ПЕРЕДМОВА

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

У публікації «Доверие к государственным документам в 21-м веке» розповідається про те, що сьогоднішній час вимагає від архівістів освоєння нових знань, таких як цифрова криміналістика і обчислювальна архівна наука.

У публікації «Аналитика данных: Тенденции в 2020 году» названо тенденції в області аналітики даних, які ми побачимо в 2020 році.

У публікації «Семинар Библиотеки Конгресса США по системам хранения» наведені витяги із доповідей на семінарі з питань розвитку передових технологій зберігання даних.

У публікації «Австралия: Национальные Архивы «не эффективно» осуществляют надзор за выполнением общегосударственной политики в области управления электронными документами» наведено інформацію Рахункової палати Австралії про недоліки у виконанні програми «Політика безперервного використання електронної інформації – 2020».

У публікації «Национальные Архивы посредством обновления своих рекомендаций прольют свет на процесс постепенного отказа от бумажных документов» розповідається про те, що Національні Архіви США встановили для федеральних органів виконавчої влади кінець 2022 року, як крайній термін оцифровки ними свої історичних документів постійного терміну зберігання.

У публікації «Счётная палата США опубликовала руководство по оценке надёжности данных» наведено мету керівництва, описані принципи, що лежать в основі оцінки надійності використовуваних в ході аудиту даних, а також кроки, пов'язані з проведенням такої оцінки.

У публікації «Мошенничество с электронной подписью. Юридическая и судебная практика» звернуто увагу на можливість використання УКЕП без відома власника, зазначено електронну адресу відеозапису доповіді.

У публікації «Европейский институт телекоммуникационных стандартов ETSI готовит технический отчёт о глобальном признании европейских услуг доверия» розповідається про роботу над технічним звітом ETSI TR 103 684 «Електронні підписи та інфраструктури - Глобальне визнання послуг довіри Євросоюзу», проект якого доступний за адресою https://docbox.etsi.org/ESI/Open/Latest_Drafts/draftTR103684v004-public.pdf.

У публікації «ИСО: Новые проекты по тематике стратегического управления информационными технологиями» розповідається про спільну роботу над новими стандартами в сфері стратегічного управління інформаційними технологіями Міжнародної організація зі стандартизації

(ISO) і Міжнародної електротехнічної комісії (МЕК). Наведено електронні адреси, за якими можна ознайомитись з проєктами нових стандартів.

У публікації «Австрия: Стандарты электронной конструкторской документации и информационного моделирования зданий» розповідається про можливості застосування електронної конструкторської документації та інформаційного моделювання будівель в архівах.

У публікації «Австрийский стандарт ÖNORM A 7700 Требования по безопасности для веб-приложений – версия 2019 года с расширенной областью применения» розповідається про розробку стандарту ÖNORM A 7700: 2019 «Обробка інформації - Вимоги з безпеки для веб-додатків» і внесених до нього доповненнях.

У публікації «ИСО: Обновлён стандарт системы менеджмента качества ISO 10015 по вопросам обучения и повышения квалификации кадров» розповідається про нову редакцію стандарту ISO 10015: 2019 «Менеджмент якості - Керівництво по менеджменту компетенцій та підвищення кваліфікації кадрів», його особливості.

У публікації «Китай: С первого января 2020 года вступают в силу новые «Правила архивной работы в вооружённых силах»» наведено мету перегляду «Правил», звернуто увагу на дотримання особливостей нової епохи, спрямування їх на зміцнення армії. У центрі їх уваги підтримка ефективного виконання збройними силами своєї місії, їх боєздатності, а також усвідомлення особливостей архівно-документаційної роботи в збройних силах в нову епоху.

ДОВЕРИЕ К ГОСУДАРСТВЕННЫМ ДОКУМЕНТАМ В 21-М ВЕКЕ

Источник: блог МСА https://blog-ica.org/2019/11/13/trust-in-public-records-in-the-21st-century/

Государственные учреждения входе выполнения своих функций создают документы, являющиеся как свидетельствами выполненной деятельности, так и подтверждением прав и полномочий отдельных лиц. Архивы, в которых хранятся эти свидетельства, веками выполняли функции доверенной стороны. В 21-ом веке документы, которые прежде в основном были бумажными, создаются в электронной форме. В настоящий момент серьезно обсуждаются такие вопросы, связанные с электронными документами, как «Как им доверять?», «Как архивисты будут обеспечивать их сохранность» и «Как будет обеспечено сохранение доказательной силы документов?».

Во многих странах государственные документы считаются аутентичными, пока не доказано обратное. Эта презумпция была справедливой для бумажных документов, которые имеют фиксированную форму и не изменяются в процессе передачи. Однако даже если электронный документ имеет фиксированную форму, определяемую набором его компонентов, существует вероятность того, что он может быть изменен во время передачи. По этой причине одна из основных обязанностей архивистов 21-го века прямо связана с доказыванием того, что форма и содержание электронных документов не подвергались несанкционированным изменениям и что их характеристики были сохранены.

Доказывание того, что свойства электронных документов сохранились неизменными, поддержание непрерывной работоспособности систем и проведение анализа рисков – всё это способы повысить доверие к электронным документам. Доверие к архивам растёт по мере того, как заинтересованные стороны во всё большей мере разделяют одни и те же ценности. Для укрепления доверия могут также использоваться хорошо продуманные индикаторы – мы используем в этом качестве технологические и организационные показатели. На что нам следует полагаться в большей степени – на технологические меры, такие как криптографические проверки и программное обеспечение; или же на организационные меры, такие, как архивные описания, процессы и процедуры управления документами и классификационные схемы и номенклатуры дел? Судя по всему, архивистам 21-го века приходится заниматься такими видами деятельности, которыми они не владеют в достаточной степени. Возможно, им потребуется серьезно повысить свою квалификацию; и чем большими знаниями и навыками они овладеют, тем больше будет уверенность в качестве их работы.

До 21-го века у архивистов не было привычки сотрудничать с представителями других специальностей, в том числе информационных

технологий. Использование электронно-цифровых технологий сделало сотрудничество архивистов с ИТ-специалистами абсолютно необходимым. Эта необходимость, в частности, связана и с тем, что архивисты не участвуют на некоторых этапах процессов. Например, при выполнении криптографических проверок не все их стадии контролируются архивистами, но они в то же время играют ключевую роль в выявлении критических-важных элементов, и это требует от архивистов освоения новых знаний. Такие дисциплины, как цифровая криминалистика и вычислительная архивная наука, по-видимому, входят в число тех, которые архивисты 21-го века должны освоить. Хотя изучение этих дисциплин может показаться сложной задачей, 21-й век может оказаться самым увлекательным временем для того, чтобы быть архивистом.

АНАЛИТИКА ДАННЫХ: ТЕНДЕНЦИИ В 2020 ГОДУ

Источник: блог компании Formtek https://formtek.com/blog/data-analytics-trends-in-2020/

Способность проводить аналитику данных вошла в число критически-важных возможностей организаций. Консультационная фирма Гартнер (Gartner) назвала тенденции в области аналитики данных, которые мы увидим в 2020 году (см. https://www.datamation.com/big-data/5-data-analytics-trends-shaping-the-future-of-analytics.htm):

- **Дополненная аналитика** (Augmented Analytics) – Аналитическое программное обеспечение станет проще в использовании, так что готовить и обрабатывать данные смогут пользователи, не имеющие специальной подготовки по работе с данными;
- **Цифровая культура** – Проблемы этики и обеспечения неприкосновенности частной жизни побудят организации разработать профессиональный кодекс поведения в сфере работы с данными;
- **Аналитика взаимоотношений** (Relationship Analytics) – Аналитические инструменты все чаще будут использоваться для выявления и высвечивания взаимоотношений между людьми и вещами для демонстрации с тем, чтобы показать связи между данными. Эту возможность в особенности будет поддерживать аналитика графов (graph analytics).
- **Интеллектуальное принятие решений** (Decision Intelligence) – Искусственный интеллект будет использоваться для объединения аналитики из ряда систем и приложений для различных функциональных групп с тем, чтобы принимать более качественные решения на основе более полных данных и аналитических рекомендаций;

- **Коммерческое использование искусственного интеллекта и машинного обучения** – До сих пор доминировали инструменты искусственного интеллекта и машинного обучения на основе открытого кода, однако к 2022 году почти три четверти ИИ-систем будут представлять собой коммерческое программное обеспечение. Поставщики корпоративного программного обеспечения обеспечивают совместимость с инструментами на основе открытого исходного кода, но добавляют функциональные возможности, обеспечивающие расширенные масштабируемость, повторное использование и интеграцию;
- **«Ткань данных»** (Data Fabric) – Согласованные методы доступа к данным в распределенной среде данных дадут пользователям возможность при доступе к данным обходить «стены» изолированных систем (siloed systems).
- **Аналитика с речевым интерфейсом** (Conversational Analytics) – Аналитические запросы все чаще будут выполняться с использованием текста или речи на естественном языке, как правило, посредством виртуального помощника. Это будет ещё одним шагом к упрощению применения инструментов аналитики.

СЕМИНАР БИБЛИОТЕКИ КОНГРЕССА США ПО СИСТЕМАМ ХРАНЕНИЯ

Источник: DSHR's Blog *блог д-ра Дэвида Розенталя* https://blog.dshr.org/2020/01/library-of-congress-storage.html , *см. также* https://www.lockss.org/contact-us/dshr/

Библиотека Конгресса США опубликовала доклады и презентации с семинара «Разработка архитектур систем хранения для цифровых коллекций» (2019 Designing Storage Architectures for Digital Collections, http://www.digitalpreservation.gov/meetings/storage19.html), который состоялся в начале сентября. Мне очень понравились предыдущие семинары этой серии, поэтому мне было жаль, что я не смог принять участие в семинаре на этот раз. Ниже я анализирую некоторые из представленных на семинаре докладов.

Доклад Роберта Фонтана (Robert Fontana) и Гэри Декеда (Gary Decad)

Как обычно, Фонтана и Декед из компании IBM представили свой замечательный обзор ландшафта решений для хранения информации, см. http://www.digitalpreservation.gov/meetings/DSA2019/Day_1/03_fontana_2018-Storage-Landscape-09092019.pdf .

