ПЕРЕДМОВА

Випуск дайджесту присвячено проблемам використання електронних інформаційних технологій установами світу.

У публікації «Программно-аппаратный комплекс "Страховой фонд электронного архива"» розповідається про пропозицію корпорації ЕЛАР щодо створення програмно-апаратного комплексу "Страховий фонд електронного архіву"

У публікації «Комплексное оснащение лаборатории для создания страхового фонда документов» зазначено перелік законів Російської Федерації, які зобов'язують установи, що працюють з архівними документами, документами на об'єкти підвищеного ризику і об'єкти систем життєзабезпечення, створювати страховий фонд документації на основі мікрографічних носіїв. Наведено перелік комплектуючого обладнання.

У публікації «Обеспечение сохранности документов в процессе копирования» наведені переваги та недоліки різних методів копіювання.

У публікації «Компания Балтнет Tier 3 Дата Центр» розповідається про роботу компанії Baltneta з надання послуг дата-центру, Інтернету, технічного обслуговування IT та ін.

У публікації «Угрозы безопасности в облаке» наведено 9 головних загроз в хмарних послугах у 2013 році і методи захисту.

У публікації «Ассоциация ARMA International одобрила «Принципы управления информацией в здравоохранении»» розповідається про те, що авторитетна міжнародна асоціація ARMA International оголосила про свою підтримку «Принципів управління інформацією в охороні здоров'я».

У публікації «Международный совет архивов: Стратегический план действий на 2014-2018 годы» надано оцінку поточної ситуації в архівній галузі та намічені цілі на майбутнє.

У публікації «США: Потратив полмиллиарда долларов на оцифровку дел ФБР, не в состоянии отыскать их» розповідається, що введена в відомстві комп'ютеризована система управління слідчими справами сповільнила проведення розслідувань та роботу.

У публікації «Франция: Начато публичное обсуждение французской редакции европейского стандарта prEN 16790:2014 «Интегрированное управление борьбой с вредителями в целях защиты культурно-исторического наследия»» розповідається про розміщення на спеціальному сайті французького органу з стандартизації AFNOR проектів стандартів для обговорення.

У публікації «ИСО: Опубликован технический отчет по выбору электронных носителей для долговременного сохранения информации» розповідається про технічний звіт ISO / TR 17797: 2014 «Електронна архівація - Вибір електронних носіїв для довготривалого збереження інформації».

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС "СТРАХОВОЙ ФОНД ЭЛЕКТРОННОГО АРХИВА"

Источник: http://www.elar.ru/resheniya/arkhivy/strakhovoy_fond_dokumentov/programno_apparatnyy_kompleks_strakhovoy_fond_elektronnogo_arkhiva/

Корпорация ЭЛАР предлагает решения по созданию программно-аппаратного комплекса "Страховой фонд электронного архива".

Основными преимуществами страхового фонда являются:

