN розглядає питання про створення нового технічного комітету «Управління та забезпечення довготривалого збереження цифрового контенту».

У публікації «ИСО: Подход к данным «по-крупному»» розповідається про набір з п'яти частин стандартів і технічних звітів серії ISO / IEC 20547 для вирішення проблем і використання можливостей, пов'язаних з великими даними.

У публікації «США: Национальный институт стандартов и технологий NIST опубликовал отчет NISTIR 8286 «Интеграция кибербезопасности и корпоративного менеджмента риска»» розповідається про те, як поліпшити ті відомості про ризики кібербезпеки, які вони надають в якості вхідних даних в ERM-процеси своєї корпорації за допомогою комунікацій і обміну інформацією про ризики.

У публікації «Вопросы, которые стоит задать на очередной веб-демонстрации для Вас продукта или услуги для управления документами» наведено перелік нагальних на сьогодні проблемних питань щодо продуктів та послуг електронного управління документами.

У публікації «Новый стратегический план Международного совета архивов «Расширение возможностей архивов и профессии, 2021-2024»» розповідається про основні засади плану які визначені на підставі опитувань, висновків фокус-груп та співбесід.

У публікації «США: Национальный институт стандартов и технологий опубликовал специальную публикацию NIST SP 800-209 «Рекомендации по безопасности для инфраструктуры хранения»» наведено всебічні рекомендації з безпеки для інфраструктур зберігання.

У публікації «Анализ перспектив: Компромиссное предложение в области электронной сохранности» розповідається про синтез взаємодоповнюючих підходів, який починається з використання об'єктів, але бере до уваги перспективи на майбутнє і розглядає забезпечення автентичності як найбільш важливу мету.

У публікації «Фінляндія: «Невидимая работа по управлению документами»» розповідається про дослідження роботи з управління документами у фінських муніципальних органах влади. Наведено висновки.

У публікації «Китай: Стандарты по вопросам управления документами и архивного дела» розповідається про стандарти які були опубліковані за останній час.


У публікації «Китай: Для публичного обсуждения опубликован проект национального закона о защите персональных данных» коротко викладаються деякі ключові положення проекту закону.

У публікації «Канада: Правительство Трюдо думает о создании национального центра рассекречивания исторических документов разведки» розповідається, що у Канади є багата історія в сфері національної безпеки, велика частина якої залишається невідомою через відсутність систематичного доступу до архівних документів.

У публікації «В рамках проекта E-ARK создана тематическая группа по архивации реляционных баз данных» розповідається, що зараз формується тематична група по архівації реляційних баз даних. Якщо Вас цікавить тема архівації баз даних, зареєструйтесь в групі. Як учасник групи, Ви будете отримувати останні новини та інформацію по темі архівації баз даних. Ви також зможете внести свій вклад в діяльність групи, ділячись своїм досвідом, допомагаючи управляти групою, підтримуючи розробку SIARD і CITS SIARD.

У публікації «Роботизированные документы: Масштабная автоматизация хранения бумажных документов» розповідається про нове сховище ФСБ США площею 256 тисяч квадратних футів (11,1 тисяч квадратних метрів) яке об'єднає документи з 56 окремих польових офісів. Операції в сховищі будуть виконувати понад 100 роботів, які використовують для управління документами «Автоматизовану систему зберігання і пошуку» (Automated Storage and Retrieval System). Площа створеної всередині сховища зони обслуговування буде приблизно відповідати двом футбольним полям.

У публікації «Италия: Обсуждаются предложения в отношении национальной стратегии в области технологий блокчейна и распределенных реестров» опубліковано резюме до розроблюваної національної стратегії в області технологій блокчейна і розподілених реєстрів. Наведено цілі та зміст документа.



# ЕВРОПЕЙСКИЙ КОМИТЕТ ПО СТАНДАРТИЗАЦИИ CEN ДУМАЕТ О СОЗДАНИИ ТЕХНИЧЕСКОГО КОМИТЕТА ПО УПРАВЛЕНИЮ И ОБЕСПЕЧЕНИЮ ДОЛГОВРЕМЕННОЙ СОХРАННОСТИ ЦИФРОВОГО КОНТЕНТА

Источник: [https://twitter.com/TAC\\_NISO/status/1320773333944836098](https://twitter.com/TAC_NISO/status/1320773333944836098)  
[http://wko.at/ooe/Branchen/Industrie/Zusendungen/C180\\_BT\\_N\\_12175%20Management%20and%20preservation%20of%20digital%20content.pdf](http://wko.at/ooe/Branchen/Industrie/Zusendungen/C180_BT_N_12175%20Management%20and%20preservation%20of%20digital%20content.pdf)



26 октября 2020 года директор американской Национальной организации по информационным стандартам (National Information Standards Organization, NISO) Тодд Карпентер поделился в Твиттере (см. [https://twitter.com/TAC\\_NISO/status/1320773333944836098](https://twitter.com/TAC_NISO/status/1320773333944836098)) новостью о том, что «с подачи» французского национального органа по стандартизации AFNOR Европейский комитет по стандартизации CEN рассматривает вопрос о создании нового технического комитета «Управление и обеспечению долговременной сохранности цифрового контента» (Management and preservation of digital content).

О комитете сказано следующее:

### **Цель и обоснование предложения**

Архивация электронного контента, под которой понимается обеспечение долговременной сохранности и управление электронными документами и данными, имеет большое значение для всех организаций, независимо от их характера.

Деятельность в области электронной сохранности позволяет организациям контролировать имеющийся у них контент, устанавливая надлежащий уровень конфиденциальности и соответствующие условия обеспечения сохранности (включая сроки хранения результатов обработки данных), а также сохраняя информацию о том, где этот контент физически находится. Это также позволяет им выявлять и защищать свою конфиденциальную и стратегическую информацию.

Начиная с создания контента, процесс обеспечения долговременной сохранности цифрового контента и управления им позволяет организациям

использовать такой контент по мере необходимости на протяжении всего его жизненного цикла. Во время, когда цифровому рынку требуется большее доверие, и когда информацию необходимо контролировать в соответствии с ценностями, принципами и правилами Евросоюза, обеспечение электронной сохранности имеет ключевое по важности значение.

Обеспечение долговременной сохранности охватывает все меры и средства, применяемые для хранения, защиты, восстановления, отслеживания, передачи и, в конечном итоге, окончательного решения судьбы и уничтожения заархивированного цифрового контента.

Таким образом, электронная архивация включает в себя все действия, инструменты и методы, реализованные для безопасного сбора, идентификации, отбора, классификации, обеспечения сохранности и уничтожения электронного контента, с целью его использования и обеспечения его доступности с течением времени, будь то в качестве доказательства или для справочных целей. Срок хранения зависит от ценности контента как доказательства, и чаще всего такие сроки устанавливаются среднесрочные или долгосрочные.

Интероперабельность - еще одна важная и необходимая особенность электронной сохранности. Различные технологические решения должны взаимодействовать друг с другом, используя протоколы обмена данными, с тем, чтобы обеспечить совместное использование и распространение данных. Интероперабельность также способствует возможности выбирать у пользователей и здоровой конкуренции между поставщиками.

Обеспечение электронной сохранности является частью более крупной экосистемы для обеспечения аутентичности доказательств. Сохраненный контент может считаться надежным и заслуживающим доверия при условии, что его невозможно изменить. В этой связи аутентичность является его наиболее важной характеристикой. Этого можно добиться с помощью ряда поддерживающих технологий, таких как хэш-функции, прослеживаемость доступа и др.

В число вспомогательных технологий входят технологии электронной подписи и управления электронными идентификационными профилями, связанные с которыми вопросы уже рассматриваются существующими техническими комитетами CEN и Европейского института телекоммуникационных стандартов ETSI. Очевидно, что предлагаемая новая работа будет зависеть от их усилий, поскольку процессы и технологии взаимодействуют друг с другом. Ожидается, что в дополнение к той отдаче, которую дают технологии, предлагаемая специальная работа над стандартами процессов обеспечения электронной сохранности обеспечит более высокий уровень доверия к электронным доказательствам и целостности контента в Европейском Союзе. Таким образом, новый комитет будет разрабатывать стандарты в иной, дополняющей плоскости, вследствие чего отсутствует риск дублирования деятельности технических комитетов, занимающихся собственно технологиями, - но имеется необходимость взаимодействия с ними.

Проблема нормативного регулирования в Евросоюзе - Сегодня данный сектор сталкивается с серьезными проблемами, связанными с исполнением законодательно-нормативных требований, с контролем рисков, связанных с защитой персональных данных и безопасностью, а также с обеспечением долговечности документального наследия и упрощением его использования.

На европейском уровне действуют два основных закона:

- «Общие правила защиты персональных данных» (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)), регламентирующие обеспечение неприкосновенности частной жизни и защиту персональных данных, а также свободное перемещение таких данных. Закон GDPR направлен в первую очередь на то, чтобы дать физическим лицам возможность контролировать их персональные данные, а также упростить и унифицировать нормативно-правовую среду для коммерческих организаций. Этот закон также регламентирует передачу персональных данных за пределы Евросоюза и Европейской экономической зоны.

- Закон «Об электронной идентификации и услугах доверия для электронных транзакций на внутреннем рынке, и об отмене Директивы 1999/93/EC» (Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC), известный также, как закон eIDAS. Этот закон регламентирует электронные подписи, электронные транзакции, вовлеченные в эту деятельность органы и их процессы, обеспечивая пользователям безопасный способ электронного ведения деловой деятельности, такой, как электронные переводы средств или электронное взаимодействие с государственными органами.

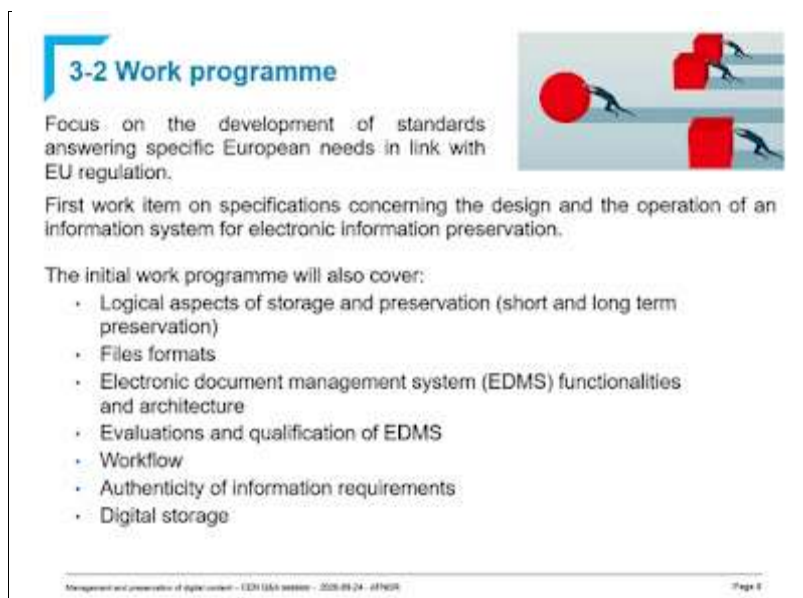
В идеале работу по стандартизации вопросов управления и обеспечения долговременной сохранности цифрового контента было бы желательно осуществлять в глобальном масштабе. Однако стало очевидно, что игроки на глобальной арене не поддерживают и не будут поддерживать разработку стандартов, соответствующим конкретным европейским ожиданиям, вытекающим из нормативно-правовой базы Евросоюза.