The 2018 Storage Landscape

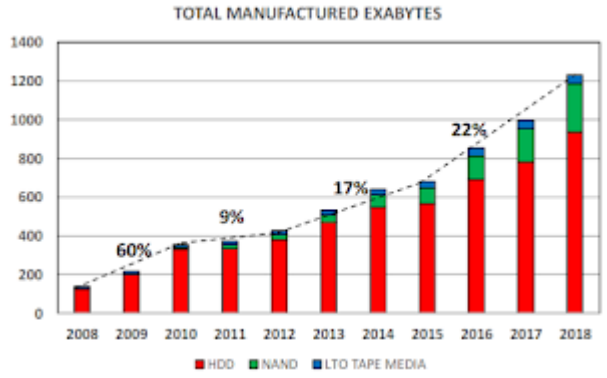
IBM

	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
HDD											
Units (HDD millions)	540	557	652	620	577	551	564	470	425	406	374
PB Shipped (PB)	125000	200000	330000	335000	380000	470000	549000	565000	693000	780000	938000
Areal Density (Gb/in^2)	380	530	635	750	750	900	900	1000	1100	1200	1200 (?)
Revenue ($B)	34.0	34.0	33.0	33.5	37.5	33.4	33.4	28.3	26.8	26.1	26.4
$/GB Shipped	0.272	0.170	0.100	0.100	0.100	0.071	0.061	0.051	0.039	0.033	0.028
NAND											
Wafers (12"-millions)	7.3	8.3	9.7	11.3	12.1	13.7	14.8	15.9	17.0	18.1	18.9
PB Shipped (PB)	3000	5430	10464	18600	28000	39000	62500	83000	120000	175000	250000
Areal Density (Gb/in^2)	200	280	330	550	550	850	1200	1500	2000	2500	3000 (?)
Revenue ($B)	10.1	12.1	18.5	21.5	22.0	24.0	32.2	33.2	38.7	56.5	63.2
$/GB Shipped	3.33	2.23	1.77	1.16	0.78	0.615	0.515	0.401	0.320	0.320	0.252
LTO TAPE MEDIA											
Units (Cart millions)	27.1	24.3	25.0	24.3	23.4	21.6	22.2	19.4	19.4	18.0	
PB Shipped (PB)	11050	11960	15340	18420	20680	24270	30100	33020	40320	44850	44850
Areal Density (Gb/in^2)	0.9	0.9	1.2	1.2	2.1	2.1	2.1	4.1	4.1	8.0	8.0
Revenue ($B) [SCCG]	1.0	0.7	0.7	0.7	0.62	0.54	0.50				
Revenue ($B) [LTO.org]								0.59	0.65	0.66	0.44
$/GB Shipped	0.0905	0.0585	0.0456	0.0380	0.0300	0.0222	0.0166	0.0177	0.0162	0.0147	0.0098

R. Fontana, G. Decad 09/09/19 © IBM 2019 2018 Storage Landscape -- Library of Congress 4

Таблица, отражающая динамику развития ведущих технологий хранения данных (Фонтана и Декед)

Ключевые аспекты их доклада включают:

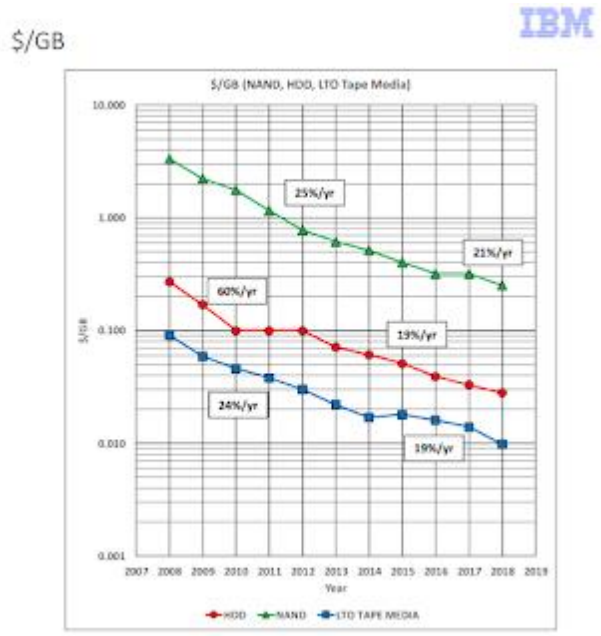


Слайд 5: Общий объём ежегодно производимых носителей информации продолжает расти в геометрической прогрессии на уровне около 20% в год. Подавляющее большинство объёма хранения (76%) – это жёсткие диски, однако доля флеш-накопителей (20%) увеличивается. Доля магнитной ленты остается очень маленькой (4%).

Слайд 12: Авторы сопоставляют этот 20% темп роста предложения на рынке с традиционно неправдоподобным 40-процентным ростом «спроса». В своём анализе они предполагают, что каждый произведенный в течение года байт систем хранения соответствует сохранённому в этом году байту данных, что не соответствует действительности (детальное разоблачение этого мифа см в моём посте 2016 года под названием «Куда делись все эти биты?» – Where Did All Those Bits Go?, https://blog.dshr.org/2016/09/where-did-all-those-

bits-go.html). Как следствие, несоответствие спроса и предложения, о котором они говорят, на самом деле представляет собой огромную, хотя и неактуальную, недооценку.

Однако они совершенно точно подметили тот ключевой момент, что жёсткие диски (HDD) обеспечивают 75% битов и 30% дохода, в то время, как флеш-накопители (NAND) – 20% битов и 70% дохода.



Слайд 9: Темпы снижения стоимости хранения в законе Марка Крайдера (Mark Kryder) для флеш-накопителей NAND, жёстких дисков и магнитных лент сопоставимы; и уменьшение стоимости хранения гигабайта данных происходит таким образом, что ни одна из технологий не получает конкурентного преимущества.

В то же время, как я писал, по крайней мере, с 2012 года (см. мой пост «В будущем хранение будет куда менее доступным, чем прежде» – Storage Will Be A Lot Less Free Than It Used To Be, https://blog.dshr.org/2012/10/storage-will-be-lot-less-free-than-it.html), показатель Крайдера значительно снизился по сравнению со старыми добрыми днями:

Стоимость в долларах хранения гигабайта информации снижается примерно на 19% в год, а не в соответствии с классическим прогнозом на основе закона Мура – на 28% в год, предполагающим удвоение плотности записи информации каждые 2 года.

Как показывает моя экономическая модель (см. https://blog.dshr.org/2017/08/economic-model-of-long-term-storage.html), это приводит к тому, что долговременное хранение данных требует значительно больших инвестиций.

EXABYTES	2018	2026	Increase
NAND	250	4371	17.4X
HDD	938	4033	4.3X
LTO TAPE	44	116	4.2X
TOTAL	1232	8520	6.9X

REVENUE	2018	2026	Increase
NAND	$63.2B	$183.6B	2.9X
HDD	$26.4B	$28.2B	1.1X
LTO TAPE	$0.44B	$0.49B	1.1X
TOTAL	$90.0B	$211.8B	2.4X

$/GB	2018	2026	Decrease
NAND	$0.252/GB	$0.042/GB	0.167X
HDD	$0.028/GB	$0.007/GB	0.248X
LTO TAPE	$0.010/GB	$0.0024/GB	0.24X

- Issue: In 2026 is there demand for 7X more manufactured storage annually and is there sufficient value for this storage to spend $122B more annually (2.4X) for this storage.

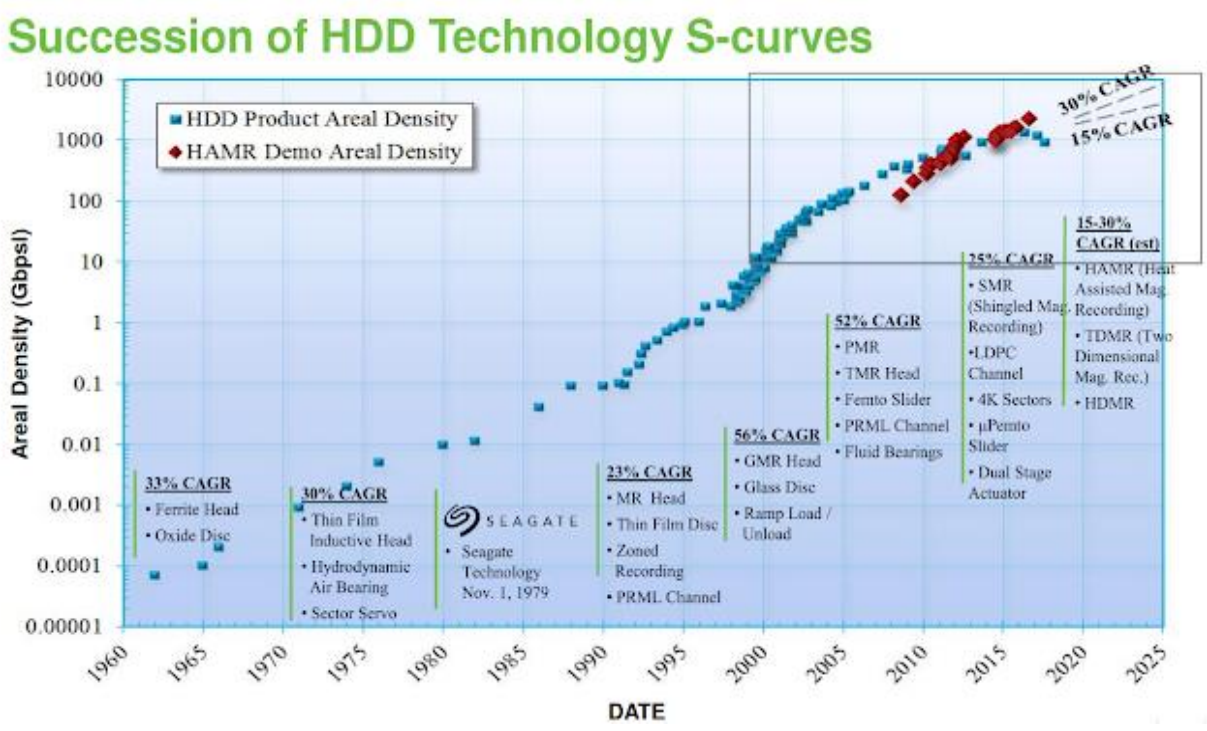
Прогноз развития рынка систем хранения к 2026 году

Слайд 11: В 2017 году флеш-память была в 9,7 раза дороже, чем память на жёстких дисках. В 2018 году различие было в 9 раз. Таким образом, несмотря на восстановление рынка после дефицита поставок в 2017 году, флеш-память не достигла значительных успехов в сокращении преимуществ жесткого диска в стоимости хранения гигабайта информации.

Исходя из текущих тенденций, авторы прогнозируют, что к 2026 году (см. рис выше) будет поставляться больше байтов флеш-памяти, чем памяти на жёстких дисках. Однако они также прогнозируют, что флеш-память всё равно будет в 6 раз дороже за байт. Поэтому они задают хороший вопрос: «Будет ли в 2026 году спрос на семикратно большее по объёму ежегодное производство носителей информации, и будет ли ценность хранимой информации оправдывать на 122 миллиарда долларов большие ежегодные расходы (рост в 2,4 раза)?».

Доклад Джона Трентама (Jon Trantham)

Джон Трентам (Jon Trantham) из компании Seagate подтвердил, что, как это уже продолжалось в течение десяти лет (см. мой пост https://blog.dshr.org/2019/06/hamr-ing-home-my-point.html), дата начала массовых поставок HAMR-накопителей (*это накопители на основе т.н. термомагнитной записи, или магнитной записи с нагревом носителя, heat-assisted magnetic recording, потенциально обеспечивающей более высокую плотность записи данных и более высокую скорость их передачи*), все еще отодвигается в будущее: «В настоящее время компания Seagate поставляет HAMR-приводы в ограниченных количествах ключевым клиентам».



Последовательность S-кривых роста плотности хранения данных на жёстких дисках

Жёсткие диски

Его презентация (см. http://www.digitalpreservation.gov/meetings/DSA2019/Day_1/05_trantham_LibraryOfCongress_2019_Trantham_Seagate.pdf) интересна тем, что в ней раскрываются некоторые подробности об исключительных проблемах, связанных с производством HAMR-приводов, включая изображения, показывающими, насколько всё миниатюрно:

- Расстояние от нижней части читающей головки (slider) до верхней части лазерного модуля составляет менее 500 микрон (*полмиллиметра*);
- Воздушный зазор при движении головки над поверхностью диска составляет всего 1-2 нанометра (*нанометр – одна миллионная миллиметра*)

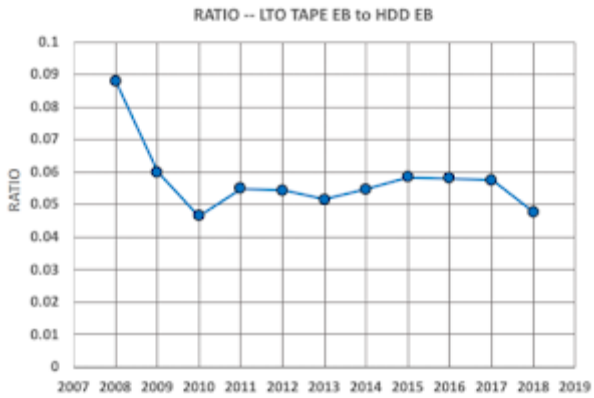
Как обычно, я прогнозирую, что отрасль с большей вероятностью достигнет совокупного среднегодового темпа роста (compound annual growth rate, CAGR) в 15% для плотности записи (см. приведенный выше график), чем в 30%. Обратите внимание на выполаживание кривой для жёстких дисков «HDD Product» на протяжении последних примерно пяти лет.