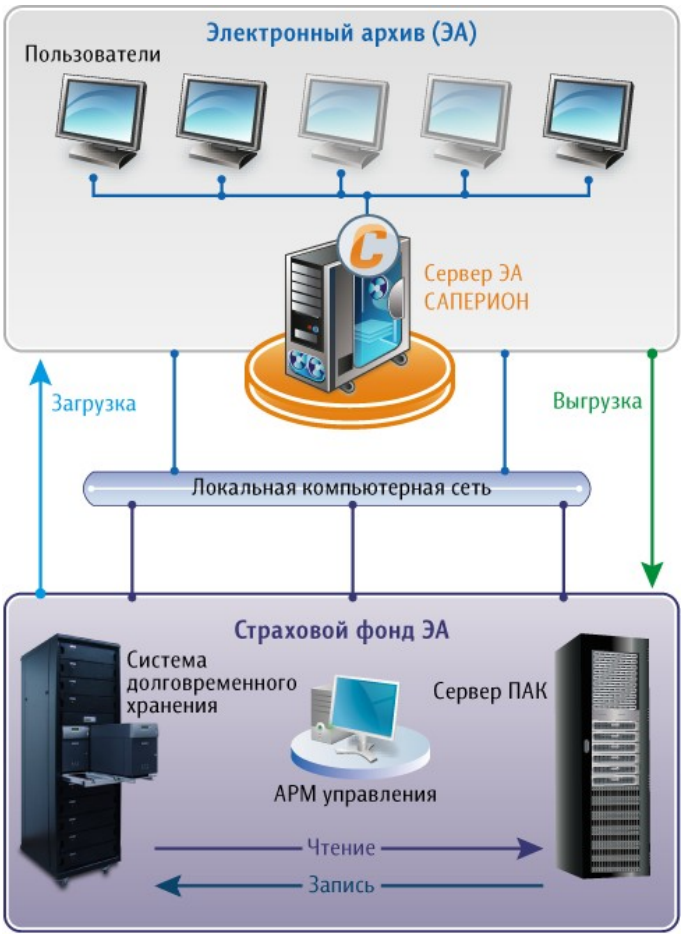
- Оптимальная технология для долговременного хранения;
- Гарантии работоспособности и долговечности носителя (свыше 50 лет) от производителей;
- Физическое исключение перезаписи информации (соответствие спецификации TRUE WORM);
- Низкая совокупная стоимость хранения документа за счет долговечности хранения и высокой ёмкости носителей.

В системе мер по обеспечению безопасности и сохранности документов электронного архива особое место занимает страховое копирование. Альтернативой сохранению резервных копий на основе ленточных накопителей является создание полноценного страхового фонда. Резервные копии предназначены для кратковременного хранения данных, тогда как страховой фонд — для длительного хранения. Существенным преимуществом страхового фонда в отличие от резервных копий является то, что информация в нем проиндексирована для удобства извлечения, тогда как резервные копии представляют собой записанные блоки данных, и осуществляется не полная перезапись, а актуализация: добавление новых или измененных документов за указанный период. Предлагаемое решение «Страховой фонд электронного архива» представляет собой программно-аппаратный комплекс, предназначенный для создания и пополнения страхового фонда документов, оперативного поиска архивных документов в страховом фонде в случае отключения программно-технических средств электронного архива или в иных чрезвычайных ситуациях.

Функциональные возможности и принцип работы комплекса

Комплекс предназначен для формирования и дальнейшей периодической актуализации страхового фонда архивных документов для электронного архива на базе программного обеспечения САПЕРИОН. Система электронного архива и программно-аппаратный комплекс функционируют независимо друг от друга. Передача данных осуществляется через промежуточный буфер, в который модуль выгрузки копирует документы и индексные данные из электронного архива для последующей загрузки в страховой фонд. Комплекс является автономным решением и не является составной частью программно-технических средств электронного архива.

Модуль выгрузки электронных архивных документов и их индексных данных из электронного архива в систему долговременного хранения на оптических дисках обеспечивает выгрузку индексных данных документов из БД электронного архива; формирование записей в БД модуля выгрузки с индексными данными документов; связку индексных данных документов с соответствующими электронными документами; проверку целостности файла с базой данных и файлов с электронными образами документов и распознанными текстами и последующую запись выгруженных документов на оптические носители системы долговременного хранения. Выгруженные из электронного архива документы хранятся в системе долговременного хранения в виде обычной файловой структуры. Для навигации по структуре используется встроенный в операционную систему Проводник, а для просмотра самих документов программное обеспечение, позволяющего просматривать электронные документы соответствующего формата.



Модуль загрузки используется при необходимости восстановления данных после отказа программно-аппаратного комплекса электронного архива данные из страховой фонда.

Состав комплекса

Программно-аппаратный комплекс состоит из следующих компонентов:

- Архивный роботизированный накопитель
- Специализированное программное обеспечение для управления роботизированными накопителями
- Модуль выгрузки документов из электронного

архива (первичной пакетной и регулярной)

- Модуль пакетной загрузки актуальных версий документов из страхового фонда в электронный архив
- Средства просмотра электронных архивных документов страхового фонда.