По этой причине работа по стандартизации в рамках CEN представляется ключевой по важности с точки зрения разработки набора стандартов, отвечающих требованиям названных законов и нормативных актов с точки зрения качества, безопасности, интероперабельности; а также с точки зрения обеспечения целостности и долговременной сохранности цифрового контента.

Технический комитет не будет заниматься стандартизацией технологий, а сосредоточит внимание исключительно на процессах. Это те процессы, которые необходимы для исполнения требований законодательства и обеспечения сохранности культурно-исторического наследия. Они будут определять, чего именно требовать в этом отношении от

технологий, как в государственных, так и в частных организациях. В этом отношении европейские страны действуют в очень специфической правовой среде, в частности, ввиду существования основополагающих законов Евросоюза GDPR и eIDAS, - что оправдывает начало такой работы на уровне CEN. Усилия нового технического комитета CEN дополняют работу, проделанную на международном уровне в технических комитетах ИСО TC171 и TC46.

28 октября 2020 года инициаторы создания нового технического комитета из французского органа по стандартизации AFNOR организовали открытый онлайн-вебинар, на котором представили эту идею. В вебинаре приняли участие около 40 специалистов, в том числе ряд экспертов ИСО – и, надо сказать, французам пришлось нелегко! Они так и не смогли убедительно объяснить, почему эту работу нельзя провести в рамках ИСО, и каким образом они собираются избежать ненужного дублирования усилий. Практически никто из участников вебинара вслух идею создания нового, чисто европейского комитета не одобрил.



**3-2 Work programme**

Focus: on the development of standards answering specific European needs in link with EU regulation.

First work item on specifications concerning the design and the operation of an information system for electronic information preservation.

The initial work programme will also cover:

- Logical aspects of storage and preservation (short and long term preservation)
- Files formats
- Electronic document management system (EDMS) functionalities and architecture
- Evaluations and qualification of EDMS
- Workflow
- Authenticity of information requirements
- Digital storage

Management and preservation of digital content - CEN ISA series - 2020-09-24 - AFNOR Page 5

**Представленный на вебинаре слайд с планом работ нового технического комитета. Его тематика включает вопросы организации хранения и долговременной сохранности, файловые форматы, функциональные возможности и архитектуру СЭД и их оценку, workflow-процессы, требования по аутентичности – в всё это есть в планах работы комитетов ИСО**

В современном глобальном мире большинству коммерческих организаций приходится учитывать требования законодательства своих торговых партнёров, поэтому в любом международном проекте требования GDPR и eIDAS всегда принимаются во внимание, равно как аналогичные требования иных ведущих стран.



## ИСО: ПОДХОД К ДАННЫМ «ПО-КРУПНОМУ»

Источник: сайт ИСО <https://www.iso.org/news/ref2578.html> Клер Нейден

Наш мир буквально тонет в данных - настолько, что их сбор, хранение, обработка и использование образуют отрасль, объём которой оценивается в 70,5 миллиардов долларов, и который, как ожидается, к 2027 году увеличится более чем втрое (<https://www.reportlinker.com/p0960361/Global-Big-Data-Industry.html>). Хотя в этом быстром росте нет ничего нового, спектр необходимых технологий постоянно меняется, и в некоторых случаях технологии не успевают за темпами роста, в результате чего возникают несоответствия и неупорядоченность, которые могут привести к появлению ненужных проблем.

Чтобы устранить все неясности и заложить стабильную основу для решения проблем и использования возможностей, связанных с большими данными, только что был опубликован всесторонний набор из ряда стандартов и технических отчетов. Состоящая из пяти частей серия ISO/IEC 20547 (<https://www.iso.org/advanced-search/x/title/status/P,U/docNumber/20547/docPartNo/docType/0/langCode/ics/currentStage/true/searchAbstract/true/stage/stageDateStart/stageDateEnd/committee/sdg>) описывает эталонную архитектуру больших данных (big data reference architecture, BDRA) и рамочную структуру, которые организации могут использовать для того, чтобы эффективно и последовательно описывать собственные архитектуры и их реализации.

При правильном использовании большие данные могут помочь организациям принимать важные стратегические решения, экономить время и ресурсы, а также лучше понимать тенденции рынка и потребности клиентов. С помощью больших данных можно получить ценные знания, приводящие к новым изобретениям и решениям в различных областях, таких, как борьба с заторами на дорогах, медицинская диагностика и лечение, безопасность пищевых продуктов и многое другое.

Ваэль Уильям Диаб (Wael William Diab), председатель одного из двух комитетов ИСО/МЭК, разработавших эти стандарты, отметил: «В основе четвертой промышленной революции лежит способность производить идеи и знания в условиях мира, который все больше ориентируется на данные. Вычислительные системы «больших данных» обеспечивают цифровую трансформацию в самых разных отраслях промышленности. Данные стандарты являются ответом на растущую потребность в большей ясности и последовательности концепций и процессов при обработке больших данных».

Во Чанг (Wo Chang), координатор рабочей группы WG2 «Большие данные», действующей в рамках технического подкомитета ИСО/МЭК JTC1/SC42 по искусственному интеллекту, подчеркнул, что документы серии ISO/IEC 20547 дополняют основополагающий стандарт терминологии

больших данных ISO/IEC 20546 и описывают всестороннюю эталонную архитектуру больших данных (BDRA).



По его словам, «В рамках BDRA рассматриваются требования, архитектура, вопросы безопасности и неприкосновенности частной жизни, варианты использования и соображениям, которые архитекторам, поставщикам приложений и принимающим решения лицам следует принять во внимание при развертывании системы больших данных. BDRA будет способствовать повышению доверия и взаимопонимания между заинтересованными сторонами и в масштабах всей отрасли, обеспечивая безопасное и эффективное использование технологий больших данных».

Серия документов ISO/IEC 20547 включает:

- Технический отчёт ISO/IEC TR 20547-1:2020 «Информационные технологии – Эталонная архитектура больших данных – **Часть 1: Концепция и процесс внедрения**» (Information technology - Big data reference architecture - Part 1: Framework and application process), см. <https://www.iso.org/standard/71275.html> и <https://www.iso.org/obp/ui#!/iso:std:71275:en>
- Технический отчёт ISO/IEC TR 20547-2:2018 «Информационные технологии – Эталонная архитектура больших данных – **Часть 2: Варианты использования и производные требования**» (Information technology - Big data reference architecture - Part 2: Use cases and derived requirements), см. <https://www.iso.org/standard/71276.html> и <https://www.iso.org/obp/ui#!/iso:std:71276:en>.
- Стандарт ISO/IEC 20547-3:2020 «Информационные технологии – Эталонная архитектура больших данных – **Часть 3: Эталонная архитектура**» (Information technology - Big data reference architecture - Part 3: Reference architecture), см. <https://www.iso.org/standard/71277.html> и <https://www.iso.org/obp/ui#!/iso:std:71277:en>.



- Стандарт ISO/IEC 20547-4:2020 «Информационные технологии – Эталонная архитектура больших данных – **Часть 4: Безопасность и неприкосновенность частной жизни**» (Information technology - Big data reference architecture - Part 4: Security and privacy), см. <https://www.iso.org/standard/71278.html> и <https://www.iso.org/obp/ui#!/iso:std:71278:en>.

- Технический отчёт ISO/IEC TR 20547-5:2018 «Информационные технологии – Эталонная архитектура больших данных – **Часть 5: Обзор относящихся к «большим данным» стандартов**» (Information technology - Big data reference architecture - Part 5: Standards roadmap), см. <https://www.iso.org/standard/72826.html> и <https://www.iso.org/obp/ui#!/iso:std:72826:en>.

Части 1- 3 и 5 серии ISO/IEC 20547 были разработаны техническим подкомитетом SC42, «Искусственный интеллект», а часть 4 – техническим комитетом SC 27 «Информационная безопасность, кибербезопасность и защита неприкосновенности частной жизни», поддержку работы секретариатов которых обеспечивают, соответственно, члены ИСО - американский орган по стандартизации ANSI и немецкий орган по стандартизации DIN. Оба подкомитета работают под эгидой Объединенного технического комитета ИСО/МЭК JTC1 «Информационные технологии».

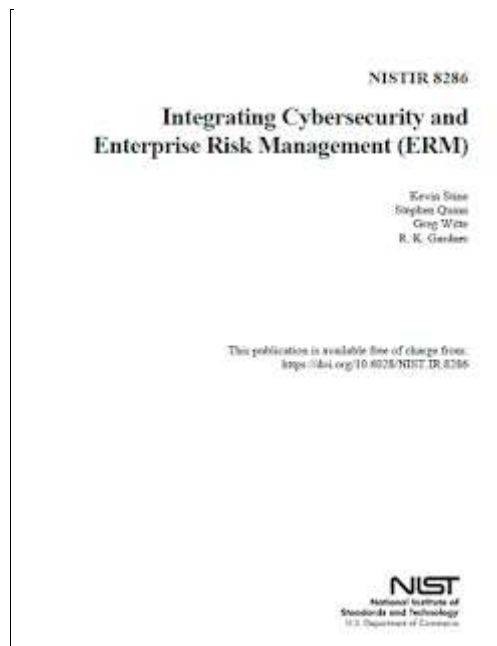
Документы серии ISO/IEC 20547 можно приобрести через национальные органы по стандартизации - члены ИСО, либо в интернет-магазинах ИСО и МЭК.



## **США: НАЦИОНАЛЬНЫЙ ИНСТИТУТ СТАНДАРТОВ И ТЕХНОЛОГИЙ NIST ОПУБЛИКОВАЛ ОТЧЁТ NISTIR 8286 «ИНТЕГРАЦИЯ КИБЕРБЕЗОПАСНОСТИ И КОРПОРАТИВНОГО МЕНЕДЖМЕНТА РИСКА»**

Источник: сайт NIST <https://csrc.nist.gov/publications/detail/nistir/8286/final>

В октябре 2020 года сайт американского Национального института стандартов и технологий сообщил о публикации отчёта **NISTIR 8286 «Интеграция кибербезопасности и корпоративного менеджмента риска»** (Integrating Cybersecurity and Enterprise Risk Management (ERM)) объёмом 74 страницы, см. <https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf>



В аннотации на документ отмечается:

«Растущая частота, изобретательность и серьезность последствий атак кибербезопасности означает, что все корпорации должны обеспечить, чтобы рискам кибербезопасности уделялось должное внимание в рамках их корпоративных программ управления менеджмента риска (enterprise risk management, ERM).

Настоящий документ предназначен для того, чтобы помочь отдельным организациям в рамках корпорации улучшить те сведения о рисках кибербезопасности, которые они предоставляют в качестве входных данных в ERM-процессы своей корпорации посредством коммуникаций и обмена информацией о рисках.

Поступая таким образом, корпорации и входящие в их состав организации смогут лучше выявлять, оценивать и управлять своими рисками кибербезопасности в контексте выполнения ими своей миссии и достижения деловых целей.