Магнитная лента

Анализ ленточных накопителей выявил противоречивые факторы.

Гэри Декед и Роберт Фонтана из компании IBM (см. http://www.digitalpreservation.gov/meetings/DSA2019/Day_1/07_fontana2_Cloud-Storage-and-Tape-09092019.pdf) подчеркнули вполне стабильное будущее ленты, показав, что:

- Лента, в отличие от жёстких дисков, последовательно достигала запланированных показателей увеличения ёмкости; и что



В течение последних 8 лет отношение произведенных экзабайт хранения на ленте к объёмам произведенных накопителей на жёстких дисках оставалось постоянным в диапазоне 5,5 %.

В отличие от жестких дисков, физика магнитной ленты не является ограничивающим фактором, поскольку битовые ячейки на ленте в 60 раз больше битовых ячеек жёсткого диска ... Расчётная плотность записи на магнитной ленте в 2025 году (90 Гбит на кв.дюйм) в 13 раз меньше, чем сегодняшняя плотность записи на жёстком диске, и такая плотность уже продемонстрирована в лабораторных условиях.

Карл Уоттс (Carl Watts) в докладе «Проблемы индустрии магнитных лент» (Issues in Tape Industry, http://www.digitalpreservation.gov/meetings/DSA2019/Day_1/06_watts_Issues-in-Tape-Industry.pdf) предложил ряд контраргументов, отметив, что риски для лент не являются технологическими:

- IBM является последним из производителей оборудования:
  - IBM - единственный разработчик лент стандарта LTO8;
  - IBM - единственный оставшийся поставщик ленточных накопителей корпоративного класса;
  - Если у Вас есть только один производитель, каким образом можно смягчать риски?
- Все эти облачные архивные решения используют ленту:
  - Amazon AWS Glacier и Glacier Deep (1 доллар за терабайт в месяц)
  - Архив общего назначения Azure General Purpose v2 (2 доллара за терабайт в месяц)
  - Google GCP Coldline (7 долларов за терабайт в месяц)
- Если это одна и та же лента, каким образом можно смягчать риски?

Если, как утверждают Декед и Фонтана, «хранение на магнитной ленте является стратегическим выбором для публичных, гибридных и частных облаков», то, значит, фирма IBM добилась монопольного положения на

рынке, и это будет иметь последствия для ценовых преимуществ ленточного хранения.

В докладе Джона Трантама (Jon Trantham, http://www.digitalpreservation.gov/meetings/DSA2019/Day_1/05_trantham_LibraryOfCongress_2019_Trantham_Seagate.pdf) описана работа компании Seagate над роботизированными системами, похожими на ленточные и Blu-Ray роботизированные библиотеки, разработанных компанией Facebook (о них см. https://blog.dshr.org/2014/09/more-on-facebooks-cold-storage.html), но, в отличие от них, содержащими картриджи для жёстких дисков, произошедшими от тех, что мы рассматривали в публикации 2008 года «Прогнозирование архивного срока службы съемных жестких дисков» (Predicting the Archival Life of Removable Hard Disk Drives, http://lockss.org/locksswiki/files/ISandT2008.pdf). Тогда мы показали, что биты на пластинах «живут» аналогично битам на ленте. Конечно, у ленты есть то преимущество, что она фактически является трёхмерным носителем информации, а диск - фактически двумерным.

Облачное хранение

На семинаре с полезными маркетинговыми презентации выступили представители компаний

- Amazon – *Фрэнк Патера (Frank Paterra) с докладом «Перемещение данных, их хранение и обработка на Периферии» (Moving, Storing, and Edge Processing Data, см.* http://www.digitalpreservation.gov/meetings/DSA2019/Day_1/11_12_paterra-LOC-Digital-Preservation-2019-09-9.pdf - *H.X.*);
- Wasabi – *Дэвид Френд (David Friend) с докладом «Тенденции облачного хранения» (Trends in Cloud Storage, см.* http://www.digitalpreservation.gov/meetings/DSA2019/Day_1/10_Wasabi_David_Friend_2019_LOC_V3.pdf - *H.X.*); и
- Ceph – *Глен Найнле (Glenn Heinle) с докладом «Что такое Ceph» (Unlocking CEPF, см.* http://www.digitalpreservation.gov/meetings/DSA2019/Day_1/13_heinle_LoC_2019_Heinle_v2.pdf - *H.X.*).

Джулиан Морли (Julian Morley) сообщил о переходе Стэнфордского университета с собственной системы ленточного хранения на облачное хранилище (см. http://www.digitalpreservation.gov/meetings/DSA2019/Day_1/20_Morley_Tape_to_Cloud.pdf - *доклад называется «Путешествие в Облака» - H.X.*), приведя ценные данные о затратах. Ранее я уже рассказывал об экономическом моделировании (см. https://blog.dshr.org/2019/02/economic-models-of-long-term-storage.html), которое Морли использовал для обоснования этого решения.

В опубликованной в популярном ИТ-издании «The Register» статье Тима Андерсона (Tim Anderson) под названием «Архивное хранение появляется в Google Cloud: Станет ли оно конкурентом AWS и Azure?» (Archive storage comes to Google Cloud: Will it give AWS and Azure the cold

shoulder?, см. https://www.theregister.co.uk/2020/01/09/archive_storage_comes_to_google_cloud_how_does_it_compare_to_aws_and_azure/) дано удобное сопоставление ценовых планов, предлагаемых ведущими поставщиками услуг облачного хранения для целей архивного хранения данных (см. рис. ниже), при этом сделан следующий вывод:

	Cold storage	Prices in US$ / month
AWS	1000GB	0.99
	10,000 write operations	0.05
	10,000 read operations	0.004
	1GB retrieval	0.02
	Early deletion charge:	180 days
Azure	1000GB	0.99
	10,000 write operations	0.1
	10,000 read operations	5
	1GB retrieval	0.02
	Early deletion charge:	180 days
Google	1000GB	1.2
	10,000 operations	0.5
	1GB retrieval	0.12
	Early deletion charge:	365 days

Стоимость долговременного хранения и использования неактивной информации (cold storage) в различных системах, в долларах в месяц

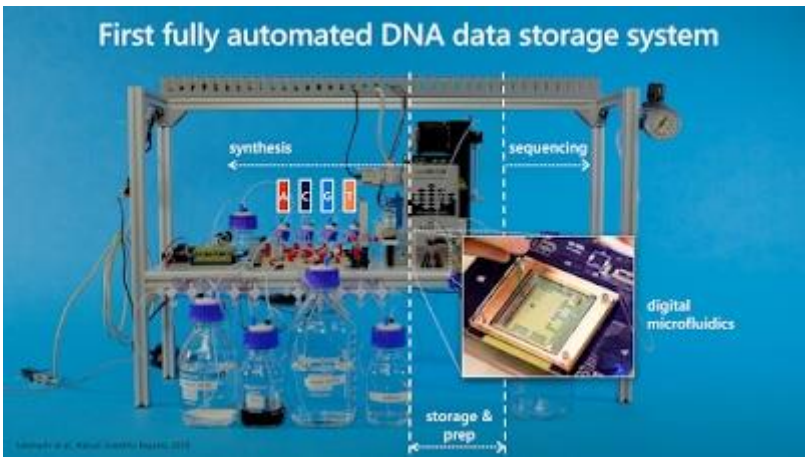
«Обратите внимание на то, что данная таблица даёт очень сильно упрощённую картину. Ценообразование является очень сложным; операции классифицированы более детально, чем просто «чтение» и «запись»; предоставляемые услуги различаются в деталях; и могут предоставляться скидки на зарезервированное хранение. Стоимость передачи данных в рамках Вашей облачной инфраструктуры может быть ниже. Единственный способ обеспечить достоверное сравнение - это сформулировать Ваши точные требования (а также узнать, способен ли поставщик облачных услуг удовлетворить их), и согласовать с поставщиком цену для вашего конкретного случая».

Хранение данных в ДНК

Я уже писал с большим энтузиазмом о потенциале ДНК-хранения в долговременной перспективе, при этом скептически относясь к среднесрочному будущему этой технологии в качестве среды архивного

хранения в течение более чем семи лет (см. https://blog.dshr.org/2018/02/dnas-niche-in-storage-market.html и https://blog.dshr.org/2012/10/forcing-frequent-failures.html).

Меня всегда впечатляли усилия в этой области совместной группы компании Microsoft и университета штата Вашингтон, и работа Карин Стросс (Karin Strauss) и Луиса Цезе (Luis Ceze) по ДНК-хранению и обработке данных не является исключением (см. http://www.digitalpreservation.gov/meetings/DSA2019/Day_2/01_Strauss_LoC-DNAStorage-Sep2019-web.pdf).



Слайд из презентации к докладу Стросс и Цезе

Доклад включает подробности подготовленного ими прототипа законченной автоматической системы для записи и чтения (см. их статью об этом проекте https://doi.org/10.1038/s41598-019-41228-8 , и видео: https://www.youtube.com/watch?v=60Gi5lqL-dA&feature=youtu.be), а также обсуждение методов выполнения вычислений над записанными ДНК-данными в рамках технологий «больших данных».

Энн Фишер (Anne Fischer) в своём докладе рассказала об исследовательской программе американского агентства по передовым военным научно-техническим проектам (Defense Advanced Research Projects Agency, DARPA) в области молекулярной информатики (см. http://www.digitalpreservation.gov/meetings/DSA2019/Day_2/02_fischer_Molecular-Informatics_LOC_Fischer.pdf). Одним из его предшественников этой работы был семинар DARPA в 2016 году (см. https://blog.dshr.org/2016/05/the-future-of-storage.html). В докладе Фишер подчеркивалась разнообразие малых молекул, которые можно использовать в качестве носителя информации. В прошлом году уже писал об одном подходе без использования ДНК, предложенным университетом Гарварда (см. https://blog.dshr.org/2019/05/storing-data-in-oligopeptides.html).

В своём посте «Снижение затрат на запись данных в ДНК» (Cost-Reducing Writing DNA Data, см. https://blog.dshr.org/2019/03/cost-reducing-writing-dna-data.html) я писал о подходе компании Catalog

(https://www.catalogdna.com/), где нить собирается из библиотеки коротких последовательностей основных аминокислот. Это хорошая идея, позволяющая преодолеть один из крупных недостатков ДНК как носителя информации – низкую пропускную способность при записи.

Однако слайды к докладу Девина Лика (Devin Leake - см. http://www.digitalpreservation.gov/meetings/DSA2019/Day_2/03_leake_20190910_LoC_Leake.pdf) небогаты подробностями, и весь доклад больше похож на «речь в лифте» (elevator pitch) с целью уговаривания инвесторов. Доклад начинается с повторения смехотворного прогноза фирмы IDC о количестве «произведенных байтов» (см. мой пост https://blog.dshr.org/2016/09/where-did-all-those-bits-go.html), которое приравнивается к спросу на объёмы хранения и, в частности, архивного хранения. Если Вы развиваете компанию, Вам необходимо гораздо лучшее представление о рынке, на который Вы нацеливаетесь, чем это (см. https://blog.dshr.org/2018/03/archival-media-not-good-business.html - *есть перевод на русский язык здесь:* https://rusrim.blogspot.com/2018/03/blog-post_15.html).