При внедрении программно-аппаратного комплекса производится первичная выгрузка документов из электронного архива. Для выгрузки новых или измененных документов за указанный период модуль выгрузки запускается по расписанию или администратором системы. Рациональная периодичность выгрузки устанавливается, исходя из критичности данных и объемов изменений.

КОМПЛЕКСНОЕ ОСНАЩЕНИЕ ЛАБОРАТОРИИ ДЛЯ СОЗДАНИЯ СТРАХОВОГО ФОНДА ДОКУМЕНТОВ

Источник:
http://www.elar.ru/resheniya/arkhivy/strakhovoy_fond_dokumentov/kompleksnoe_osnashchenie_laboratorii_dlya_sozdaniya_strakhovogo_fonda_dokumentov/

Создание страхового фонда стратегической информации и культурного наследия регламентируется различного рода постановлениями органов государственной власти:

- **Постановлением Правительства Российской Федерации №65** от 18.01.95 «О создании единого российского страхового фонда документации
- **Постановлением Правительства Российской Федерации №971** от 13.08.96 «Об обеспечении создания единого российского страхового фонда документации»
- **Постановление Правительства Республики Казахстан N 578** от 28 мая 2002 года Об утверждении Положения о Государственном страховом фонде копий документов
- **Законом Украины N 2310-IV (2310-15)** от 11.01.2005 «О страховом фонде документации»
- **Законом Республики Беларусь № 3277-XII** 6 октября 1994 г. «О Национальном архивном фонде и архивах в Республике Беларусь»
- **Законом Республики Узбекистан от N 768-I** 15.04.1999 Г. «Об Архивах».

Все вышеперечисленные законы обязывают учреждения, работающие с архивными документами, документами на объекты повышенного риска и объекты систем жизнеобеспечения, создавать страховой фонд документации

на основе микрографических носителей. Это обусловлено тем, что только микрографические носители являются единственным общепринятым стандартом долговременного хранения документации и позволяют гарантировать:

- **Сохранность оригинала** – более 500 лет (В архиве Германии есть микропленки, отснятые более 150 лет назад)
- **Невозможность изменения** информации на микроформе
- **Универсальный формат** (Микроформу можно легко посмотреть на любом оборудовании, изготовленном в любое время, используя обыкновенную лупу)
- **Высокая степень «сжатия» информации** (на одной микрофише А6 могут быть расположено до 420 документов снятые с уменьшением в 72х)

Благодаря всем вышеперечисленным свойствам микрографических носителей, в случае утраты бумажного оригинала, документы на микроформах могут быть признаны на правах подлинника.

Для обеспечения гарантии сохранности микроформ процесс микрофильмирования регламентируется международными и государственными стандартами (см. приложение 1.)

В состав микрографических лабораторий могут входить следующие модули:

- Модуль «Микрофильмирования» Микрофильмирования на 35 мм пленку»
- Модуль «Микрофиширования» Микрофильмирования на микрофиши DIN A6
- Модуль «Создания СФД (Страхового Фонда Документации)»
- Модуль «Создания ЭФП (Электронного Фонда Пользования)»

1. Типовая микрофильмирующая лаборатория начального уровня

Функционал лаборатории позволяет производить съемку документов до формата А0 на негативную галогенидосеребряную или цветную рулонную пленку шириной 35 мм. Проводить химико-фотографическую обработку отснятой пленки, а так же контролировать качество микрофильма соответствию стандартам ISO по следующим характеристикам – оптическая плотность (в денситометре), разрешение (с помощью микроскопа), резкость изображения и наличие дефектов (в читальном аппарате с большим экраном).

В состав решения входят:

- Микрофильмирующая камера PS 2002 R2-A0/A1 производства фирмы ProServ GmbH
- Процессор химико-фотографической обработки HT 105/51 BW производства фирмы Hostert Pro GmbH
- Читальный аппарат Indus 4601- 11
- Микроскоп 75х
- Денситометр X-Rite 301
- Стартовый комплект расходных материалов на 1 год (200 тыс. кадров)

- Пленка негативная 35 мм х 30 м Kodak Imagelink HQ 1461 – 250 рулонов
- Химические реактивы - проявитель (концентрат) Kodak – 20 литров
- Химические реактивы - фиксаж (концентрат) Kodak – 25 литров

2. Типовая микрофильмирующая лаборатория по созданию СФД и микрографического фонда пользования

Для создания СФД и микрографического фонда пользования к составу типовой микрофильмирующей лаборатории начального уровня **добавляется модуль «Фонд пользования»**, который позволяет создавать дубликаты микроформ для получения позитивных копий необходимых для создания фонда пользования.