Уделяя основное внимание использованию регистров рисков для определения рисков кибербезопасности, данный документ объясняет ценность «поднятия» мер в отношении тех рисков, с которыми обычно борются на более низких уровнях системы / отдельной организации, на более высокий уровень корпорации.»

Содержание документа следующее:

Резюме для руководства

1. Введение
2. Пробелы в менеджменте рисков кибербезопасности как исходная информация для корпоративного менеджмента риска
3. Соображения, связанные с рисками кибербезопасности, на протяжении процесса корпоративного менеджмента риска
4. Менеджмент рисков кибербезопасности как часть «портфельной» точки зрения (Portfolio View)

Литература  
Приложение А: Сокращения  
Приложение В: Глоссарий  
Приложение С: Федеральные государственные источники по вопросам выявления рисков



## **ВОПРОСЫ, КОТОРЫЕ СТОИТ ЗАДАТЬ НА ОЧЕРЕДНОЙ ВЕБ-ДЕМОНСТРАЦИИ ДЛЯ ВАС ПРОДУКТА ИЛИ УСЛУГИ ДЛЯ УПРАВЛЕНИЯ ДОКУМЕНТАМИ**

Источник: блог «Управление документами следующего поколения» (Next Generation Records Management) <https://nextgenrm.com/2020/04/30/questions-for-your-next-records-management-product-or-service-demonstration-webcast/> Дон Людерс

Карантин, введенный из-за пандемии коронавируса, дал мне возможность посмотреть несколько веб-трансляций, посвященных новым продуктам и услугам для управления документами. Все эти презентации были довольно неплохими и давали достаточное количество полезной информации. В моей карьере был период, когда я сам проводил такие же веб-трансляции, так что я знаю, насколько сложно бывает их организовать, поэтому отдаю дань уважения всем ведущим этих трансляций, которых я видел за последние пару месяцев.

Тем не менее, для меня было разочарованием видеть, что все презентации, которые я посмотрел, сводились к очень узкому (и безопасному для докладчика) набору функциональных требований к управлению документами, - и ни в одной из них не было попыток затронуть действительно сложные проблемы, с которыми современные специалисты в области управления документами сталкиваются в реальном мире.

Все это заставило меня задуматься о том, были ли докладчики просто не в курсе этих проблем (что вполне возможно, учитывая, что все презентации проводились представителями служб продаж, а не специалистами по управлению документами), - или же они знали о проблемах, но не знали, с какой стороны подойти к ним, поскольку у них нет для них реального решения.

Как бы то ни было, мне пришла в голову мысль, что как для поставщиков продуктов и услуг, так и для их потенциальных клиентов было бы полезно, если бы я предложил им список связанных с этими проблемами

вопросов, в надежде, что ответы на них могут со временем появиться в некоторых будущих презентациях.

Итак, вот мой список вопросов (приведенных в произвольном порядке). Каждый слушатель веб-презентации по продуктам и услугам электронного управления документами должен подумать о том, чтобы задать их, и каждый докладчик должен быть готов на них ответить:

- **Невозможность внесения изменений в электронный контент (immutability)** – Как Ваш продукт / услуга обеспечивает целостность электронных документов в целях представления их в качестве доказательств? Как гарантируется отсутствие внесения в документ каких-либо изменений?

- **Долговременное хранение** – некоторые документы «временного» срока хранения требуют хранения в течение 50 или даже 100 лет. Как Ваше решение решает проблему устаревания программного и аппаратного обеспечения?

- **Уничтожение, после которого восстановление информации невозможно даже средствами компьютерной криминалистики** - Простое нажатие кнопки «Удалить» при работе с документом на деле не удаляет документ из места хранения, а лишь делает это место доступным для записи в более позднее время. Каким образом Ваш продукт / услуга обеспечивает, что документ не может быть восстановлен после того, как он был уничтожен на этапе окончательного решения судьбы документов (т.е. уничтожения или передачи на архивное хранение)?

- **Единый источник истины** - Электронные документы размножаются с ошеломляющей скоростью. Многочисленные версии распространяются в сообщениях электронной почты, плодятся на общих дисках, на ноутбуках и флеш-накопителях и даже остаются в памяти сетевых принтеров. Каким образом Ваш продукт / услуга обеспечивает, что конкретный документ является «единственным источником истины»?

- **Структурированная информация** - Все больше и больше документов, обычно создаваемых типичной организацией, трансформируются от неструктурированных форматов в структурированную информацию в базе данных. Однако требования к срокам хранения и уничтожению информации, содержащейся в этих структурированных документах, остаются такими же, какими они были тогда, когда эта информация была представлена в неструктурированном виде. Каким образом Ваш продукт / услуга обеспечивает применение соответствующего требованиям законодательства управления жизненным циклом информации к структурированным документам?

- **Активная и неактивная («спящая») информация** - Точно так же, как перемещение бумажных документов из шкафов для документов в подразделениях в защищенный центр хранения документов в тот момент, когда их статус меняется с «активного» на «неактивный», значительно повышает безопасность неэлектронных документов, - перемещение неактивных электронных документов в автономные или подключаемые к сети по требованию системы хранения существенно улучшает стратегию

кибербезопасности организации. Поддерживает ли Ваш продукт / услуга миграцию неактивных электронных документов из их исходного местоположения в автономные или подключаемые к сети по требованию системы хранения/носители информации для целей долгосрочного хранения? Если да, то каким образом?

- **Условные сроки хранения и запускающие их отсчёт события-триггеры** - Каким образом Ваш продукт / услуга фиксирует уникальные события-триггеры, от которых отсчитываются условные сроки хранения документов? Можно ли ими эффективно управлять при большом их количестве?

- **Искусственный интеллект и машинное обучение** – Согласно общепринятому мнению, в условиях продолжающегося экспоненциального роста объёмов вновь создаваемой информации, искусственный интеллект (в частности, машинное обучение) станут необходимыми компонентами большинства корпоративных решений для управления документами. Использует ли Ваш продукт / услуга в настоящее время искусственный интеллект для поддержки управления жизненным циклом информации? Если нет, есть ли у Вас план внедрения ИИ в Ваш продукт / решение?

- **Удобство использования / освоение пользователями** - Учитывая, что управление документами - это горизонтальное направление деятельности, которое требуется в любой организации, предполагается, что Вы сами в своей компании используете разработанный Вами продукт / услугу. Можете ли вы продемонстрировать, как Ваша компания использует Ваш собственный продукт / услугу для эффективного управления жизненным циклом Вашей корпоративной информации?



## **НОВЫЙ СТРАТЕГИЧЕСКИЙ ПЛАН МЕЖДУНАРОДНОГО СОВЕТА АРХИВОВ «РАСШИРЕНИЕ ВОЗМОЖНОСТЕЙ АРХИВОВ И ПРОФЕССИИ, 2021-2024»**

Источник: сайт МСА <https://www.ica.org/en/empowering-archives-and-the-profession-2021-2024-ica-s-new-strategic-plan>

[https://www.ica.org/sites/default/files/ga\\_2020-7a\\_strategic\\_review\\_.pdf](https://www.ica.org/sites/default/files/ga_2020-7a_strategic_review_.pdf)

Международный совет архивов (МСА) рад сообщить, что его новый стратегический план был одобрен на первой виртуальной ежегодной Генеральной ассамблее, проведенной в 16 ноября 2020 года.

Данный план отражает взгляды и мнения, высказанные во время кампании «МСА силами своих членов, для своих членов» (ICA by its

members, for its members), и в нём представлены предложения, полученные от членов МСА в масштабе всей ассоциации. Мы благодарны за вклад, который члены МСА внесли посредством участия в опросах, фокус-группах и беседах, тем самым помогая руководству МСА в разработке этого стратегического плана.

План построен на трех основных принципах: «Общение и сотрудничество» (Networked and Collaborative), «Прозрачность, подотчётность и инклюзивность» (Transparent, Accountable and Inclusive) и «Расширение возможностей МСА, помощь в расширении возможностей членов МСА и актуальность» (Empowered, Empowering and Relevant).

На вебинаре более подробно будут представлены итоги кампании «МСА силами своих членов, для своих членов», а также будет рассказано о том, как формировалась стратегия «Расширение возможностей архивов и профессии, 2021-2024», а также о реформах устройства МСА, которые мы проводим для того, чтобы начать согласование деятельности МСА с амбициями, изложенными в стратегическом плане. Присоединяйтесь к нам!



Ниже приведен стратегический обзор, в котором более детально изложены цели в рамках каждого принципа. Мы надеемся, что Вы найдёте время, чтобы прочитать его и поделиться с нами своим мнением в ходе вебинара либо по адресу [ica@ica.org](mailto:ica@ica.org).

Мы ещё раз благодарим всех наших членов за их усилия и потрясающую работу! МСА не смог бы существовать без Вас и Вашего вклада.

В присоединённом к новости документе (см. [https://www.ica.org/sites/default/files/ga\\_2020-7a\\_strategic\\_review\\_.pdf](https://www.ica.org/sites/default/files/ga_2020-7a_strategic_review_.pdf)), представляющим собой инфографику, новый стратегический план МСА описан следующим образом:

«Архивы, наряду с архивистами и специалистами по управлению документами, абсолютно необходимы для хорошего управления, обеспечения подотчетности, прозрачности и сохранению культуры. Международному совету архивов как международному органу, представляющему интересы архивно-документоведческой профессии на международном уровне, необходимо расширять возможности сети своих

членов посредством (1) сотрудничества, (2) большей прозрачности, подотчетности и инклюзивности своей деятельности, а также (3) своей актуальности.

Основываясь на результатах проведенной в 2019 году кампании «МСА силами своих членов, для своих членов», стратегия МСА «Расширение возможностей архивов и профессии, 2021-2024» отражает отзывы и данные, полученные от членов ассоциации посредством проведения опросов, фокус-групп и собеседований.

**1. Общение и сотрудничество** – МСА будет укреплять сеть своих членов, способствуя более тесному сотрудничеству и активно участвуя в таком сотрудничестве. МСА:

1.1. Упростит и сделает более согласованными свои внутренние процессы, способствуя обмену информацией и сотрудничеству между своими членами;

1.2. Предоставит более удобные платформы для обмена информацией и механизмы для взаимодействия и сотрудничества;

1.3. Обеспечит более тесное взаимодействие между администрацией МСА и отделениями ассоциации, облегчая взаимодействие между отделениями и секциями;

1.4. Обеспечит взаимодействие между администрацией МСА и секциями ассоциации, облегчая взаимодействие между отделениями и секциями;

1.5. Улучшит процессы оперативной деятельности для облегчения своевременного и эффективного взаимодействия между членами и администрацией МСА;

1.6. Будут более четко проработаны возможности волонтерской деятельности и обязательства волонтеров; МСА обеспечит должное признание вклада своих волонтеров.

**2. Прозрачность, подотчётность и инклюзивность** – МСА станет более прозрачной, подотчетной, эффективной и инклюзивной организацией. МСА:

2.1. Обеспечит более эффективное, действенное и прозрачное стратегическое управление;

2.2. Понизит сложность организации своей деятельности;

2.3. Будет более прозрачным в вопросах назначения своих членов на посты в управляющих комитетах или органах управления МСА;

2.4. Будет более прозрачным в финансовых вопросах, и будет лучше информировать о том, как расходуются членские взносы;

2.5. Станет более разнообразным и инклюзивным, особенно в плане представительства профессий и географических регионов;

2.6. Разработает более стабильную финансовую модель, превратившись в организацию, опирающуюся на взносы основной массы своих членов (*в отличие от текущего положения, когда 80% средств поступает от немногочисленных национальных архивных служб*) и предлагающую своим членам более интересные для них услуги.