Доклад Генри Ньюмена (Henry Newman)

Добрый доктор Панглосс (*известный персонаж романа Вольтера «Кандид», довольно-таки карикатурно изображающий учёного философа – Н.Х.*) был бы в восхищении от энтузиазма Генри Ньюмана в отношении сетей 5G (см. http://www.digitalpreservation.gov/meetings/DSA2019/Day_1/04_newman_2019.DSA.hsn.v2.pdf), но я настроен куда более скептически.

Это правда, что первые образцы 5G-телефонов способны продемонстрировать скорость передачи данных около 2 гигабит в секунду в очень ограниченных зонах покрытия в некоторых городах США. Однако 5G-телефоны будут стоить дороже (см., например, https://www.cnet.com/news/the-6-hardest-truths-weve-learned-about-5g/), будет дороже их использование, меньше срок службы батареи. У них будет проблема перегрева, менее постоянная полоса пропускания и практически несуществующее покрытие. Взамен Вы получите более высокую пиковую пропускную способность, которую большинство людей не использует. Клиенты уже замечают, что их существующие телефоны «достаточно хороши» (см. https://www.zdnet.com/article/my-four-year-old-iphone-is-too-good-to-upgrade-and-that-should-worry-apple/). Так что переход на 5G ну просто блестящая идея! (см. также https://www.techdirt.com/articles/20200106/08554343687/theres-recurring-theme-with-5g-disappointment.shtml).

Причина, по которой операторы строят сети 5G, связаны отнюдь не с телефонами, а с тем, что они видят золотую жилу в «интернете вещей». Но объедините пропускную способность в 2 Гбит/с с печально известным отсутствием безопасности «интернета вещей» (см., например, https://www.cbsnews.com/news/ring-and-nest-hackers-home-security-cameras-vulnerable-to-cyberattacks/), и у Вас на руках будет катастрофа, которую операторы связи просто не могут допустить.

Интернет вещей распространился по двум причинам. «Вещи» очень дёшевы, и подключение их к интернету не регулируется, поэтому поставщики интернет-услуг не могут создавать здесь препятствий. Однако для подключения «вещи» к 5G-интернету потребуется тарифный план для передачи данных от оператора связи, и это позволит операторам навязывать требования и, следовательно, расходы. Среди требований может быть требование о наличии у «вещей» UL-сертификации (https://www.techdirt.com/articles/20191209/13065843536/ul-pushes-security-standards-internet-broken-things.shtml - *здесь имеется в виду система сертификации, продвигаемая американской компанией по стандартизации и сертификации в области техники безопасности Underwriters Laboratories, о ней см.* https://ru.wikipedia.org/wiki/UL_(Underwriters_Laboratories)), адекватной безопасности и поддержки, включая своевременное обновление программного обеспечения в течение, возможно, довольно длительно срока службы в подключённом состоянии. Именно отсутствие этих дорогостоящих свойств сделало «интернет вещей» столь широко распространённым и таким кошмаром для безопасности (см. https://www.androidpolice.com/2020/01/02/uh-oh-xiaomi-camera-feed-showing-random-homes-on-a-google-nest-hub-including-still-images-of-sleeping-people/)!

Контроль целостности (fixity)

В двух докладах обсуждалась проверка неизменности (fixity checks). Марк Купер (Mark Cooper, см. http://www.digitalpreservation.gov/meetings/DSA2019/Day_1/18_mcooper_lc_dcm_slides.pdf), рассказал об усилиях по проверке как полноты состава, так и контрольных сумм определенной части цифровой коллекции Библиотеки Конгресса США. Был сделан вывод о том, что если технические части общей системы были надежными, то человеческие - не совсем:

- Контент в системе хранения корректен, в отличие от реестров;
- Хранители контента обходят системные ограничения, что приводит к некорректности реестров;
- Контент в электронной системе хранения следует рассматривать как потенциально динамичный, в особенности в плане его представления и доступа;
- Система должна обеспечивать необходимые операции таким образом, чтобы поддерживались их протоколирование и контроль версий.

Представитель компании Google Базз Хейс (Buzz Hayes, см. http://www.digitalpreservation.gov/meetings/DSA2019/Day_1/22_hays_Fixity-on-GCP-Overview.pdf) рассказал о рекомендуемом компанией методе контроля целостности данных в облаке Google. Существуют сценарии для двух традиционных подходов:

- Чтение и вычисление хеша записанных данных, что при больших масштабах обходится дорого из-за оплаты доступа и пропускной способности;
- Хеширование данных непосредственно в облаке, в котором те хранятся, что предполагает доверие к облаку в том плане, что хеш

действительно будет вычислен заново, а не просто будет взято значение, запомненное при приёме данных на хранение.

Мне всё еще предстоит увидеть облачный API-интерфейс, в котором будет реализован метод, опубликованный 12 лет тому назад Мехулом Шахом и др. (Mehul Shah et al, см. https://www.usenix.org/legacy/events/hotos07/tech/full_papers/shah/shah_html/), который предполагает передачу владельцем данных облачному провайдеру однократно используемого случайного числа (nonce), с тем, чтобы тот вычислил во время проверки хеш данных с учётом этого числа. См. также мой пост «Аудит целостности многочисленных экземпляров электронного объекта» (Auditing The Integrity Of Multiple Replicas, https://blog.dshr.org/2019/11/auditing-integrity-of-multiple-replicas.html).

Блокчейн

Шармила Бхатия (Sharmila Bhatia) в своём докладе рассказала об инициативе Национальных Архивов США по изучению потенциала блокчейна для способствования управлению государственными документами (см. http://www.digitalpreservation.gov/meetings/DSA2019/Day_1/08_bhatia_Blockchain-LC-20190909.pdf). В заключение она сделала следующие выводы:

Целостность и аутентичность

- Функциональные возможности технологий блокчейна и распределенных реестров являются новым способом обеспечения целостности и аутентичности электронных документов
- Они могут не помочь при решении задач обеспечения долговременной сохранности и доступности, и могут даже усложнить эти проблемы.

Важно отметить, что то, что Национальные Архивы США подразумевают под «государственными документами», весьма отличается от того, что обычно понимается под термином «документы», - и законодательно-нормативная база, на основе которой действуют Национальные Архивы, может сделать внедрение технологии блокчейна проблематичным.

Бен Фино-Радин (Ben Fino-Radin) и Мишель Ли (Michelle Lee) прорекламировали стартап Starling (см. http://www.digitalpreservation.gov/meetings/DSA2019/Day_1/24_fino-radin_Starling-LC-storage-architectures-mtg.pdf), утверждая, в частности, что он «использует упрощенное и скоординированное децентрализованное хранение в сети Filecoin».

Их слайды описывают, как технология, работает, однако не дают представления о том, сколько это может стоить. Как и в случае с ДНК-хранением и другими экзотическими носителями информации, реальная проблема является экономической, а не технической.

Я уже писал скептически об экономике сети Filecoin в постах «Четырех самых дорогостоящих слова английского языка» (The Four Most Expensive Words in the English Language, https://blog.dshr.org/2018/06/the-four-most-

expensive-words-in.html) и «Триумф жадности над арифметикой» (Triumph Of Greed Over Arithmetic, см. https://blog.dshr.org/2018/08/triumph-of-greed-over-arithmetic.html), сравнивая возможное ценообразование этого решения с решениями S3 и S3 RRS фирмы Amazon. Конечно, цифры выглядели бы намного хуже для Filecoin, если бы я сопоставил их цены с ценами Wasabi.

Заключительные рекомендации организаторам

Такие семинары всегда являются захватывающими событиями. Но, пожалуйста, рассылая в следующем году приглашение принять участие в очередном семинаре, недвусмысленно дайте понять, что любой, кто рискнёт использовать в своих слайдах прогнозы для «произведенных данных» (см. https://blog.dshr.org/2016/09/where-did-all-those-bits-go.html) в качестве актуальных для «хранения данных» и особенно архивного хранения, будет прогнан со сцены калёной метлой.

Дэвид Розенталь (David Rosenthal)

АВСТРАЛИЯ: НАЦИОНАЛЬНЫЕ АРХИВЫ «НЕ ЭФФЕКТИВНО» ОСУЩЕСТВЛЯЮТ НАДЗОР ЗА ВЫПОЛНЕНИЕМ ОБЩЕГОСУДАРСТВЕННОЙ ПОЛИТИКИ В ОБЛАСТИ УПРАВЛЕНИЯ ЭЛЕКТРОННЫМИ ДОКУМЕНТАМИ

Источник: сайт ZNet.com https://www.zdnet.com/article/national-archives-ineffective-in-overseeing-government-wide-digital-record-policy/

Проверив три органа исполнительной власти центрального правительства, австралийская Счётная палата (Australian National Audit Office, ANAO) выявила, что те уже почти на год отстают с достижением определенных целей.

«Политика непрерывного использования электронной информации – 2020» (Digital Continuity 2020 Policy, см. https://www.naa.gov.au/information-management/information-management-policies/digital-continuity-2020-policy , была разработана в 2015 году как инструмент подталкивания органов правительства Австралии к переходу, помимо прочего, на полностью электронно-цифровые рабочие процессы и на управление информацией как активом.

Предполагалось, что эта политика поможет в достижении более широких целей электронного правительства и цифровой экономики, а также обеспечит поддержку внедрения эффективного управления электронной информацией в масштабе центрального правительства Австралии.

Эта политика была принята в соответствии с Законом об архивах 1983 года (Archives Act 1983). Она применима в отношении всей информации, данных и документов государственных органов, в дополнение к системам, услугам и процессам. Администрирование данной политики было поручено Национальным Архивам Австралии.

Счётная палата Австралии (ANAO), однако, заявила, что Национальные Архивы в значительной степени неэффективны в выполнении данной своей обязанности.

«Органы правительства Австралии вряд ли сумеют реализовать цели «Политики непрерывного использования электронной информации» к концу 2020 года, а Национальные Архивы Австралии в значительной степени оказались неэффективными в части мониторинга, оказании помощи и поощрении государственных органов к достижению целей политики», – написала Счётная палата в своём отчёте.

Счётная палата отметила, что выпущенные Национальными Архивами в помощь государственным органам с реализацией данной политики продукты, рекомендации и нормативно-методические документы в основном соответствуют своим задачам, однако в них отсутствует стратегия вовлечения и информационного взаимодействия с заинтересованными сторонами.

Согласно политике, органы государственной власти должны переходить на полностью электронно-цифровые рабочие процессы, а информация должна создаваться и управляться в электронном формате. Политика также требует, чтобы информация, системы и процессы были интероперабельными, соответствующими стандартам краткосрочного и долгосрочного управления; а также повышения качества информации и обеспечения доступности, удобства передачи и повторного использования информации.

Счётная палата считает, что не было обеспечено эффективное определение рисков для реализации политики, управление и информирование о них.

«Приоритеты, цели и задачи, использовавшиеся Национальными Архивами для измерения собственной эффективности в плане надзора над реализацией политики, не были проработаны таким образом, чтобы обеспечить надлежащее соответствие целям и задачам политики», – говорится в отчете ANAO.