Как правило, полученные копии распределяются следующим образом: мастер-микрофильм передается на хранение в Государственное Специальное Хранилище, одна копия остается на хранение в собственном архиве микроформ, остальные передаются заказчику. В соответствии со сроком хранения, страховые копии делают на серебросодержащей пленке, а пользовательские – на диазо или везикулярных пленках.

В состав микрофильмирующей лаборатории по созданию СФД и микрографического фонда пользования входят:

- Микрофильмирующая камера PS 2002 R2-A0/A1 производства фирмы ProServ GmbH
- Процессор химико-фотографической обработки HT 105/51 BW производства фирмы Hostert Pro GmbH
- Читальный аппарат Indus 4601- 11

- Микроскоп 75х
- Денситометр X-Rite 301
- Дубликатор Real RB-70
- Стартовый комплект расходных материалов на 1 год (200 тыс. кадров)
  - Пленка негативная 35 мм х 30 м Kodak Imagelink HQ 1461 – 250 роликов
  - Пленка позитивная 35 мм х 305 м Kodak Duplicating Microfilm 2462

для дуплицирования – 25 рулонов
  - Пленка прямого копирования 35 мм х 305 м Kodak Direct Duplicating Microfilm 2468 в рулонах для дуплицирования – 25 рулонов
  - Химические реактивы - проявитель (концентрат) Kodak – 45 литров
  - Химические реактивы - фиксаж (концентрат) Kodak – 55 литров

3. Типовая микрофильмирующая лаборатория по созданию СФД и ЭФП

Для создания электронного фонда пользования в состав Типовой микрофильмирующей лаборатории по созданию СФД **добавляется модуль «Создания ЭФП»,** который позволяет при помощи сканеров микроформ создавать электронные копии СФД для последующего создания электронного фонда пользования. При необходимости в состав комплекса может входить специализированное хранилище электронной информации на основе оптических роботизированных библиотек.

В состав микрофильмирующей лаборатории по созданию СФД и электронного фонда пользования фонда пользования входят:

- Микрофильмирующая камера PS 2002 R2-A0/A1 производства фирмы ProServ GmbH
- Процессор химико-фотографической обработки HT 105/51 BW производства фирмы Hostert Pro GmbH
- Читальный аппарат Indus 4601- 11
- Микроскоп 75x
- Денситометр X-Rite 301
- Дубликатор Real RB-70
- Сканер Kodak 2400/3000 DSV-E
- *(Опционально) Роботизированная оптическая библиотека ЭЛАР HCM BD 1000 + ПО Qstar HSM*
- Стартовый комплект расходных материалов на 1 год (200 тыс. кадров)
  - Пленка негативная 35 мм х 30 м Kodak Imagelink HQ 1461 – 250 рулонов
  - Пленка позитивная 35 мм х 305 м Kodak Duplicating Microfilm 2462

для дуплицирования – 25 рулонов
  - Химические реактивы – проявитель (концентрат) Kodak – 30 литров
  - Химические реактивы – фиксаж (концентрат) Kodak – 35 литров

4. Типовая лаборатория микрофиширования

Функционал лаборатории позволяет производить съемку документов до формата A0 на черно-белые или цветные микрофиши DIN A6. Проводить хим-фото-обработку отснятых микрофиш, а так же контролировать качество микрофильма соответствию стандартам ISO по следующим характеристикам: оптическая плотность (в денситометре), разрешение (с помощью микроскопа), резкость изображения и наличие дефектов (в читальном аппарате с большим экраном).