**3. Расширение возможностей МСА, помощь в расширении возможностей членов МСА и актуальность** – МСА постарается быть полезным и тесно взаимодействовать со своими членами, лучше продвигая и пропагандируя деятельность архивов, управление документами и профессию в целом. МСА:

3.1. Построит более прочные взаимосвязи и наладит партнерские отношения с родственными профессиями;

3.2. Стремится к развитию и укреплению партнерских отношений со специалистами и организациями за пределами круга наших традиционных союзников (например, с представителями наук о данных и компьютерных наук);

3.3. Лучше отразит в своем подходе и деятельности цепочку добавленной стоимости информации, от создания до доступа;

3.4. Обратит особое внимание на сквозные международные профессиональные потребности и факторы, такие как нарождающиеся технологии, экологически устойчивое развитие и изменение климата;

3.5. Будет развивать и расширять предлагаемые им возможности для повышения профессиональной квалификации, дополняя и поддерживая уже существующие возможности;

3.6. Будет отстаивать интересы архивов и специалистов (в области архивного дела, управления документами и информацией) на ключевых международных форумах».



## **США: НАЦИОНАЛЬНЫЙ ИНСТИТУТ СТАНДАРТОВ И ТЕХНОЛОГИЙ ОПУБЛИКОВАЛ СПЕЦИАЛЬНУЮ ПУБЛИКАЦИЮ NIST SP 800-209 «РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ ДЛЯ ИНФРАСТРУКТУРЫ ХРАНЕНИЯ»**

Источник: сайт NIST <https://csrc.nist.gov/publications/detail/sp/800-209/final>  
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-209.pdf>

Американский Национальный институт стандартов и технологий (National Institute of Standards and Technology, NIST) в октябре 2020 года опубликовал новую специальную публикацию **NIST SP 800-209 «Рекомендации по безопасности для инфраструктуры хранения»** (Security Guidelines for Storage Infrastructure) объёмом 79 страниц, см. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-209.pdf>



В аннотации на документ отмечается:

«Инфраструктура хранения, наряду с вычислительной (включая ОС и аппаратное обеспечение сервера) и сетевой инфраструктурами, является одним из трех основных столпов информационных технологий (ИТ). Однако, по сравнению с двумя другими инфраструктурами, ей уделяется сравнительно ограниченное внимание, когда дело касается вопросов безопасности, несмотря на то, что компрометация данных может иметь такие же негативные последствия для организации, как и нарушения безопасности в вычислительной и сетевой инфраструктурах.



Чтобы восполнить этот пробел, NIST выпускает специальную публикацию SP 800-209 «Рекомендации по безопасности для инфраструктуры хранения», в которой содержатся всесторонние рекомендации по безопасности для инфраструктур хранения. В число рассматриваемых в этом документе основных вопросов безопасности входят не только те, что являются общими для ИТ-инфраструктуры в целом – такие, как физическая безопасность, аутентификация и авторизация, управление изменениями, контроль конфигурации, реагирование на инциденты и восстановление после них, - но также и те, что являются специфическими для инфраструктуры хранения, в том числе защита данных, изоляция данных, обеспечение уверенности в возможности восстановления и шифрование данных.

Технологии хранения, как и вычислительные и сетевые технологии, эволюционировали от традиционных типов услуг хранения, таких как хранение блоков, файлов и объектов. В частности, эволюция шла в двух направлениях: в первом случае, по пути увеличения ёмкости носителей информации (таких, как ленты, жесткие диски, твердотельные накопители (SSD)), а во втором – в плане развития архитектур, от непосредственно подключаемых систем хранения (direct-attached storage, DAS) к размещения

ресурсов хранения в сетях, доступ к которым осуществляется через различные интерфейсы и протоколы, - и далее к облачным ресурсам хранения, обеспечивающим абстрагирование от программного обеспечения для всех форм используемых «за кадром» технологий хранения.

Эволюция архитектуры сопровождается увеличением сложности управления, вследствие чего увеличивается вероятность ошибок конфигурации и усиливаются связанные с ними угрозы безопасности.

В настоящем документе дан обзор эволюции ландшафта технологий хранения, текущих угроз безопасности и связанных с ними рисков.

Настоящий документ нацелен на то, чтобы предложить всесторонний набор рекомендаций по безопасности, направленных на устранение этих угроз.»

Содержание документа следующее:

Резюме для руководства

1. Введение

2. Технологии хранения данных: Базовые сведения

3. Угрозы, риски и поверхности атаки (attack surfaces)

4. Руководство по безопасности для развертываемых решений для хранения данных

5. Итоги и выводы

Литература

Приложение А: Сокращения



## **АНАЛИЗ ПЕРСПЕКТИВ: КОМПРОМИССНОЕ ПРЕДЛОЖЕНИЕ В ОБЛАСТИ ЭЛЕКТРОННОЙ СОХРАННОСТИ**

Источник: сайт Hypotheses <https://archive20.hypotheses.org/9912>

Автор: Кай Науман

С открытыми архивами я ассоциирую открытую культуру, в том числе в плане дальнейшего развития технических процедур и процессов; а также максимальную сдержанность при отделении своих убеждений от убеждений моих коллег. Выделение собственных идей полезно лишь в том случае, если оно не только служит для профилирования человека или учреждения, но также и увеличивает нашу продуктивность и нашу общую полезность.

На этом фоне мне хотелось бы остановиться на двух недавних публикациях и предложить определенный компромисс. Речь идет о следующих статьях:

- Михаэль Пухта (Michael Puchta), «Свойства, существенные для «неизвестного целевого сообщества»» (Signifikante Eigenschaften für eine „Unknown Community“), журнал Archivar («Архивист»), том 73 (2020) выпуск 3, стр. 259-268, <https://www.archive.nrw.de/landesarchiv-nrw/wir-ueber-uns/der-archivar> (прямая ссылка на PDF-файл: [https://www.archive.nrw.de/sites/default/files/media/files/Archivar\\_2020-3-Internet.pdf](https://www.archive.nrw.de/sites/default/files/media/files/Archivar_2020-3-Internet.pdf)).

В данной публикации содержится ценный обзор литературы, который очень помогает в документировании текущего состояния дискуссии по данному вопросу в Германии и за рубежом, и приводятся весьма подробные и убедительные аргументы.

- Андреас Ромейке (Andreas Romeyke) в своей дискуссионной статье «Существенные свойства долговременного архива Саксонской государственной и университетской библиотеки» (Signifikante Eigenschaften im SLUB Langzeitarchiv), вышедшей в 2020 году, см. <https://slubarchiv.slub-dresden.de/technische-standards-fuer-die-ablieferung-von-digitalen-dokumenten/> (прямая ссылка на PDF-файл: [https://slubarchiv.slub-dresden.de/fileadmin/groups/slubsite/slubarchiv/SLUBArchiv\\_Diskussionspapier\\_Signifikante\\_Eigenschaften\\_v1.0.pdf](https://slubarchiv.slub-dresden.de/fileadmin/groups/slubsite/slubarchiv/SLUBArchiv_Diskussionspapier_Signifikante_Eigenschaften_v1.0.pdf)), какой-либо библиографии не приводит, но его подход заслуживает подражания: вынести ключевые вопросы на обсуждение до того, как Саксонская государственная и университетская библиотека (Sächsische Landes- und Universitätsbibliothek, SLUB) опубликует окончательную версию своих технических стандартов передачи на хранение электронных документов.

В своих публикациях авторы обсуждают два разных методологических подхода к обеспечению электронной сохранности. Соответственно, имеет большое значение, из чьих интересов исходить при выборе мер по обеспечению сохранности объектов определенного класса: из интересов создателей объектов - назовем это ретроспективным методом (Rückschaumethode); или же из интересов вероятных будущих пользователей – это т.н. прогностический метод (Vorschaumethode). Ретроспективный метод, согласно идеологии его сторонников, обеспечивает только аутентичное восприятие пользователем (Nutzungserlebnisses, англ. user experience – *впечатления от использования*) и не связывает себя с какими-либо сценариями использования – что смотрится весьма скромно на фоне тех безмерных возможностей, которые будут в распоряжении будущих пользователей. Методологи прогностического метода придают большое значение свободе действий будущих пользователей, и стремятся предложить для этой свободы наилучшие концептуальные рамки.

Однако прогностический метод, судя по всему, не всегда способен на многое в краткосрочной перспективе; он, как писал Бенджамин Буссманн (Benjamin Bussmann) в 2015 году, является «менее пригодным на практике». На мой взгляд, однако, в долгосрочной перспективе этот подход больше соответствует потребностям и ожиданиям людей, чем ретроспективный метод – мы, например, уже не используем перья и чернильные авторучки, и

лишь изредка пишем от руки, и у нас вызвало бы раздражение, если бы нам пришлось изучать дела 1950-х годов с использованием инфраструктуры 1950-х годов. Нам нравится современная инфраструктура с её инструментами распознавания текста и решениями типа Citavi и им подобными. Конечно, было бы неприятно, если бы дела мы могли бы получить только в оцифрованном виде, а их оригиналы исчезли бы - но пока вопрос об этом не стоит.

Ретроспективный метод, как объясняет Михаэль Пухта, обеспечивает большее доверие к документам, чем прогностический метод. В частности, он указывает на интересы соответствующих государственных органов, которые его работодатель - государственное архивное управление, должен учитывать в первую очередь. Но давайте посмотрим на данный вопрос повнимательнее: даже судебная система, а также многие другие органы государственного управления в Германии временами используют прогностический метод, когда проводят замещающее сканирование бумажных дел и объявляют полученные электронные копии «источником истины» для следующего поколения судей и прокуроров. Некоторые свойства при этом теряются, другие добавляются. По словам Михаэля Пухта, «определимые (исторические) научные и правовые факты», которые, по его мнению, как раз определяют существенные свойства, в этом случае будут уже не точными, а скорее неоднозначными.

Даже в случае с электронными делами, когда мы подробно расспрашиваем лиц, ответственных за ведение электронных дел в органах власти и судах, то выясняется, что не всё там так хорошо, как нам хотелось бы. Электронные дела, как утверждается в некоторых концепциях, представляют собой простые наборы документов в формате А4, которые должны быть понятны только в контексте специализированных процедур. Если мы, архивисты, не станем думать о будущих пользователях, то будем собирать и складировать массивы документов, по определению являющихся подлинными электронными делами, но не имеющими достаточной индексирующей информации. Мы получим эту информацию только в том случае, если сможем получить метаданные из вторичных источников, а именно из специализированных процедур. Мы используем такую информацию для формирования нового электронного объекта, дополняя сдаточный информационный SIP-пакет А ещё одним сдаточным SIP-пакетом В для формирования архивного информационного АIP-пакета С. Это не является чем-то предосудительным, если только происхождение этой новой архивной единицы хранения С четко задокументировано.