«Процессы мониторинга и отчетности были интегрированы в ежегодное обследование органов центрального правительства, однако относящиеся к эффективности сведения не были четко согласованы с самой политикой, не охватывались в достаточной степени процессами обеспечения качества и не включали четких и последовательных измеримых показателей, позволяющих оценить степень успешности».

В отчете Счётной палаты содержится семь рекомендаций, первая из которых требует от Национальных Архивов создать эффективные внутренние механизмы для администрирования и контроля над реализацией данной политики, а также любых последующих политик, которые будут

включать в себя надлежащие меры управления и стратегию, направляющую их администрирование.

Счётная палата также рекомендует разработать эффективную стратегию вовлечения и информационного взаимодействия с заинтересованными сторонами, а также стратегию, включающую в себя возможности мониторинга и сравнительного анализа, с тем, чтобы информация о достигнутом прогрессе непрерывно поступала в Национальные Архивы.

Счётная палата также потребовала разработать план управления рисками.

Для оценки степени реализации политики Счётная палата решила провести аудит в Управлении Генерального прокурора (Attorney-General's Department, AGD), Управлении безопасности гражданской авиации (Civil Aviation Safety Authority, CASA) и Управлении Генерального инспектора в области разведки и безопасности (Inspector-General of Intelligence and Security, IGIS).

Аудит выявил, что все эти три государственных учреждения лишь частично реализовали предусмотренные политикой задачи, крайний срок выполнения которых был 31 декабря 2018 года.

Тем временем, как отметила Счётная палата, Управление Генерального прокурора полностью выполнило или достигло значительного прогресса по всем 17 целям, а Управление безопасности гражданской авиации частично выполнило все задачи, кроме одной. Управление Генерального инспектора в области разведки и безопасности не реализовала ряд целей, в особенности те, что связаны со вторым принципом политики (*Этот принцип гласит, что «Информацией следует управлять в электронной форме»*).

В отчете сообщается, что AGD и CASA создали конкретные механизмы для внутреннего мониторинга и отчетности о прогрессе в достижении целей политики, в то время как IGIS не имеет таких механизмов.

«Хотя IGIS может оказаться не в состоянии оцифровать определённые аналоговые документы из-за ограничений, наложенных органами-создателями этих документов, он пока что не реализовал ни одной из общих целей, связанных с управлением информацией в электронной форме», - пишет ANAO.

Счетная палата предложила IGIS разработать план реализации политики в котором особое внимание должно быть уделено задачам, которые должны были быть реализованы к концу 2018 года.

НАЦИОНАЛЬНЫЕ АРХИВЫ ПОСРЕДСТВОМ ОБНОВЛЕНИЯ СВОИХ РЕКОМЕНДАЦИЙ ПРОЛЬЮТ СВЕТ НА ПРОЦЕСС ПОСТЕПЕННОГО ОТКАЗА ОТ БУМАЖНЫХ ДОКУМЕНТОВ

Источник: сайт FederalNewsNetwork.com https://federalnewsnetwork.com/digital-government/2019/12/nara-to-shed-more-light-on-paper-records-phase-out-through-updated-guidance/

Этим летом Национальные Архивы США (National Archives and Records Administration, NARA) вызвали переполох в сообществе специалистов по управлению документами, когда установили для федеральных органов исполнительной власти конец 2022 года как крайний срок оцифровки ими свои исторических документов постоянного срока хранения.

Помимо этого, соответствующий меморандум, выпущенный совместно с Административно-бюджетным управлением (Office of Management and Budget, OMB), запрещает федеральным ведомствам после декабря 2022 года содержать собственные центры хранения документации. После этой даты Национальные Архивы также не будут принимать бумажные документы на архивное хранение.

Но помимо установления крайнего срока, представители NARA 5 декабря 2019 года на организованным изданием Federal Computer Week (FCW) семинаре по управлению электронными документами заявили, что обновленное руководства и рекомендации вскоре дадут федеральным органам лучшее представление о том, чего ожидать от перехода с бумажных на электронные документы.

Ведущий аналитик по политике управления документами (Supervisory Records Management Policy Analyst) в офисе руководителя направления управления документами Национальных Архивов США (Senior Agency Official for Records Management) Ариан Раванбакш (Arian Ravanbakhsh) отметил, что в меморандуме для федеральных органов исполнительной власти установлены «смелые цели».

И хотя эти усилия по модернизации потребуют от NARA и ведомственных документационных служб пересмотра их методов ведения деловой деятельности, это, по мнению Раванбакша, необходимые перемены.

«Это именно то, чего, как я полагаю, ожидают от нас наши клиенты, и, честно говоря, это то, что мы в NARA должны сделать, чтобы сохранить свою актуальность и нужность как Национальных Архивов», – сказал он. «Мы больше не можем позволить себе делать двойную работу, поддерживая процессы как для аналоговых, так и для электронных документов. Мы должны сконцентрировать свои ресурсы и внимание на переходе на электронные документы. Для достижения этой цели мы установили четкую веху перемен, что часто необходимо, если мы хотим, чтобы перемены действительно произошли».

Поступая таким образом, Национальные Архивы открыли дверь для инновационных технологий, таких, как технологии автоматизации, которые, по словам Равanбахша, выведут управление документами на «новый уровень».

В течение нескольких месяцев, прошедших с момента публикации меморандума, представители Национальных Архивов собирали отзывы и вопросы от ведомств, касающиеся реализации положений директивы. Равanбахш сообщил, что на основе этой обратной связи Национальны Архивы планируют выпустить дополнительные указания и рекомендации в первом квартале 2020 календарного года.

Обновленное рекомендации, по его словам, также прольют больше света на возможные варианты, которые будут у федеральных органов после закрытия ими собственных центров хранения документации.

Старший аналитик Национальных Архивов по политике в области электронных документов Кортни Андерсон сообщила, что готовящиеся руководства дадут федеральным органам более четкое представление о том, на каких вопросах им следует сконцентрировать внимание в ближайшие годы.

«Национальные Архивы информируют федеральные ведомства о том, что им следует делать для реализации предписываемой политики в виде руководств и бюллетеней. Они действительно нуждаются в помощи по вопросу – как на самом деле им управлять своими электронными документами», отметила Андерсон.

Позднее в этом финансовом году Национальные Архивы завершат свою работу над «вариантами использования» (use cases), которые в деталях разъяснят государственным органам, как им управлять определенными типами документов. Андерсон сказала, что к настоящему моменту Национальные Архивы опубликовали варианты использования электронных документов, сообщений в социальных сетях и передачи документов постоянного срока хранения на архивное хранение в NARA.

«В них действительно пошагово описывается процесс, как всё это делается. Федеральные органы могут использовать данные рекомендации в процессе оценки предлагаемых поставщиками решений, – а поставщики могут с помощью демонстрационных примеров показать, как они на самом деле соответствуют требованиям, которые перечислены в вариантах использования», – отметила Андерсон.

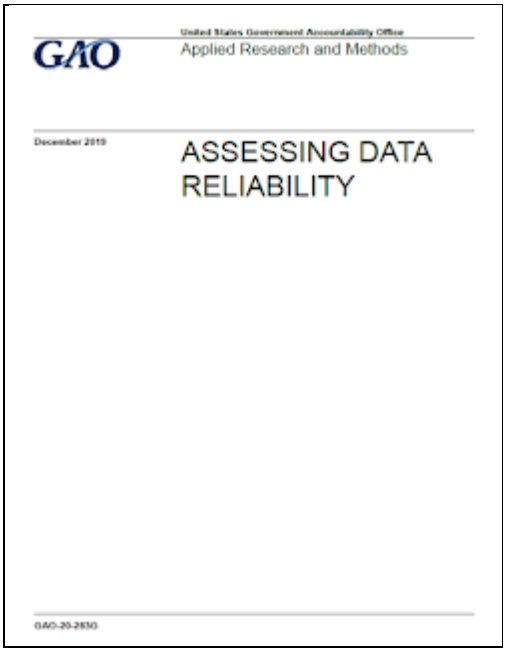
Чтобы упростить закупку федеральными органами услуг по управлению документами, Национальные Архивы в рамках своей «Федеральной инициативы по модернизации управления электронными документами» (Federal Electronic Records Modernization Initiative, FERMI) заключила партнерское соглашение с Управлением общих служб правительства США (General Services Administration, GSA) с тем, чтобы перейти к модели общих служб для целей управления документами.

«Инструменты для управления их электронными документами нужны всем федеральным органам исполнительной власти, и чем выходить на рынок поодиночке и приобретать их самостоятельно, нам выгоднее работать совместно через GSA, чтобы иметь возможность коллективно закупать их на более высоком уровне», - подчеркнула Андерсон.

СЧЁТНАЯ ПАЛАТА США ОПУБЛИКОВАЛА РУКОВОДСТВО ПО ОЦЕНКЕ НАДЁЖНОСТИ ДАННЫХ

Источник: сайт Счётной палаты США https://www.gao.gov/products/GAO-20-283G https://www.gao.gov/assets/710/703275.pdf

16 декабря 2019 года Счётная палата США (Government Accountability Office, GAO) опубликовала любопытный документ **GAO-20-283G «Оценка надёжности данных»** (Assessing Data Reliability) объёмом 72 страницы, см. https://www.gao.gov/products/GAO-20-283G (прямая ссылка на PDF-файл: https://www.gao.gov/assets/710/703275.pdf).



Содержание документа следующее:

Предисловие

1. Что означает «надёжность данных»
2. Принятие решения о необходимости проведения оценки надёжности данных
3. Определение сферы охвата оценки надёжности данных
4. Этапы сбора информации при проведении оценки надёжности данных
5. Принятие заключения о надёжности данных
6. Включение в отчёт надлежащих формулировок
7. Дополнительные соображения

Приложение I: Пример запросов на представление документации и вопросы к собеседованиям

Приложение II: Оценка надёжности данных, поступающих из органов статистики

Приложение III: Примеры тестов для данных

Приложение IV: Примеры формулировок при описании надёжности данных

Приложение V: Благодарности.

Во введении отмечается следующее:

«Данные из внешних источников часто имеют решающее значение для аудита. Хотя эти данные являются лишь одним из видов доказательств, на которые полагаются аудиторы, для надлежащей оценки их надежности могут потребоваться большие технические усилия, чем для других типов доказательств.

Целью настоящего руководства является описание принципов, лежащих в основе оценки надёжности используемых в ходе аудита данных, а также шагов, связанных с проведением такой оценки.

Настоящее руководство согласуется с «жёлтой книгой» – «Стандартами государственного аудита 2018 года» (GAO-18-568G Government Auditing Standards – 2018 Revision, https://www.gao.gov/assets/700/693136.pdf) – которая устанавливает общепринятые государственные стандарты аудита (generally accepted government auditing standards, GAGAS) и заменяет руководство Счётной палаты «Оценка надежности компьютерно-обработанных данных» (GAO-09-680G, Assessing the Reliability of Computer-Processed Data, https://www.gao.gov/assets/80/77213.pdf), выпущенное в 2009 году.

Настоящее руководство охватывает данные, обработанные с помощью вычислительной техники (далее по тексту – просто «данные»), которые являются результатом компьютерной обработки или ввода данных в компьютерную систему. Данные могут различаться по форме и могут размещаться в электронных файлах или в таблицах в опубликованных отчётах. Более подробное обсуждение типов данных, охватываемых данных руководством, содержится в разделе 1.

Различные критерии (tests) оценки достаточности и относимости применяются ко всем типам доказательств, независимо от того, являются ли они частью набора данных, с тем, чтобы определить, соблюдены ли установленные требования к доказательствам. Поскольку в случае данных оценка достаточности и относимости может потребовать более технического анализа, чем для других видов доказательств, может показаться, что в отношении таких данных установлены более жёсткие требования, чем для доказательств иных видов. На самом деле это не так.