- Микрофильмирующая UKM-3

- Процессор химико-фотографической обработки HT 105/51 BW производства фирмы Hostert Pro GmbH (фишное исполнение)
- Читальный аппарат Indus 4601-11
- Микроскоп 75x
- Денситометр X-Rite 301
- Стартовый комплект расходных материалов на 1 год (200 тыс. кадров)
  - Микрофиши KODAK 1461,100 листов по 105 x148 mm – 25 пачек
  - Химические реактивы - проявитель (концентрат) Kodak – 20 литров
  - Химические реактивы - фиксаж (концентрат) Kodak – 20 литров
  - Конверты для микрофиш, лавсан по 1000 листов – 2 упаковки

Дополнительное оборудование

Лаборатории микрофильмирования могут комплектоваться дополнительным оборудованием:

- Шкафы для хранения микроформ
- Устройства ультразвуковой сварки пленок
- Монтажно- просмотровые столы
- Пост водоподготовки
- Системы регенерации серебра
- COM-системы
- И др.

Сервисное обслуживание и техподдержка

В корпорации «Электронный Архив» действует служба технической поддержки микрографического оборудования.

Наши специалисты осуществляют гарантийное, послегарантийное и сервисное сопровождение всего спектра микрографической техники

- Сервисное обслуживание поставляемого оборудования и технических средств. Инсталляция поставляемого оборудования
- Консультации по работе с оборудованием и программным обеспечением, обучение персонала
- Обеспечение бесперебойного функционирования отдельных устройств или комплексов

Заключение контрактов на сопровождение техники нашим сервисным центром является залогом бесперебойной работы дорогостоящих комплексов и защищает Ваши инвестиции. Кроме того, наличие такого договора дает Вам ряд преимуществ:

- Фиксированное время реакции на вызов
- Запланированные выезды специалистов для проведения ТО
- Резервирование запчастей на складе
- Консультирование по телефону

Приложение 1.

Международные стандарты, используемые при создании страхового фонда документации на основе микрографических носителей.

ISO 10594:2006,	Микрография. Системы микрофильмирующих аппаратов динамической съемки. Испытательная мира для проверки эксплуатационных характеристик
ISO 11962:2002	Микрография. Знак изображения (метка) на пленке для микрофотокопирования шириной 16 мм и 35 мм
ISO 11928-1:2000	Микрография. Контроль качества графических записывающих устройств COM. Часть 1. Характеристики испытательных рамок
ISO 18919:1999	Материалы регистрирующие. Микропленка на основе серебра, термически обработанная. Технические условия на устойчивость
ISO/TR 12654:1997	Электронная обработка изображений. Рекомендации для управления системами электронной записи для записи документов, которые могут понадобиться в качестве свидетельских показаний на оптических дисках WORM
ISO 6198:1993	Микрография. Считывающие устройства для прозрачных микроформ. Рабочие характеристики

ОБЕСПЕЧЕНИЕ СОХРАННОСТИ ДОКУМЕНТОВ В ПРОЦЕССЕ КОПИРОВАНИЯ

(по материалам Федерального центра консервации библиотечных фондов)

Автор: С. С. Пралькова, ведущий библиотекарь читального зала гуманитарной литературы, http://www.nbchr.ru/PDF/pralkova.pdf

Стремление библиотек хранить документы в виде различного вида копий вполне естественно и вызвано различными причинами:

- возможностью быстрого и значительного расширения доступа к информации;
- постоянной нехваткой площадей в хранилищах;
- недолговечностью бумаги, появившейся во второй половине 19 в. и распространившейся в 20 в.

Изготовление копий документов осуществляют методами фото-, микро-, ксерокопирования и использованием электронных технологий.

ГОСТ 7.48-2002. «СИБИД. Консервация документов. Термины и определения» дает следующие понятия: фотокопия – копия, изготовленная с помощью фотографического процесса; ксерокопия – копия, изготовленная с

помощью электрофотографического процесса; микрокопия – копия, изготовленная с уменьшением в 10 и более раз; электронная копия – копия, изготовленная в цифровой форме*.

Изготовление копий документов возможно данными методами не более одного раза.