Теперь о статье Саксонской государственной и университетской библиотеки (SLUB): Андреас Ромейке задал серию вопросов в отношении каждого из методов. При использовании ретроспективного метода следует узнать: 1) об авторе, 2) о его намерениях, 3) о природе объектов и их связи с намерениями автора, с тем, чтобы в конечном итоге выделить существенные свойства. Однако при использовании прогностического метода важно:

- 1) классифицировать объект, отнеся его к определенному типу информации;
- 2) объединить схожие типы информации в классы;
- 3) определить целевые группы пользователей;
- 4) для этих групп установить цели использования;
- 5) установить существенные свойства для соответствующего класса.

Можно действовать именно таким образом. Тем не менее, представляется, что лучше избегать строгой последовательности шагов при определении существенных свойств, и вообще не проводить различие между вопросами, характерными для ретроспективного и прогностического методов. Лучше действовать подобно инженеру, который должен спроектировать мост в труднопроходимой местности: а именно, задокументировать ситуацию в целом во всех измерениях, взвесить обстоятельства, свериться со стандартами и, наконец, строить. В одном случае происхождение объекта будет для меня решающим (например, электронное дело), в других – это будут будущие возможности использования в своей деловой деятельности (например, данные из ГИС-системы), в третьи случае – определяющим фактором будут затраты (например, хранение 2 петабайт материалов медиа-арта). Или же придётся учитывать комбинацию этих факторов.

С моей личной точки зрения, дискуссии о «единственно правильном методе» и четких границах не приносят пользы ни для одного из направлений деятельности архива, потому что «правильный метод» представляет собой синтез взаимно-дополняющих подходов, который, естественно, прагматично начинается с известного использования объектов, но принимает во внимание перспективы на будущее и рассматривает обеспечение аутентичности как наиболее важную цель. Когда я оцениваю историческую ценность класса объектов и планирую их приём-передачу, я помню об имеющихся свойствах. Вместе с моими коллегами я быстро обсуждаю вопрос о том, является ли этот класс объектов достаточно перспективным, и улучшаю эти свойства, но, конечно же, таким образом, чтобы объекты оставались «полностью понятными» (говоря словами Михаэля Пухта). Я также могу посмотреть, можно ли обеспечить сохранение соответствующих свойств в архиве с финансовой точки зрения. В итоге получается ретроспективный метод с проверкой «на перспективу». Что Вы об этом думаете?

Приведу пример из архивной практики. В 2010 году архив земли Баден-Вюртемберг принял на хранение списки военных захоронений 1950-х годов, которые больше не были нужны Региональному совету Штутгарта. Мы получили а) электронные копии, и, через полтора года, б) бумажную версию. Мы заметили, что электронные копии в некоторых деталях отличались от бумажных документов. Мы решили принять отсканированные образы в качестве второго представления бумажных оригиналов, но с учетом соответствующих отклонений в объектах (пример см. здесь: <http://www.landesarchiv-bw.de/plink/?f=2-2967055> ). Можно было также

создать две серии объектов с взаимными ссылками. В 2015 году мы смогли объявить о завершении создания базы данных на основе этих списков. Метаданные, ввод которых обошёлся недорого благодаря использованию краудсорсинга, были интегрированы в состав существующих метаданных системы каталогов. Юридически значимыми остаются списки жертв войны в бумажной форме, но возможности для исследователей существенно расширились благодаря онлайн-доступности сканированных образов и базы



**Рис.1 Начиная с левого верхнего угла, по часовой стрелке: Адекватность/соразмерность, Аутентичность, Финансово-экономическая реализуемость, Возможность автоматизации.**

**Источник: Christian Keitel, AUdS 2017, Basel, Folie 10**

Идея синтеза, о котором я говорю, наглядно показана на рис.1. Эта диаграмма была представлена Христианом Кейтелем (Christian Keitel) на конференции AUdS (Archivierung von Unterlagen aus digitalen Systemen) в Базеле в 2017 году. Перед нами, архивистами, ставятся различные, порой противоречивые цели, и мы ищем верный путь, стараясь не проявлять «излишней интерпретации» (о которой в ряде случаев предупреждает Пухта). Заслуживающие сохранения свойства можно определить только в контексте конкретных вариантов использования. Такого рода синтез в настоящее время на практике лучше всего реализован в баварском проекте, направленном на то, чтобы доступ к цифровым объектам всегда был в соответствующем контексте в плане существенных свойств. Однако я надеюсь, что данный проект иногда будет отходить от жёсткой фиксации на контексте, в котором документы были созданы, и, например, будет принимать во внимание интересы будущих пользователей и финансовые возможности.

Работа над созданием модуля обеспечения сохранности DIMAG, в которой я сейчас участвую, и обзор международных разработок («Реестры действий по обеспечению долговременной сохранности» - Preservation Action Registries, <https://parcore.org/>; сайт Библиотеки Конгресса США «Цифровые форматы» - Digital Formats,

<https://www.loc.gov/preservation/digital/formats/intro/intro.shtml> ; «Концепция планирования долговременной сохранности» Национальных Архивов США - Preservation Planning Framework (<https://github.com/usnationalarchives/digital-preservation>) позволяют мне надеяться, что теоретические дискуссии скоро выльются в живой разговор о возможностях и оценке наилучших вариантов реализации электронной сохранности.

Тем временем, параллельно с теоретическими рассуждениями, несколько миллионов файлов были произведены в процессах сканирования в неверно выбранном формате, и некоторые новички снова задавали своему начальству замечательные вопросы о форматах, не получая чёткого ответа. С моей точки зрения, главное в электронной архивации - это гармонизация хорошей концепции с эффективными производственными операциями. Именно в этом заключается реальная отдача от исторических наук.



## **ФИНЛЯНДИЯ: «НЕВИДИМАЯ РАБОТА ПО УПРАВЛЕНИЮ ДОКУМЕНТАМИ»**

Источник: сайт JournalTOCs / сайт ScienceDirect  
<http://www.journaltoCs.ac.uk/index.php?action=tocs&journalID=4977>  
<https://www.sciencedirect.com/science/article/abs/pii/S0740624X1930317X?amp=1>



12 марта 2020 года сайт выходящего в издательстве Elsevier ежеквартального журнала «Государственная информация» (Government Information Quarterly) сообщил об онлайн-публикации статьи финских специалистов Туйи Каутто (Tuija Kautto – проектировщик решений для управления документами и информацией из финского органа социального страхования Kansaneläkelaitos); и Пекки Хентонена (Pekka Henttonen - профессор факультета ИКТ университета города Тампере) на тему **«Управление документами как невидимая работа: Опыт финских муниципальных органов власти»** (Records management as invisible work: A study of Finnish municipalities), см. <https://doi.org/10.1016/j.giq.2020.101460>

**Основные результаты:**

- Специалисты по управлению документами в финских муниципалитетах «невидимы»;
- Профессия управления документами в финских муниципальных органах власти сильно фрагментирована, и ею занимаются преимущественно женщины;
- Работа по управлению документами также выполняется в рамках неформальных структур временным персоналом.

#### **Аннотация**

Документы являются стратегическими инструментами электронного правительства, используемыми для информационного взаимодействия между государственными органами и гражданами и для укрепления доверия между ними.

Специалисты по управлению документами несут ответственность за повседневную практику управления документами в организации. Быстрое развитие технологий изменило статус специалистов по управлению документами и отодвинуло их на второй план, в то время как на первый план вышли другие профессиональные группы, такие как ИТ-специалисты.

В данном исследовании изучалась «видимость» деятельности по управлению документами и соответствующих специалистов в финских муниципальных органах. Данные были собраны с помощью полуструктурированных интервью и анкетирования. В качестве инструмента анализа использовалась теоретическая концепция невидимой работы.

Полученные данные показывают, что управление документами и соответствующие специалисты в финских муниципальных органах «невидимы», исходя из анализа факторов, которые, как показали предыдущие исследования, связаны с невидимой работой.

Профессия управления документами в финских муниципальных органах сильно фрагментирована, ею занимаются преимущественно женщины, и иногда такая работа выполняется в рамках неформальных структурах временным персоналом.

Связь этих факторов с «невидимой» работой и особенно их влияние на управление документами в органах и организациях государственного сектора ранее не привлекала особого внимания исследователей. Следовательно, для продвижения заслуживающего доверия электронного правительства необходимы в будущем дополнительные исследования, в рамках которых будет изучена «видимость» деятельности по управлению документами и соответствующих специалистов в различных органах и организациях государственного сектора.



# КИТАЙ: СТАНДАРТЫ ПО ВОПРОСАМ УПРАВЛЕНИЯ ДОКУМЕНТАМИ И АРХИВНОГО ДЕЛА

Источники: <http://www.naa.gov.cn/> сайт Госархива КНР / портал китайского органа по стандартизации

В Китае стандарты по вопросам управления документами и архивного дела, согласно национальной классификации, относятся к группе A14 «Библиотеки, архивы, документы и интеллектуальная деятельность», [http://www.csres.com/sort/Chtype/A14\\_1.html](http://www.csres.com/sort/Chtype/A14_1.html) . По международной классификации эти стандарты попадают в раздел 01.140.20 «Информатика», см. [http://www.csres.com/sort/ics/01.140.20\\_1.html](http://www.csres.com/sort/ics/01.140.20_1.html) .

За последнее время были опубликованы следующие документы:

**DA/T 68.1-2020 «Требования в отношении передачи на аутсорсинг работ, выполняемых архивно-документационной службой - Часть 1: Общие правила»** ( 档案服务外包工作规范 第1部分：总则, название на английском языке: Specifications on the work of archives service outsourcing - Part1: General rules) объёмом 19 страниц, опубликован 18 мая 2020 года, вступил в силу 1 июня 2020 года, см. <http://www.csres.com/detail/345210.html> и <https://www.doc88.com/p-37139707210342.html> .



**DA/T 68.2-2020 «Требования в отношении передачи на аутсорсинг работ, выполняемых архивно-документационной службой - Часть 2: Услуги по оцифровке документов»** (档案服务外包工作规范 第2部分：档案数字化服务, название на английском языке: Specifications on

the work of archives service outsourcing - Part2: Archives digitization service) объёмом 9 страниц, опубликован 18 мая 2020 года, вступил в силу 1 июня 2020 года, см. <http://www.csres.com/detail/345211.html> и <https://www.doc88.com/p-89516909428097.html>.

**ДА/Т 68.3-2020 «Требования в отношении передачи на аутсорсинг работ, выполняемых архивно-документационной службой - Часть 3: Консультационные услуги по вопросам управления документами и архивного дела» (档案服务外包工作规范 第3部分：档案管理咨询服务, название на английском языке: Specifications on the work of archives service outsourcing - Part 3: Archives management consulting service) объёмом 9 страниц, опубликован 18 мая 2020 года, вступил в силу 1 июня 2020 года, см. <http://www.csres.com/detail/345212.html> и <https://www.doc88.com/p-30987010523108.html>.**



## **КИТАЙ: ДЛЯ ПУБЛИЧНОГО ОБСУЖДЕНИЯ ОПУБЛИКОВАН ПРОЕКТ НАЦИОНАЛЬНОГО ЗАКОНА О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ**

Источник: издание «Национальное правовое обозрение» (National Law Review) <https://www.natlawreview.com/article/china-issues-draft-personal-information-protection-law>

21 октября 2020 года в Китайской народной республике (КНР) для общественного обсуждения был опубликован проект Закона о защите персональных данных (中华人民共和国个人信息保护法(草案), см. [https://www.dataguidance.com/sites/default/files/china\\_draft\\_personal\\_data\\_law.pdf](https://www.dataguidance.com/sites/default/files/china_draft_personal_data_law.pdf), в статье используется англоязычная аббревиатура PIPL от Personal Information Protection Law). Это событие предвещает введение в Китае всесторонней системы защиты персональных данных.