Настоящее руководство предлагает гибкую, основанную на анализе риска концепцию оценки надежности данных, которая может быть адаптирована к конкретным обстоятельствам каждого задания на проведение аудита. Концепция позволяет структурировать планирование и отчетность, поощряя аудиторов:

- Использовать имеющиеся сведения о данных,

- Проводить аудиторскую работу лишь в объёме, необходимом для установления того, являются ли данные достаточно надёжными для целей аудита;
- Выносить свои суждения максимально профессионально, и
- Вовлекать в принятие ключевых решений соответствующих лиц, включая представителей руководства и заинтересованных сторон.

Основное внимание при оценке надёжности данных уделяется определению того, могут ли данные использоваться для намеченных целей аудита. Настоящее руководство должно помочь аудиторам сделать надлежащую доказуемую оценку наиболее эффективным способом.»

Также в документе отмечается следующее:

«Хотя настоящее руководство в первую очередь относится к структурированным данным – данным, которые организованы в упорядоченные записи, в которых каждому полю предназначен определенный тип данных (например числовые, текстовые, даты, и т.д.), – однако некоторые из предлагаемых принципов могут быть применимы при изучении неструктурированных данных, которые часто представлены в виде текстовой информации, которая не была организована в структурированный формат для целей анализа».

Ключевая идея отчёта сформулирована следующим образом:

«Чтобы определить, являются ли данные достаточно надёжными для выполнения задания, аудиторы должны учитывать все связанные с аудитом факторы, а также проделанную оценочную работу.

Эти факторы включают в себя:

- Ожидаемая важность данных для итогового отчета;
- Наличие подтверждающих доказательств;
- Риск использования данных;
- Результаты проделанной оценочной работы.

Сила подтверждающих доказательств и степень риска влияют на принятие решения о надёжности данных. Например, если подтверждающие доказательства являются убедительными и риск низок, то данные с большей вероятностью будут признаны достаточно надежными для целей аудита.

Если же подтверждающие доказательства слабы и риск высок, то повышается вероятность того, что данные будут признаны недостаточно надёжными или что их надёжность не будет установлена.

Если при тестировании данных не возникают вопросы и результаты соответствуют существующей документации, то данные с большей вероятностью будут признаны достаточно надёжными для целей аудита».

МОШЕННИЧЕСТВО С ЭЛЕКТРОННОЙ ПОДПИСЬЮ. ЮРИДИЧЕСКАЯ И СУДЕБНАЯ ПРАКТИКА

Источник: Сайт конференции Antifraud Russia – 2019 / YouTube / Google https://vipforum.ru/conferences/antifraud_russia/archive/antifraud_russia_2019/ https://www.youtube.com/watch?v=AnpHFVmIkrE https://drive.google.com/file/d/1ClPwGRJ7qH620cPPfeTvElNsNl0R6n7F/view?usp=sharing , автор: Наташа Храмцовская

Юбилейный X международный форум «Борьба с мошенничеством в сфере высоких технологий. Antifraud Russia – 2019» прошел в Москве. Это главное мероприятие в сфере противодействия компьютерному мошенничеству стало завершающим в осенне-зимнем конференционном марафоне 2019 года, и в нём приняли участие около 650 участников.

Традиционно организаторы форума приглашают на конференцию экспертов смежных отраслей. Так в рамках форума прошел мой семинар **«Мошенничество с электронной подписью. Юридическая и судебная практика»**.

В своём выступлении я, в частности, обратила внимание на то, что существует несколько возможных сценариев использования УКЭП без ведома владельца, в том числе следующие (список не исчерпывающий):

- Владелец сам передает средства создания УКЭП другому лицу, которое злоупотребляет доверием;
- Похищение ключа подписания у владельца;
- Взлом используемой подписантом системы с целью использования её для подписания «левого» документа без похищения ключа подписания;
- Если пара ключей создается УЦ – утечка ключа подписания из УЦ;
- Несанкционированный выпуск сертификата УКЭП посредством обмана честного УЦ;
- Несанкционированный выпуск сертификата УКЭП специально созданным мошенниками УЦ.

В последнее время повышенное внимание общественности привлёк несанкционированный выпуск сертификата УКЭП, и именно этой атаке в основном и был посвящён данный семинар.

Видеозапись доклада выложена по адресу: https://www.youtube.com/watch?v=AnpHFVmIkrE

Презентация к докладу доступна по адресу: https://drive.google.com/file/d/1ClPwGRJ7qH620cPPfeTvElNsNl0R6n7F/view?usp=sharing

ЕВРОПЕЙСКИЙ ИНСТИТУТ ТЕЛЕКОММУНИКАЦИОННЫХ СТАНДАРТОВ ETSI ГОТОВИТ ТЕХНИЧЕСКИЙ ОТЧЁТ О ГЛОБАЛЬНОМ ПРИЗНАНИИ ЕВРОПЕЙСКИХ УСЛУГ ДОВЕРИЯ

Источник: сайт ETSI https://docbox.etsi.org/ESI/Open/Latest_Drafts/draftTR103684v004-public.pdf

Согласно информации на сайте Европейского института телекоммуникационных стандартов (European Telecommunications Standards Institute, ETSI), в настоящее время идёт работа над техническим отчётом **ETSI TR 103 684 «Электронные подписи и инфраструктуры - Глобальное признание услуг доверия Евросоюза»** (Electronic Signatures and Infrastructures (ESI); Global Acceptance of EU Trust Services), проект которого (версия 0.0.4, август 2019 года) объёмом 90 страниц доступен по адресу https://docbox.etsi.org/ESI/Open/Latest_Drafts/draftTR103684v004-public.pdf .

Как сказано в его вводной части, «В настоящем документе представлены результаты изучения существующих сервисов и услуг доверия, работающих в разных регионах мира, и их возможного взаимного признания / глобального признания.

В частности, одной из целей исследования является определение дальнейших шагов, которые могут быть предприняты для облегчения взаимного признания между услугами доверия Евросоюза, оказываемых на основе стандартов ETSI, поддерживающих европейский закон eIDAS (*это закон «Об электронной идентификации и услугах доверия для электронных транзакций на внутреннем рынке», см.* http://eur-lex.europa.eu/legal-

content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN), и услугами доверия на иной основе. Основное внимание уделяется существующих услугам доверия на основе инфраструктуры открытых ключей (PKI), поскольку они являются наиболее распространенными в мире.

В отчёте, во-первых, описывается методология, используемая при сравнении иных услуг доверия на основе PKI с теми, которые регламентированы в существующих стандартах ETSI, и основанная на четырех основных элементах услуги доверия: обстоятельствах (контексте) применения, надзоре и аудите, технических стандартах и информировании о доверии (trust representation). Далее в документе представлена информация, собранная об основных схемах оказания услуг доверия на основе PKI по всему миру и о том, как они соотносятся с европейской схемой оказания услуг доверия, основанной на законе eIDAS и стандартах ETSI. В заключение представлены выводы о тех шагах, которые могут быть предприняты для облегчения взаимного признания».

Содержание документа следующее:

Предисловие

Введение

1. Область применения

2. Ссылки

3. Определения терминов, обозначения и сокращения

4. Методология исследования

5. Информация о существующих схемах оказания услуг доверия на основе PKI

6. Анализ благоприятных факторов и препятствий для взаимного признания

7. Предварительные выводы

Приложение A: Анкета, использованная в процессе исследования

Приложение B: Пример процесса взаимного признания

Приложение C: Модель eIDAS, используемая в качестве эталона для сравнения

На данный момент в разделе «Предварительные выводы» сказано следующее:

Примечание. Приведенные ниже соображения являются предварительными в процессе подготовки окончательных выводов отчёта, и поэтому могут не отражать окончательные результаты данного исследования.

а) Для обеспечения взаимного признания между отдельными услугами доверия на основе PKI, необходимо провести их сопоставление по 4 фундаментальным характеристикам:

- правовой контекст,
- надзор,
- аудит и требования политик в отношении систем на основе PKI,
- информирование о доверии.

b) Принятие общих стандартов, наподобие стандартов ETSI, в качестве основы для предоставления услуг доверия, значительно поможет при обеспечении взаимного признания.

ИСО: НОВЫЕ ПРОЕКТЫ ПО ТЕМАТИКЕ СТРАТЕГИЧЕСКОГО УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ ТЕХНОЛОГИЯМИ

Источник: сайт ИСО

Над новыми стандартами в сфере стратегического управления информационными технологиями, совместно работают Международная организация по стандартизации (ИСО) и Международная электротехническая комиссия (МЭК). В целом к стандартам по данной теме в последнее время проявляется повышенный интерес, поскольку специалисты многих других направлений начинают работать над собственными документами по стратегическому управлению и используют эти стандарты в качестве отправной точки.

Наиболее готов и близок к публикации стандарт **ISO/IEC FDIS 38506 «Информационные технологии – Стратегическое управление ИТ – Использование ISO/IEC 38500 для стратегического управления инвестициями, связанными с применением ИТ»** (Information technology – Governance of IT – Application of ISO/IEC 38500 to the governance of IT enabled investments) объёмом 14 страниц основного текста, см. https://www.iso.org/standard/56640.html и https://standardsdevelopment.bsigroup.com/projects/2016-01820 .

Данный стандарт подготовлен техническим подкомитетом SC40 «Управление ИТ-услугами и стратегическое управление ИТ» Объединённого технического комитета ИСО/МЭК JTC.

В аннотации на данный стандарт отмечается следующее (см. https://standards.globalspec.com/std/13190140/iso-iec-dis-38506):

«Настоящий документ содержит рекомендации по управлению инвестициями, связанными с внедрением и применением информационных технологий (IT enabled investments), адресованные руководящим органам организаций всех форм собственности, как частных, так и государственных. Стандарт будет в равной степени применим вне зависимости от размера организации, отрасли или сектора. Термины «деловая деятельность» (business) и «результат деловой деятельности» (business outcome) в данном документе применяются в отношении всех форм организаций, которые охватываются данным документом (*данные термины включают деятельность государственных и некоммерческих организаций*).

Документ также содержит рекомендации для других сторон, взаимодействующих с руководящими органами, таких, как персонал проекта, бухгалтеры, консультанты по вопросам управления и специалисты по управлению инвестиционным портфелем.

Под «инвестициями, связанными с применением информационных технологий» в рамках настоящего документа понимаются инвестиции любого масштаба, от приобретения бизнеса до любых затрагивающих информационные технологии изменений в деловой деятельности, создания новых бизнес-сервисов или повышения эффективности и продуктивности оперативных ИТ-услуг с целью достижения конкурентного преимущества, независимо от того, являются ли эти сервисы внутренними или предоставляются сторонними организациями.

Настоящий документ также содержит рекомендации, которые можно применять в процессе комплексной проверки, осуществляемой в рамках проявления разумной предусмотрительности (due diligence process) в связи с приобретением бизнеса.

Данный документ может служить руководством по применению принципов, сформулированных в международном стандарте ISO/IEC 38500:2015 «Информационные технологии – Стратегическое управление ИТ в организации» (Information technology – Governance of IT for the organization, *см.* https://www.iso.org/standard/62816.html *и* https://www.iso.org/obp/ui/#!iso:std:62816:en ; *в России адаптирован как ГОСТ Р ИСО/МЭК 38500-2017 «Информационные технологии. Стратегическое управление ИТ в организации», см.* http://protect.gost.ru/v.aspx?control=8&baseC=6&id=210585 , *а также пост о нём здесь:* https://rusrim.blogspot.com/2017/10/blog-post_58.html), для ранжирования связанных с ИТ инвестиций, включая оценку полезности и рисков элементов ИТ - в контексте инвестиционно-банковской деятельности (investment banking) или в том виде, в каком она делается инвестиционными компаниями.