Закон Китая о кибербезопасности (中华人民共和国网络安全法, см. [http://www.csrc.gov.cn/pub/newsite/flb/flfg/flx zsf/201805/t20180518\\_338285.html](http://www.csrc.gov.cn/pub/newsite/flb/flfg/flx zsf/201805/t20180518_338285.html)), проект Закона о безопасности данных (中华人民共和国数据安全法(草案), см. <https://npcobserver.files.wordpress.com/2020/07/data-security-law-draft.pdf>) и проект Закона о защите персональных данных образуют триаду основных законов о кибербезопасности и защите данных. Проект Закона о персональных данных содержит положения, касающиеся проблемных вопросов, связанных с новыми технологиями и приложениями, - при этом некоторые вопросы оставлены открытыми, и они

получат свое отражение либо в будущем законодательстве, либо в необязательных руководствах.

Проект закона состоит из восьми глав и 70 статей, охватывающих такие темы, как:

- обработка персональных данных;
- трансграничная передача персональных данных;
- права субъектов данных в отношении обработки их персональных данных;
- обязанности обработчиков данных;
- уполномоченный орган по вопросам защиты персональных данных;
- гражданско-правовая ответственность.

中华人民共和国个人信息保护法(草案)	
目 录	
第一章	总 则
第二章	个人信息处理规则
第一节	一般规定
第二节	敏感个人信息的处理规则
第三节	国家机关处理个人信息的特别规定
第三章	个人信息跨境提供的规则
第四章	个人在个人信息处理活动中的权利
第五章	个人信息处理者的义务
第六章	履行个人信息保护职责的部门
第七章	法律责任
第八章	附 则

Под персональными данными понимаются различные типы информации, записанной в электронных или иных форматах, и относящейся к идентифицированным и идентифицируемым физическим лицам. Определение охватывает как информацию, которая может использоваться для идентификации субъектов данных, так и информацию, относящуюся к субъектам данных.

Ниже кратко излагаются некоторые ключевые положения проекта закона:

### **Государственные органы, ответственные за защиту персональных данных**

В число органов, ответственных за защиту персональных данных, входят Администрация киберпространства Китая (国家互联网信息办公室), соответствующий департамент Государственного Совета и соответствующие департаменты местных и региональных органов власти, начиная с уровня округа и выше.

## **Область применения**

Закон будет применяться за пределами Китая в той мере, в какой это необходимо для защиты интересов субъектов данных в Китае. В случаях, когда целью обработки персональных данных за пределами Китая является предоставление продуктов или оказание услуг лицам на территории Китая, или же анализ и оценка поведения людей, находящихся в Китае, - такая деятельность по обработке данных будут регламентироваться данным законом.

Кроме того, обработчики данных, находящиеся за пределами Китая, но подпадающие под действие данного закона, должны создавать структуры или назначать уполномоченных лиц, ответственных за защиту персональных данных. Сведения о такой структуре или имя и контактная информация уполномоченного лица должны быть сообщены в соответствующий уполномоченный государственный орган Китая.

Закон не будет применяться в отношении физического лица, обрабатывающему собственные персональные данные или персональные данные членов семьи.

## **Семь принципов обработки данных**

Проект закона о персональных данных предусматривает семь принципов защиты персональных данных, среди которых законность, явно установленная цель обработки, обработка минимально необходимых данных, прозрачность, точность, подотчетность и безопасность данных. Это первый случай, когда точность упоминается в контексте обработки персональных данных.

## **Согласие на обработку и исключения из требования о получении согласия**

Согласно проекту закона, обработка персональных данных не ограничивается только теми случаями, когда получено согласие (как это предусмотрено Законом о кибербезопасности). В соответствии с Законом о защите персональных данных, обработчик данных может обрабатывать персональные данные на основании:

- согласия субъекта персональных данных;
- в связи с необходимостью заключения или исполнения контракта;
- в связи с необходимостью исполнения требования законодательства или установленной законодательством обязанности;
- при реагировании на чрезвычайную ситуацию в сфере общественного здравоохранения или в случае необходимости обеспечить безопасность жизни и имущества человека; либо
- при публикации новостей; и при надзоре, в разумных пределах и в интересах общества, со стороны общественного мнения.

Обработчик данных не должен отказывать в предоставлении продуктов или услуг на том основании, что физическое лицо не дает согласия на обработку своих персональных данных или отзывает своё согласие, - за

исключением случаев, когда обработка персональных данных абсолютно необходима для предоставления продуктов или услуг.

### **Совместная обработка данных и обработка данных по доверенности**

Если несколько обработчиков данных обрабатывают персональные данные совместно, то все они несут солидарную ответственность в случаях нарушения личных интересов.

Если обработчик данных поручает обработку персональных данных третьей стороне, то эти стороны обязаны заключить соглашение, в котором устанавливается цель обработки персональных данных, способ обработки, типы обрабатываемых персональных данных, меры защиты, а также права и обязанности обеих сторон. В подобных случаях обработчик данных должен контролировать деятельность по обработке персональных данных. В проекте закона конкретные методы надзора не указаны. После завершения исполнения договора или прекращения обработки по доверенности, персональные данные подлежат возврату или удалению.

### **Предоставление персональных данных третьей стороне**

При предоставлении персональных данных третьей стороне, обработчик данных обязан сообщить субъекту данных название и контактную информацию третьей стороны, цель обработки данных, способ обработки и тип охватываемых обработкой персональных данных, а также получить отдельные согласие субъекта персональных данных.

### **Автоматическое принятие решений**

Что касается автоматического принятия решений, обработчики данных обязаны обеспечивать прозрачность принятия решений и справедливость результата. В случае, если субъекты персональных данных считают, что автоматическое принятие решений оказывает существенное негативное влияние на их интересы, они имеют право запросить у обработчика данных объяснения, и субъект персональных данных может отказать обработчику данных в праве принимать решения в его отношении исключительно с использованием автоматических средств. Если обработчик данных применяет автоматическое принятие решений в целях проведения маркетинговых и рассылки пуш-сообщений, то субъект персональных данных вправе запретить обработчику данных обработку такого рода, нацеленные на личные характеристики человека.

### **Специальные (чувствительные) персональные данные**

Проект закона предусматривает дополнительные ограничения на обработку специальных (высокочувствительных) персональных данных. К этой категории относится информация, которая вследствие утечки или злоупотребления ею может нанести ущерб личной репутации или поставить под серьезную угрозу личную безопасность и безопасность имущества. К специальным данным относятся сведения о расе, национальности, религии, биометрическая информация, сведения о здоровье, о финансовых счетах, о местонахождении человека, а также иная информация. Обработка специальных персональных данных разрешается только в том случае, если

обработчик персональных данных ставит конкретную цель обработки, необходимость которой достаточно обоснована, и получает отдельное согласие или письменное согласие от субъектов персональных данных.

Обработчик данных обязан информировать субъекта данных о необходимости проведения обработки специальных персональных данных и о последствиях такой обработки для субъекта данных.

### **Изображение человека, полученное оборудованием, установленным в общественных местах**

Изображение человека и персональные данные, собранные с помощью установленного в публичном месте устройства для фиксации изображений и идентификации лиц, могут быть использованы только в целях поддержания общественной безопасности, и не могут быть раскрыты или предоставлены другим сторонам без согласия физического лица, - если только такое раскрытие/передача не разрешены законами или нормативными актами.

### **Раскрытые персональные данные**

Что касается раскрытых персональных данных, их обработка должна соответствовать тем целям, для которых они были раскрыты. В случаях обработки данных, выходящей за разумные рамки заявленной цели обработки, обработчики данных обязаны проинформировать субъектов данных и получить их согласие до начала обработки.

Если в момент раскрытия персональных данных цель их раскрытия была не ясна, обработчики данных обязаны обрабатывать персональные данные, проявляя разумность и осмотрительность. В случае, если обработка раскрытых персональных данных может оказать существенное негативное влияние на субъектов данных, обработчики данных обязаны проинформировать субъектов данных и получить их согласие.

### **Трансграничная передача персональных данных**

Проект закона предусматривает три метода трансграничной передачи персональных данных. Как правило, трансграничная передача персональных данных должна быть одобрена уполномоченными государственными органами, либо обработчик данных должен заключить соглашение о трансграничной передаче с их получателем, находящимся за пределами Китая, и обеспечить соответствие обработки стандарту защиты, предусмотренному в законе Китая о защите персональных данных. Если обработчик данных относится к категории оператора критической информационной инфраструктуры, или если объём обрабатываемых обработчиком данных превышает уровень, установленный Администрацией киберпространства Китая, то трансграничная передача персональных данных должна пройти оценку безопасности, проводимую Администрацией киберпространства Китая.

В случаях трансграничной передачи персональных данных обработчик данных должен сообщить субъектам данных имя/название и контактную информацию зарубежной принимающей стороны, цель обработки данных, способ обработки, тип обрабатываемых персональных данных и способ

реализации субъектами данных своих прав, предусмотренных данным законом, - а также получить отдельное согласие от субъектов данных.

Что касается трансграничной передачи персональных данных с целью оказания международной судебной и правоохранительной помощи органов, такая передача должна быть одобрена компетентным органом.

Согласно проекту закона, если юридическое или физическое лицо нарушает интересы китайских граждан в отношении персональных данных, или если какая-либо страна или регион принимают необоснованные меры в отношении Китая в вопросах, связанных с защитой персональных данных, то Администрацией киберпространства Китая вправе принять определенные контрмеры против такой страны или региона.

### **Локализация**

В дополнение к требованию одобрения трансграничной передачи персональных данных, применимому в отношении к операторам критической информационной инфраструктуры и обработчикам данных, которые обрабатывают данные, превышающие установленный объём, - эти обработчики данных обязаны хранить персональные данные в Китае.

### **Права субъектов данных в отношении обработки данных**

Субъекты данных имеют право знать, право принимать решения и право ограничивать либо возражать против обработки их персональных данных иными сторонами. Субъекты данных также имеют право на доступ и копирование своих персональных данных, находящихся в распоряжении обработчиков данных, и право требовать от обработчиков данных исправления или дополнения их персональных данных. При определенных обстоятельствах субъекты данных имеют право потребовать удаления своих персональных данных, право отозвать согласие и право потребовать, чтобы обработчик данных объяснил правила обработки.

Обработчик данных обязан реализовать механизм, позволяющий субъекту данных осуществлять свои права.