Настоящий документ не предписывает и не устанавливает какой-либо конкретной практики управления, необходимой для инвестиций, связанных с использованием ИТ.

За рекомендациями по внедрению эффективного стратегического управления ИТ в целом следует обращаться к техническим спецификациям

ISO/IEC TS 38501:2015 «Информационные технологии – Стратегическое управление ИТ – Руководство по внедрению» (Information technology – Governance of IT – Implementation guide, см. https://www.iso.org/standard/45263.html и https://www.iso.org/obp/ui/#!iso:std:45263:en).

Рекомендации ISO/IEC TS 38501 могут помочь определить внутренние и внешние факторы, связанные со стратегическим управлением ИТ, и выявить полезную отдачу и доказательства успеха.

По вопросам интеграции с деятельностью руководящего органом и с управлением организацией в целом см. технический отчёт ISO/IEC TR 38502:2017 «Информационные технологии – Стратегическое управление ИТ – Концепция и модель» (Information technology – Governance of IT – Framework and model, см. https://www.iso.org/standard/74358.html и https://www.iso.org/obp/ui/#!iso:std:74358:en ; *о нём также см. пост здесь*: https://rusrim.blogspot.com/2014/02/blog-post_21.html).»

Кроме того, в настоящее время идёт работа над ещё двумя документами:

- **ISO/IEC CD 38503 «Информационные технологии – Стратегическое управление ИТ – Оценка стратегического управления ИТ»** (Information technology – Governance of IT – Assessment of governance of IT, см. https://www.iso.org/standard/75547.html и https://standardsdevelopment.bsigroup.com/projects/2018-01751);
- **ISO/IEC AWI 38507 «Информационные технологии – Стратегическое управление ИТ – Последствия для стратегического управления использования организацией искусственного интеллекта»** (Information technology – Governance of IT – Governance implications of the use of artificial intelligence by organizations, см. https://www.iso.org/standard/56641.html и https://standardsdevelopment.bsigroup.com/projects/2018-01742).

АВСТРИЯ: СТАНДАРТЫ ЭЛЕКТРОННОЙ КОНСТРУКТОРСКОЙ ДОКУМЕНТАЦИИ И ИНФОРМАЦИОННОГО МОДЕЛИРОВАНИЯ ЗДАНИЙ

Источник: сайт австрийского органа по стандартизации ÖNORM https://www.austrian-standards.at/produkte-leistungen/kostenlose-downloads/supplements-zu-normen/oenorm-a-6241-1/ , https://shop.austrian-standards.at/action/de/public/details/545938/OENORM_A_6241-1_2015_07_01

В настоящее время, существующее программное обеспечение для информационного моделирования зданий, используется отдельными лицами, деловыми организациями и государственными учреждениями, которые занимаются планированием, проектированием, строительством, эксплуатацией и обслуживанием разнообразных физических инфраструктур – например, для водоснабжения, канализации, электро- и газоснабжения, связи, а также автомобильных и железных дорог, мостов, портов и туннелей».

Речь, таким образом, идёт о создании многоплановых всеохватывающих информационных моделей, которые превращаются в основной источник сведений об объекте и сопровождают его на протяжении всего его жизненного цикла, вплоть до завершения этапа вывода из эксплуатации. Данные модели могут иметь долговременную научно-техническую и историческую ценность, оправдывающую их сохранение даже после вывода объекта из эксплуатации. Именно поэтому данный вопрос представляет интерес для современных электронных архивистов и специалистов по управлению документами.

Википедия: (см. https://en.wikipedia.org/wiki/Building_information_modeling) даёт следующее определение: **Информационное моделирование зданий (building information modeling, BIM)** – это процесс, поддерживаемый различными инструментами, технологиями и контрактами, и включающий создание и управление электронно-цифровыми представлениями физических и функциональных характеристик мест и объектов.

BIM-модели – это файлы (часто, хотя и не всегда, представленные в проприетарных форматах и содержащие проприетарные данные). Эти файлы можно извлекать, обмениваться ими или объединять связями для поддержки принятия решений в отношении построенного объекта.

Использование подхода BIM и соответствующих инструментов пока что не является обязательным, однако они уже сегодня нередко применяются крупными фирмами при строительстве и эксплуатации разнообразных объектов. В связи с этим в Австрии сочли нужным разработать состоящий из нескольких частей национальный стандарт **ÖNORM A 6241 «Электронная строительная документация»** (Digitale Bauwerksdokumentation, английское самоназвание Digital structure documentation).

В 2015 году были опубликованы первые две части стандарта, разработанные техническим комитетом ТК11 «Общие вопросы строительства зданий» (Komitee 011 Hochbau Allgemeines / Building construction):

- **ÖNORM A 6241-1:2015 «Электронная строительная документация – Часть 1: Структуры САПР-данных и информационное моделирование зданий (BIM) – Уровень 2»** (Digitale Bauwerksdokumentation – Teil 1: CAD-Datenstruktur und Building Information Modeling (BIM) – Level 2), см. https://shop.austrian-standards.at/action/de/public/details/545938/OENORM_A_6241-1_2015_07_01

Данный стандарт регламентирует техническую реализацию обмена и хранения данных о строительстве зданий и связанных с ними пространственно-образующих конструкциях гражданского строительства, которые необходимы в ходе управления жизненным циклом недвижимости.

Данный австрийский стандарт определяет наиболее важные термины, структуры и принципы представления для основных методов передачи двумерных САПР-фалов и для информационного моделирования зданий.

В 2019 году начата подготовка новой редакции данного документа.

- **ÖNORM A 6241-2:2015 «Электронная строительная документация – Часть 2: Информационное моделирование зданий (BIM) - Уровень 3 – iBIM»** (Digitale Bauwerksdokumentation - Teil 2: Building Information Modeling (BIM) - Level 3 – iBIM), см. https://shop.austrian-standards.at/action/de/public/details/545935/OENORM_A_6241-2_2015_07_01

Данный стандарт регламентирует техническую реализацию унифицированных структурированных 3D+ моделей данных для гражданских зданий и связанных с ними пространственно-строительных конструкций гражданского строительства на основе информационного моделирования зданий (BIM).

Модель данных является основой для сотрудничества (в плане технической реализации обмена данными, использования общей модели данных, а также управления данными) всех участников процесса управления жизненным циклом, начиная от идеи, планирования и строительства, через последующее управления и до вывода из эксплуатации и сноса.

Данный стандарт создает основу для всестороннего, унифицированного, нейтрального к программным продуктам и систематического обмена графическими данными и метаданными. Предусмотрена обратная совместимость со стандартом ÖNORM A 6241-1.

Также идёт работа ещё над несколькими частями стандарта:

- **ÖNORM A 6241-3:2019 «Электронная строительная документация – Часть 3: Информационное моделирование зданий (BIM) – Автоматизированное управление зданиями и сооружениями на основе BIM»** (Digitale Bauwerksdokumentation - Teil 3: Building Information Modeling (BIM) – BIM basiertes Computer Aided Facility Management (CAFM));
- **ÖNORM A 6241-4:2019 «Электронная строительная документация – Часть 4: Информационное моделирование зданий (BIM) – Автоматизация зданий и управления ими»** (Digitale Bauwerksdokumentation – Teil 4: Building Information Modeling (BIM) – Gebäudeautomation);
- **ÖNORM A 6241-10:2019 «Электронная строительная документация – Часть 10: Информационное моделирование зданий (BIM) – Определения и основы»** (Digitale Bauwerksdokumentation – Teil 10: Building Information Modeling (BIM) – Begriffsbestimmungen und Grundlagen).

АВСТРИЙСКИЙ СТАНДАРТ ÖNORM A 7700 ТРЕБОВАНИЯ ПО БЕЗОПАСНОСТИ ДЛЯ ВЕБ-ПРИЛОЖЕНИЙ – ВЕРСИЯ 2019 ГОДА С РАСШИРЕННОЙ ОБЛАСТЬЮ ПРИМЕНЕНИЯ

Более дюжины экспертов по вопросам безопасности на протяжении последних двух лет активно участвовали в работе группы австрийского органа по стандартизации ÖNORM по разработке стандарта AG001.77, принеся в него свои конкретные знания в соответствующих областях.

Предыдущая версия стандарта (ÖNORM A 7700:2008, Informationsverarbeitung - Sicherheitstechnische Anforderungen an Webapplikationen, см. https://shop.austrian-standards.at/action/de/public/details/318145/OENORM_A_7700_2008_12_01) была опубликована в декабре 2008 года и, учитывая высокие темпы развития ИТ, уже несколько устарела. В рамках необходимого обновления содержания стандарта мы также решили расширить сферу его применения. Она была сосредоточена исключительно на технических аспектах безопасности веб-приложений и не включала базовых требований в отношении безопасного оперативного использования. Также в предыдущей версии не рассматривались вопросы, связанные с защитой персональных данных.

Теперь эти вопросы добавлены в новую версию ÖNORM A 7700:2019 «Обработка информации – Требования по безопасности для веб-приложений» (Informationsverarbeitung – Sicherheitstechnische Anforderungen an Webapplikationen). Это сделало необходимым разделить ранее единый документ на ряд частей.

Стандарт ÖNORM A 7700 был разделён на четыре части, чтобы четко разграничить отдельные темы. В первой части определена основная терминология, а в частях со второй по четвёртую – описаны технические требования:

- ÖNORM A 7700-1: «Определения» (Begriffsbestimmungen);
- ÖNORM A 7700-2: «Требования по защите персональных данных» (Anforderungen durch Datenschutz);
- ÖNORM A 7700-3: «Требования по безопасности» (Sicherheitstechnische Anforderungen);
- ÖNORM A 7700-4: «Требования к безопасной эксплуатации» (Anforderungen an den sicheren Betrieb).

Направленность и задачи такого документа, как стандарт, четко определены национальным органом по стандартизации. В качестве документа, устанавливающего требования, определяющие текущую практику, стандарт ÖNORM A 7700 должен предписывать, что делать, а не как это делать. В результате в стандартах данной серии отсутствуют какие-

либо указания, связанные с конкретными технологиями, и сформулированы высокоуровневые общие требования, на способы реализации которые не накладывают каких-либо ограничений. Если Вам нужны технически-нейтральные требования, Вы найдете их в данном стандарте!

Требования к веб-приложениям по защите персональных данных

Уже через год после публикации нового европейского законодательства о защите персональных данных – «Общих правил защиты персональных данных» (General Data Protection Regulation, GDPR, см. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN), появилась потребность в конкретных рекомендациях по вопросам исполнения требований GDPR. С точки зрения защиты персональных данных веб-приложениями, мы стремимся сформулировать соответствующие основные правила.

В результате этих усилий появился стандарт ÖNORM A 7700-2. Наша цель заключалась в том, чтобы определить требования к защите персональных данных, которые бы не были неоправданно избыточными в сравнении с GDPR. Стандарт учитывает конкретные потребности разработчиков, которым необходимо знать требования по защите персональных данных при разработке и внедрении веб-приложений, а также дает перекрестные ссылки на GDPR.

Хотя в центре внимания стандарта, по понятным причинам, находятся веб-приложения, которые собирают персональные данные, он также включает рекомендации и для тех веб-приложений, которые этого не делают. В частности, рассмотрены вопросы идентификации и отслеживания пользователей, даже если никакие персональные данные явным образом не собираются.