### **Обязанности обработчика данных**

В проекте закона отдельная глава посвящена обязанностям обработчиков данных в отношении обработки данных. Обязательства включают установление внутренних административных политик и оперативных процедур, обеспечение конфиденциальности и иерархического администрирования персональных данных, принятие разумных решений относительно разрешений на обработку данных, проведение регулярных тренингов и обучения, создание и выполнение планов действий в чрезвычайных ситуациях, принятие технических мер безопасности и проведение регулярных аудитов деятельности по обработке персональных данных.

### **Уполномоченное лицо по защите персональных данных**

Если объем обрабатываемых персональных данных достигает порога, установленного Администрацией киберпространства Китая, обработчик данных обязан назначить уполномоченное лицо по защите персональных данных, ответственное за обработку персональных данных. Имя и контактная

информация такого лица должны быть опубликованы и переданы в соответствующий уполномоченный орган государственной власти.

### **Предварительная оценка рисков**

Обработчик данных обязан заранее провести оценку рисков до начала обработки специальных персональных данных, трансграничной передачи персональных данных, автоматического принятия решений на основе персональных данных, передачи персональных данных на обработку третьей стороне, предоставления персональных данных третьей стороне и раскрытия персональных данных. Отчет об оценке и условиях уничтожения данных должен храниться в течение трех лет.

### **Утечки данных**

В случае утечки данных обработчик данных обязан немедленно принять меры по исправлению положения и уведомить соответствующий уполномоченный орган и субъектов данных. В проекте закона регламентировано, какие сведения должны быть включены в уведомление. Тем не менее, предусмотрено одно исключение из требования об уведомлении субъектов данных. Если принятые обработчиком данных меры позволяют избежать ущерба, который мог быть нанесён ввиду раскрытия персональных данных, то обработчик данных не обязан уведомлять субъектов данных, если только уполномоченный государственный орган не определит, что раскрытие всё-таки может причинить ущерб.

### **Гражданско-правовая ответственность**

Проект закона расширяет диапазон наказаний помимо тех, что предусмотрены Законом о кибербезопасности. Помимо исправления недостатков, конфискации незаконных доходов, предупреждений, штрафов до 1 миллиона юаней, приостановки деловой деятельности, приостановки деятельности для исправления недостатков и отзыва соответствующих разрешений или лицензий в соответствии с Законом о кибербезопасности, - проект данного закона также предусматривает, что в серьезных случаях на обработчиков данных могут быть наложены штрафы в размере до 50 миллионов юаней или до 5% от выручки за предыдущий год.



## **КАНАДА: ПРАВИТЕЛЬСТВО ТРЮДО ДУМАЕТ О СОЗДАНИИ НАЦИОНАЛЬНОГО ЦЕНТРА РАССЕКРЕЧИВАНИЯ ИСТОРИЧЕСКИХ ДОКУМЕНТОВ РАЗВЕДКИ**

Источник: сайт Kamloops <https://www.kamloopsthisweek.com/trudeau-government-eyes-national-declassification-centre-for-historical-spy-documents-1.24231263> Автор: Джим Бронскилл



Как следует из недавно опубликованного меморандума, правительство Трюдо ищет способы раскрыть для общественности заброшенные канадские хранилища документов, относящихся к национальной безопасности, - возможно, путем создания центра для рассекречивания исторических документов.

Однако заставить канадские федеральные министерства ведомства раскрыть большие объёмы секретных документов «будет непросто без всеобъемлющей политики и ресурсов», - говорится во внутренней записке, подготовленной ранее в этом году для заместителя министра государственной безопасности Канады.

Агентство «Канадская пресса» получила копию этого меморандума на основании Закона о доступе к государственной информации (Access to Information Act).

В документе отмечается, что у ключевых союзников Канады в области разведывательной деятельности имеются политика и практики, которые позволяют им рассекречивать исторические документы по безопасности и делать их доступными для общественности через национальные архивы, президентские библиотеки или академические учреждения.

В меморандуме говорится, что отсутствие в Канаде такого стандартизированного подхода к разведывательным материалам создает «проблему управления информацией» в масштабе всего правительства.

В настоящее время основным инструментом обеспечения публичного доступа к документам по безопасности являются запросы, подаваемые в соответствии с Законом о доступе к государственной информации.

Однако, как сообщила федеральный уполномоченный по информации (federal information commissioner), выполняющая функции омбудсмана для пользователей этого закона, в прошлом году почти 20% жалоб в её управление были связаны с документами, относящимися к национальной безопасности.

Профессор истории Университета Торонто Тимоти Эндрюс Сэйл (Timothy Andrews Sayle) ждёт ответа на запросы о открытии доступа к документам, касающихся разведанных 1940-х годов, которые в некоторых случаях старше 75 лет.

Сэйл говорит, что было бы неумно позволить кому-либо из его студентов выбрать связанную с разведкой тему для курсовой работы или диссертации. «Документы могут поступить через семь, восемь или девять лет после запроса, если они вообще когда-нибудь придут».

Как отметил эксперт по разведывательной деятельности Уэсли Уорк в подготовленном в этом году дискуссионном документе для федерального уполномоченного по информации, у Канады имеется богатая история в сфере национальной безопасности имеющая важное значение, большая часть которой остаётся неизвестной из-за отсутствия систематического доступа к архивным документам.

В результате этого канадская литература по вопросам национальной безопасности и разведки «серьезно отстает» от аналогичной литературы

основных стран-союзников, пишет Уорк, работающий приглашенным профессором на кафедре государственных и международных отношений Оттавского университета.

В меморандуме министерства государственной безопасности сообщается, что с конца 2018 года правительство разрабатывает концепцию рассекречивания документов, относящихся к национальной безопасности и разведке, которая призвана обеспечить последовательный подход к раскрытию документов.

Пресс-секретарь министерства государственной безопасности Зара Малик сообщила, что министерство вместе с другими федеральными органами исполнительной власти занимается окончательной доработкой концепции, но «в настоящее время не может предоставить её копию, поскольку концепция всё ещё находится на стадии разработки и консультаций».

В меморандуме для заместителя министра говорится, что федеральные должностные лица также ищут долгосрочные политические решения, которые могут включать внесение поправок в законодательство, бюджетные запросы на ресурсы или же создание национального центра рассекречивания.

По словам Уорка, меморандум обнадеживает, однако в нём не указаны конкретные действия и сроки. По его словам, без доступа к документам, касающимся национальной безопасности и разведки, у Канады просто нет основанной на доказательствах истории деятельности в области безопасности.

В результате важный инструмент для совершенствования деятельности канадских органов исполнительной власти и для «повышения осведомленности канадцев о практике, значении и проблемах национальной безопасности теряется», - добавляет Уорк.

Сэйл, которого в прошлом году пригласили представить свои идеи по этому вопросу министерству государственной безопасности, сказал, что он умеренно оптимистичен в отношении того, что политика или концепция рассекречивания позволят опубликовать полезные материалы и улучшить текущую ситуацию.

«Думаю, что хуже не станет. Но станет ли лучше? К сожалению, у меня не очень большая надежда на это», - отметил он. «Когда дело доходит до раскрытия информации, у нас есть законодательная база, которая позволяет это сделать. У нас нет недостатка в правилах и политиках, - но у нашего правительства нет политической воли поделиться своей историей».



## В РАМКАХ ПРОЕКТА E-ARK СОЗДАНА ТЕМАТИЧЕСКАЯ ГРУППА ПО АРХИВАЦИИ РЕЛЯЦИОННЫХ БАЗ ДАННЫХ

Источник: сайт Фонда «Открытая сохранность» (Open Preservation Foundation, OPF) <https://openpreservation.org/news/e-ark-establishes-a-relational-database-archiving-interest-group>

Реляционные базы данных широко используются для сбора и управления данными. Часто эти данные имеют долгосрочную ценность, и их необходимо регулярно архивировать. На сегодняшний день стандартом де-факто для архивации реляционных баз данных является формат SIARD (Software Independent Archiving of Relational Databases – «программно-независимое архивное хранение реляционных баз данных»). Это формат разработанный для упрощения архивации реляционных баз данных Федеральным архивом Швейцарии (Schweizerische Bundesarchiv, BAR).

В 2020 году «Совет по стандартам интероперабельности электронной информации на протяжении её жизненного цикла» DLM-форума (Digital Information LifeCycle Interoperability Standards Board, DILCIS) и европейский проект разработки типового блока электронной архивации (eArchiving Building Block) начали разработку Спецификаций типа контента (Content Information Type Specification, CITS) для SIARD – это спецификации, содержащие рекомендации по упаковке контента SIARD вместе с дополнительной документацией и метаданными.

Для поддержки SIARD и спецификаций CITS SIARD, Совет DILCIS и проект eArchiving Building Block в сотрудничестве с Федеральным архивом Швейцарии формируют сейчас тематическую группу по архивации реляционных баз данных. Это будет сообщество, в которого можно будет обмениваться информацией о SIARD, CITS SIARD, об инструментах архивации баз данных, передовых практиках, вариантах использования и соответствующими новостями. Если Вас интересует тема архивации баз данных, зарегистрируйтесь в группе, используя форму по адресу [https://docs.google.com/forms/d/e/1FAIpQLSeRRdac509j6Z2VdQarW8ApzVWaZWmCX-x1C00Cyet\\_gk8PFQ/viewform](https://docs.google.com/forms/d/e/1FAIpQLSeRRdac509j6Z2VdQarW8ApzVWaZWmCX-x1C00Cyet_gk8PFQ/viewform)

Как участник группы, Вы будете получать последние новости и информацию по теме архивации баз данных. Вы также сможете внести свой вклад в деятельность группы, делясь своим опытом, помогая управлять группой, поддерживая разработку SIARD и CITS SIARD - или же просто перенаправив данную ссылку тем из Ваших знакомых, кому членство в группе может быть полезным.

Ссылки на дополнительную информацию:

- Спецификации SIARD: <https://dilcis.eu/content-types/siard>
- Спецификации CITS SIARD: <https://dilcis.eu/content-types/siard>

Проект аналитического отчета по архивации реляционных баз данных, [https://dilcis.eu/images/2020review/9\\_Draft\\_SIARD\\_Case\\_Study\\_1.pdf](https://dilcis.eu/images/2020review/9_Draft_SIARD_Case_Study_1.pdf)

Проект аналитического отчета по архивации реляционных баз данных, часть 2: [https://dilcis.eu/images/2020review/10\\_Draft\\_SIARD\\_Case\\_Study\\_2.pdf](https://dilcis.eu/images/2020review/10_Draft_SIARD_Case_Study_2.pdf)



## **РОБОТИЗИРОВАННЫЕ ДОКУМЕНТЫ: МАСШТАБНАЯ АВТОМАТИЗАЦИЯ ХРАНЕНИЯ БУМАЖНЫХ ДОКУМЕНТОВ**

Источник: блог компании Formtek <https://formtek.com/blog/robotic-records-massively-automating-paper-storage/> Дик Вейсингер

Федеральное бюро расследований США (ФБР) недавно консолидировало и модернизировало свои операции в области управления документами. 120 погонных миль документов, включающих более двух миллиардов физических страниц, собираются и перемещаются в хранилище в городе Винчестере (Winchester), штат Вирджиния. Для перевозки потребуется совершить более 500 рейсов фур, загруженных бумажными документами.

Операции в хранилище будут выполнять более 100 роботов, использующих для управления документами «Автоматизированную систему хранения и поиска» (Automated Storage and Retrieval System). Площадь создаваемой внутри хранилища зоны обслуживания будет примерно соответствовать двум футбольным полям.

Таким образом, на объекте площадью 256 тысяч квадратных футов (*11,1 тысяча квадратных метров*) объединяются документы из 56 полевых офисов. Строительство хранилища шло с 2017 года, и обошлось оно в 135 миллионов долларов.

Можно ли считать такое решение наилучшим использованием денег? Может быть. Но почему бы не оцифровать все документы? При цене 7 центов за страницу затраты на сканирование двух миллиардов страниц составили бы около 140 миллионов долларов. Долгосрочная экономия затрат за счет перехода на электронное хранение, требующее существенно меньших площадей, позволила бы упростить поддержание документов. Дополнительным преимуществом стало бы то, что данные были бы доступны для поиска, и можно было бы создавать их резервные копии, способные обеспечить непрерывность деловой деятельности в случае пожара или иной чрезвычайной ситуации.

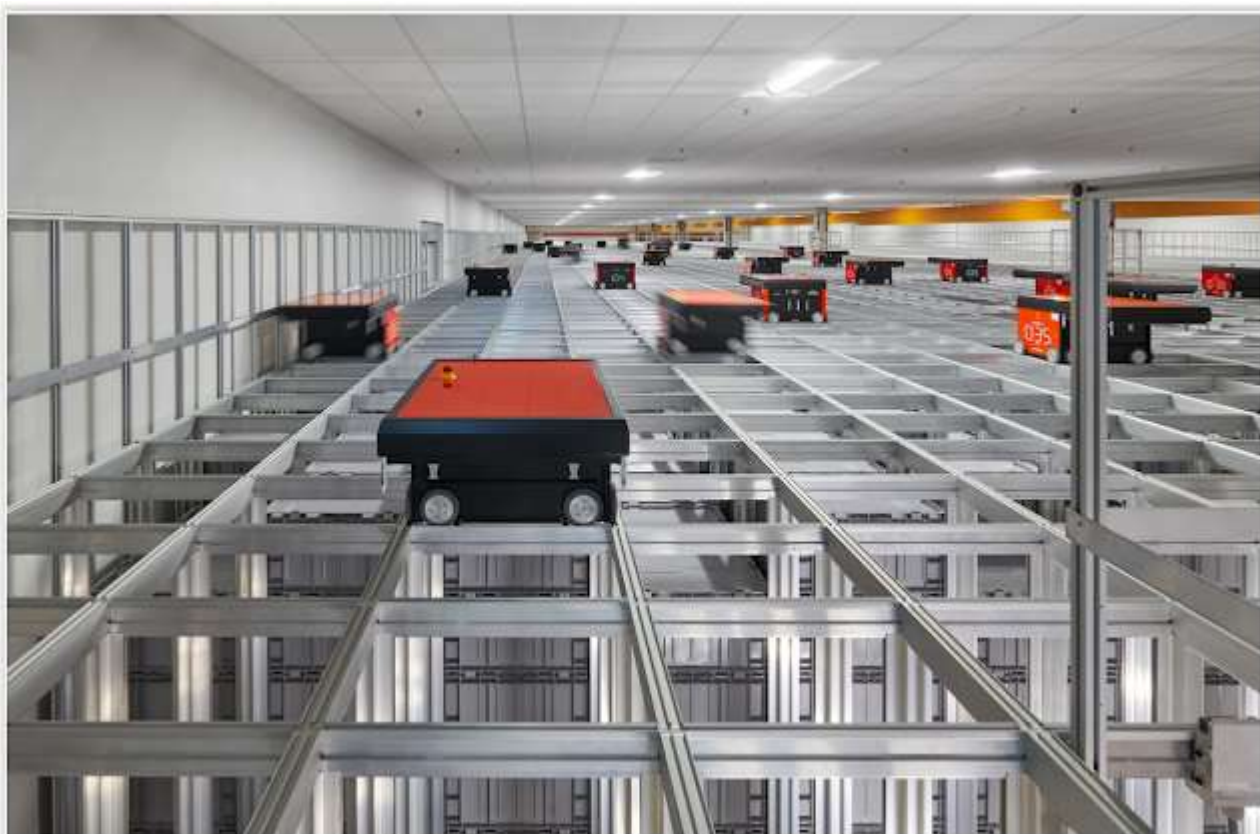


Фото с сайта FBI.gov

## **ИТАЛИЯ: ОБСУЖДАЮТСЯ ПРЕДЛОЖЕНИЯ В ОТНОШЕНИИ НАЦИОНАЛЬНОЙ СТРАТЕГИИ В ОБЛАСТИ ТЕХНОЛОГИЙ БЛОКЧЕЙНА И РАСПРЕДЕЛЕННЫХ РЕЕСТРОВ**

Источник: сайт LinkedIn [https://www.linkedin.com/posts/de-componendis-cifris-iniziativa-nazionale-8274501a5\\_i-suggerimenti-di-cifrischain-sulla-strategia-ugcPost-6717088202101985280-wAWN](https://www.linkedin.com/posts/de-componendis-cifris-iniziativa-nazionale-8274501a5_i-suggerimenti-di-cifrischain-sulla-strategia-ugcPost-6717088202101985280-wAWN)

[https://www.mise.gov.it/images/stories/documenti/Proposte\\_registri\\_condivisi\\_e\\_Blockchain\\_-\\_Sintesi\\_per\\_consultazione\\_pubblica.pdf](https://www.mise.gov.it/images/stories/documenti/Proposte_registri_condivisi_e_Blockchain_-_Sintesi_per_consultazione_pubblica.pdf)

Мы опубликовали наши размышления в качестве реакции на резюме ожидаемого документа «Предложения по итальянской стратегии в области технологий блокчейна и распределенных реестров» (Proposte per una strategia italiana in materia di tecnologie basate su registri condivisi e Blockchain).

Полное название 32-страничного документа - «Предложения по итальянской стратегии в области технологий блокчейна и распределенных реестров - Резюме для публичного обсуждения» (Proposte per la Strategia

italiana in materia di tecnologie basate su registri condivisi e Blockchain - Sintesi per la consultazione pubblica).



Минэкономразвития Италии сформировало группу из 30 экспертов, перед которыми была поставлена задача дать картину текущей ситуации, определить возможные направления развития и последующие социально-экономические последствия внедрения решений, основанных на этих технологиях. Разработанные «Предложения по итальянской стратегии в области технологий блокчейна и распределенных реестров» определяют исходный контекст для национальной стратегии и направлены на то, чтобы внести весомый вклад в европейскую дискуссию по данному вопросу.

Эти предложения направлены на достижение следующих целей:

- Создание в стране конкурентоспособной по сравнению с другими странами законодательно-нормативной базы;
- Рост государственных и частных инвестиций в технологии блокчейн и распределенных реестров (DLT), а также во взаимосвязанные с ними технологии (интернет вещей, 5G);
- Предложения в отношении областей применения этих технологий для правильного целевого использования возможных инвестиций в соответствии с интересами ключевых секторов итальянской экономики;
- Повышение эффективности и результативности взаимодействия с органами государственного управления за счет принятия принципа однократного (Once-Only, см. также [https://en.wikipedia.org/wiki/Once-only\\_principle](https://en.wikipedia.org/wiki/Once-only_principle)) предоставления информации и децентрализации;
- Способствование европейскому и международному сотрудничеству развёртывания общеевропейской инфраструктуры на основе «Европейской инфраструктуры блокчейн-сервисов» (European Blockchain Services Infrastructure, EBSI, см. также <https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI>);

- Использовать данных технологий для облегчения перехода к моделям безотходной (циклической) экономики в соответствии с документом ООН «Преобразование нашего мира: План устойчивого развития до 2030 года» (Transforming Our World – the 2030 Agenda for Sustainable Development, см. [ссылка](https://sustainabledevelopment.un.org/content/documents/21252030%20Agenda%20for%20Sustainable%20Development%20web.pdf)

<https://sustainabledevelopment.un.org/content/documents/21252030%20Agenda%20for%20Sustainable%20Development%20web.pdf> );

- Распространение информации и повышение осведомленности граждан о технологиях блокчейна и распределенных реестров.

Содержание документа следующее:

### **1. Видение и цели**

### **2. Рекомендации**

- 2.1 Общие положения
- 2.2 Развитие циклической экономики
- 2.3 Ключевые сектора для целевых инвестиций в частный сектор, финансовые технологии и кооперативные модели
- 2.4 Идентификация физических и юридических лиц и объектов
- 2.5 Рекомендации по использованию различных типов DLT-технологий
- 2.6 Рекомендации по кибербезопасности различных типов DLT-технологий
- 2.7 Цепочки поставок 4.0
- 2.8 Рекомендации по адаптации инфраструктуры
- 2.9 Рекомендации в отношении цифровых токенов, управляемых с помощью распределенного реестра
- 2.10 Рекомендации в отношении политики повышения осведомленности о секторе криптоактивов
- 2.11 Рекомендации в отношении цепочки создания стоимости (value chain) криптоактивов
- 2.12 Рекомендации по применению законодательства о борьбе с легализацией полученных преступным путём доходов
- 2.13 Рекомендации в отношении введения цифровой валюты Центральным банком
- 2.14 Формирование плана согласованных действий
- 2.15 Ясность в отношении масштабов применения
- 2.16 Ориентация на государственно-частное партнерство
- 2.17 Присутствие на всех этапах образовательного цикла
- 2.18 Акцент на университетское образование и исследования
- 2.19 Национальная координация
- 2.20 Внимание к вопросам популяризации
- 2.21 Программы распространения информации
- 2.22 Общие рекомендации по применению распределенных регистров в деятельности государственных органов

## ЗМІСТ

Передмова.....	1
Европейский комитет по стандартизации CEN думает о создании технического комитета по управлению и обеспечению долговременной сохранности цифрового контента .....	3
ИСО: Подход к данным «по-крупному» .....	7
США: Национальный институт стандартов и технологий NIST опубликовал отчёт NISTIR 8286 «Интеграция кибербезопасности и корпоративного менеджмента риска» .....	9
Вопросы, которые стоит задать на очередной веб-демонстрации для Вас продукта или услуги для управления документами .....	11
Новый стратегический план Международного совета архивов «Расширение возможностей архивов и профессии, 2021-2024» .....	13
США: Национальный институт стандартов и технологий опубликовал специальную публикацию NIST SP 800-209 «Рекомендации по безопасности для инфраструктуры хранения» ....	16
Анализ перспектив: Компромиссное предложение в области электронной сохранности .....	18
Финляндия: «Невидимая работа по управлению документами» .....	23
Китай: Стандарты по вопросам управления документами и архивного дела .....	25
Китай: Для публичного обсуждения опубликован проект национального закона о защите персональных данных .....	26
Канада: Правительство Трюдо думает о создании национального центра рассекречивания исторических документов разведки .....	32
В рамках проекта E-ARK создана тематическая группа по архивации реляционных баз данных.....	35
Роботизированные документы: Масштабная автоматизация хранения бумажных документов .....	36
Италия: Обсуждаются предложения в отношении национальной стратегии в области технологий блокчейна и распределенных реестров .....	37