Помимо обязательных требований, стандарт ÖNORM A 7700-2 также предлагает необязательные рекомендации на основе примеров (например, предоставление уведомлений). Следует отметить, что безопасность персональных данных в значительной степени зависит от устойчивости приложения и базовой инфраструктуры к атакам. В этой связи в ÖNORM A 7700-2 прямо сказано, что для соответствия требованиям данной части стандарта также необходимо соответствовать требованиям ÖNORM A 7700-3 и ÖNORM A 7700-4.

Обновление и расширение технических требований по безопасности для веб-приложений

Те, кто уже знаком с предыдущей редакцией стандарта ÖNORM A 7700: 2008, воспримут новую редакцию требований по безопасности ÖNORM A 7700-3: 2019 как её обновление и расширение. Сохранены все ранее существовавшие темы, и, кроме того, в документ были включены новые важные вопросы.

Рассмотрен вектор атак типа «подделка http-запросов» (CSRF, также известный как «угон сеанса» - session riding), о котором ранее явно не говорилось. Ранее это было проблемой, поскольку атака на межсайтовые

запросы (Cross Site Request Forgery, CSRF) является распространенной проблемой для веб-приложений. Новая версия стандарта закрывает этот пробел.

Другие улучшения включают в себя защиту от кликджекинга (*согласно Википедии, это механизм обмана пользователей интернета, при котором злоумышленник может получить доступ к конфиденциальной информации или даже получить доступ к компьютеру пользователя, заманив его на внешне безобидную страницу или внедрив вредоносный код на безопасную страницу, см.* https://ru.wikipedia.org/wiki/Кликджекинг), защиту от небезопасной сериализации и десериализации, а также требования к протоколированию специальных событий безопасности.

Тем, кто использует ÖNORM A 7700 в качестве основы для технических требований в процессе закупок, могут понравиться новыми требованиями к документации – эта та область, которой поставщики часто пренебрегают.

Требования к обеспечению безопасной работы веб-приложений

Ранее область применения стандарта ÖNORM A 7700 была ограничена собственно веб-приложением. С появлением ÖNORM A 7700-4:2019 область применения была расширена, охватив обеспечение безопасной работы веб-приложений.

В ходе процесса работы над стандартом было особенно сложно определить, какие аспекты следует включить в него, а какие лучше решать посредством других стандартов и руководств. Простое повторение требований таких стандартов систем менеджмента. как ISO/IEC 27002:2013 «Информационные технологии – Методы обеспечения безопасности – Свод хорошей практики использования мер и средств обеспечения информационной безопасности» (Information technology - Security techniques - Code of practice for information security controls, см. https://www.iso.org/standard/54533.html и https://www.iso.org/obp/ui/#!iso:std:54533:en , *в России адаптирован как ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности»,* http://protect.gost.ru/v.aspx?control=8&id=176022), не имело бы смысла.

По этой причине наличие в организации системы менеджмента информационной безопасности сделано основным требованием при обеспечении соответствия стандарту ÖNORM A 7700-4. На это опираются все остальные требования, такие как:

- Соблюдение принципа минимизации;
- Выбор и поддержка языков программирования, платформ и других компонентов;
- Безопасная конфигурация и укрепление системы;
- Безопасное администрирование;
- Защита данных во время передачи и хранения;

- Настройка HTTP-заголовков для безопасности (HTTP Security Header);
- Протоколирование.

Как уже было сказано, это общие требования, которые определяют, что делать, а не как это делать. В стандарте отсутствуют какие-либо указания, связанные с конкретными технологиями. Если требуется всесторонний список общих требований в качестве отправной точки для процесса разработки требований или в качестве обязательных спецификаций для поставщиков, то ÖNORM A 7700-4:2019 как раз является подходящим документом. Чтобы сделать данный документ еще более практичным, мы дали ссылки на более детальные руководства, такие как «Критерии Центра интернет-безопасности CIS» (CIS Benchmarks, см. https://www.cisecurity.org/cis-benchmarks/) и технические руководства американского Национального института стандартов и технологий NIST и немецкого Федерального управления по безопасности информационных технологий (Bundesamt für Sicherheit in der Informationstechnik, BSI).

Прекращается сертификация на соответствие ÖNORM A 7700

Одно важное изменение связано с использованием нового ÖNORM A 7700:2019. Австрийский национальный орган по стандартизации решил не проводить сертификацию на соответствие новой версии. Поскольку старая версия стандарта полностью заменена новой, это означает, что больше не будет возможности получить новый сертификат соответствия австрийскому стандарту ÖNORM A 7700. Если вы являетесь счастливым обладателем действующего сертификата ÖNORM A 7700, берегите его - он может стать редкостью, представляющей интерес для коллекционеров)!

ИСО: ОБНОВЛЁН СТАНДАРТ СИСТЕМЫ МЕНЕДЖМЕНТА КАЧЕСТВА ISO 10015 ПО ВОПРОСАМ ОБУЧЕНИЯ И ПОВЫШЕНИЯ КВАЛИФИКАЦИИ КАДРОВ

Источник: сайт ИСО https://www.iso.org/standard/69459.html https://www.iso.org/obp/ui/#!iso:std:69459:en

В начале декабря сайт Международной организации по стандартизации (ИСО) сообщил о публикации новой редакции стандарта **ISO 10015:2019 «Менеджмент качества – Руководство по менеджменту компетенций и повышению квалификации кадров»** (Quality management – Guidelines for competence management and people development) объёмом 15 страниц, см.

https://www.iso.org/standard/69459.html и
https://www.iso.org/obp/ui/#!iso:std:69459:en .

Стандарт пришёл на смену действовавшему 20 лет документу ISO 10015:1999 «Менеджмент качества – Руководство по обучению» (Quality management – Guidelines for training, https://www.iso.org/standard/21231.html), который в России был адаптирован как ГОСТ Р ИСО 10015-2007 «Менеджмент организации. Руководящие указания по обучению», см. http://protect.gost.ru/v.aspx?control=8&baseC=6&id=165447

Во вводной части документа, в частности, сказано:

«Настоящий документ содержит рекомендации для организаций по созданию, внедрению, поддержанию и совершенствованию систем менеджмента компетенций и повышения квалификации персонала, с целью оказания положительного влияния на результаты, связанные с соответствием продуктов и услуг, а также с потребностями и ожиданиями соответствующих заинтересованных сторон.

Данный документ применим в организациях любого типа или размера. Он не добавляет, не изменяет и не модифицирует каким-либо иным образом требования стандартов семейства ISO 9000 или каких-либо иных стандартов.

Настоящий документ был подготовлен подкомитетом SC3 «Поддерживающие технологии» (Supporting technologies) технического комитета ИСО ТС176 «Менеджмент и обеспечение качества» (Quality management and quality assurance), в сотрудничестве с Техническим комитетом ИСО ТС260 «Управление кадровыми ресурсами» (Human resource management).

Настоящая вторая редакция отменяет и заменяет первую редакцию стандарта (ISO 10015:1999), которая была содержательно пересмотрена. Основные изменения по сравнению с предыдущей редакцией следующие:

- документ был реструктурирован с целью обеспечения лучшей согласованности со стандартами семейства ISO 9000;
- стандарт обновлён таким образом, чтобы поддержать те организации, которые планово, через установленные интервалы времени пересматривают свои потребности в компетенциях;
- вопросы менеджмента компетенций были дополнительно уточнены и разъяснены.»

Содержание документа следующее:

Предисловие

Введение

1. Область применения
2. Нормативные ссылки
3. Термины и определения
4. Менеджмент компетенций
5. Менеджмент компетенций и повышение квалификации персонала

Библиография

КИТАЙ: С ПЕРВОГО ЯНВАРЯ 2020 ГОДА ВСТУПАЮТ В СИЛУ НОВЫЕ «ПРАВИЛА АРХИВНОЙ РАБОТЫ В ВООРУЖЁННЫХ СИЛАХ»

Источник: сайт газеты «Дзефандзюнь бао» / сайт Всекитайского собрания народных представителей
http://news.cnwest.com/tianxia/a/2019/12/16/18275110.html
http://www.npc.gov.cn/npc/c30834/201912/3f6bc4d715b64e22a3c1e8905bc60310.shtml
http://military.workercn.cn/32817/201912/18/191218075136978.shtml

Председатель Центральной военной комиссии Си Цзыньпин (习近平, Xi Jinping) подписал приказ об утверждении пересмотренных **«Правил архивной работы в вооружённых силах»** (《军队档案条例》), которые вступили в силу с 1 января 2020 года (*одновременно перестали действовать правила 2004 года*).

Заново пересмотренные «Правила» придерживаются идей Си Цзиньпина о социализме с китайскими особенностями в новую эпоху и тщательно реализуют указания Си Цзиньпина об укреплении армии. В центре их внимания поддержка эффективного выполнении вооружёнными силами своей миссии в новую эпоху, их боеготовности, и также глубокое осознание особенностей архивно-документационной работы в вооружённых

силах в новую эпоху. «Правила» научно-обоснованным образом регламентируют основные задачи, разделение обязанностей, требования к управлению, систему работы, поддержку архивного строительства, надзор и инспекцию военных архивов.

Текст «Правил» доступен на сайте Всекитайского собрания народных представителей по адресу http://www.npc.gov.cn/npc/c30834/201912/3f6bc4d715b64e22a3c1e8905bc60310.shtml

Содержание новых «Правил» следующее:

- Глава I: Общие положения
- Глава II: Ответственность
- Глава III: Создание и управление архивами
- Глава IV: Архивные службы и использование архивов
- Глава V: Налаживание и обеспечение безопасности архивной работы
- Глава VI: Архивная работа в военное время
- Глава VII: Надзор, инспектирование, поощрения и взыскания
- Глава VIII: Вспомогательные положения

Документ в общей сложности содержит 8 глав и 66 статей, и он будет служить фундаментом архивно-документационной работу современной армии. «Правила» разъясняют обязанности органов управления архивным делом и подразделений, выполняющих профессиональную архивную работу на всех уровнях, служб делопроизводства и военнослужащих, внедряют систему ответственности за архивно-документационную работу, а также устанавливают порядок архивной работы с учётом деловых потребностей соответствующих подразделений.

«Правила» устанавливают типовой порядок работы с документами для всех военнослужащих; стандартизируют механизм работы архивов в военное время, упрощают процесс использования архивов и способствуют повышения уровня участия архивов в процессе боевой подготовки военных.

«Правила» разъясняют методы управления электронными архивами и способствуют их эффективности, а также стандартизируют обмен архивной информацией и использование сетевых сервисов.

Документ обобщает опыт работы военных архивов, усиливает положения о надзоре и управлении архивной работой, создаёт механизм оценки качества архивной работы, совершенствует меры поощрения и наказания, и в целом направлен на достижение целей архивной работы.

Мой комментарий: Впечатляет внимание первых лиц Китая к вопросам управления документами и архивного дела, равно как и подчёркнутое внимание к вопросам работы с электронными документами. Деятельность архивов связывается в первую очередь с поддержкой боевых действий и военно-политической подготовки армии, защитой прав и интересов военнослужащих, а не просто с сохранением истории.

В отдельно опубликованных комментариях к «Правилам» отмечается:

«С быстрым развитием информационных технологий в архивном деле всё больше применяются современные информационные технологии, такие как большие данные, блокчейн и искусственный интеллект. Деятельность военных архивов должна идти в ногу со временем и адаптироваться к требованиям построения «информационной» армии. Пересмотр нормативно-правовых актов направлен на то. чтобы вводить новшества и изменения на системном уровне и содействовать информатизации и трансформации работы военных архивов».

ЗМІСТ