Последующее копирование выполняют с копии. При копировании недопустимо механическое повреждение документов.

Преимущества и недостатки методов копирования

1. Ксерокопирование

Преимущества:

– быстрота и простота изготовления копии;

– для изготовления копии требуется только копировальный аппарат;

– сохраняется носитель и формат оригинала, формат копии легко изменить;

– дешевизна изготовления копии;

– предпочтение пользователей.

Недостатки:

– частичная утрата информации, особенно при копировании изображений (цветных рисунков, фотографий и т. д.);

– для хранения копии требуется дополнительное место;

– механическая нагрузка на переплет документа;

– интенсивное воздействие света и температуры.

2. Микрофильмирование

Преимущества:

– стабильность во времени (микрографические копии хранятся без изменения 100 и более лет и не подвержены воздействию электромагнитных полей);

– неизменность технологии (технология микрофильмирования является универсальной, и сегодня микрофильм, изготовленный десятки лет назад, может быть без ограничений использован в работе);

– малый физический объем хранения (практически большой архив можно свести к объему нескольких шкафов);

– юридическая правомочность (в большинстве стран, в том числе и в России, микрографический документ обладает юридической силой);

– низкая стоимость хранения информации.

* ГОСТ 7.48-90. СИБИД. Консервация документов. Основные термины и определения. – М., 1991.– С. 3.

Недостатки:

– низкая скорость обработки информации;

– большое время обслуживания пользователей;

– быстрый износ копий, особенно рабочих;

– механическая нагрузка на переплет документа;

– интенсивное воздействие света и температуры.

3. Электронная копия

Преимущества:

– высокая скорость обработки запросов пользователей и выдачи документов;

– удобство и быстрота копирования документа или его части;

– возможность циркулирования информации, как по локальным компьютерным сетям, так и в глобальной сети Internet и связанная с этим высокая скорость рассылки;

– простота организации ограничений доступа пользователей к информации и создание иерархических структур.

Недостатки:

– высокая степень подверженности внешним воздействиям, особенно электромагнитным полям;

– зависимость от источников электропитания;

– опасность со стороны разного рода компьютерных вирусов;

– возможность внесения изменений в документ (именно поэтому электронный документ не имеет юридической силы);

– частая смена технической и программной базы в мировом компьютерном производстве (во многих случаях приходится полностью менять оборудование, носители информации и переписывать весь фонд хранения);

– механическая нагрузка на переплет документа;

– интенсивное воздействие света и температуры.

При непрерывном копировании в течение 1 часа температура на поверхности документа может подняться на 5-6° С. Повышается температура и в помещении.

Основным методом копирования документов в большинстве библиотек являются ксерокопирование и сканирование.

Рекомендации по ксерокопированию документов

1. При ксерокопировании документов особое внимание должно уделяться переплетенным томам.

2. При ксерокопировании книг необходимо соблюдать следующие требования:

2.1. Содержать в чистоте стекло копировального аппарата;

2.2. Не давить на крышки и корешок переплета;

2.3. Аккуратно перелистывать страницы книги;

2.4. Не раскрывать книгу на 180°С, если переплет не позволяет это сделать или поврежден. Практически такие экземпляры ксерокопировать нельзя.

3. Не подлежат ксерокопированию рукописные памятники, издания уникальные, имеющие высокую культурно-историческую ценность или находящиеся в библиотеке в единственном экземпляре.

4. Для документов, перечисленных в п. 3, необходимо изготовление микрофильмов или цифровых копий с последующим изготовлением с них копий на бумаге.

5. Ксерокопирование документов, выполненных на бумаге, содержащей древесную массу, возможно с учетом их ценности, сохранности, количества экземпляров в библиотеке. Возможно однократное ксерокопирование единственного экземпляра при условии его хорошей сохранности.

Последующее ксерокопирование выполняется с этой копии. При плохой сохранности документа ксерокопирование недопустимо.

6. ВНИМАНИЕ! Недопустимо ксерокопирование документов с текстами и пометами, выполненными железо-галловыми чернилами. При ксерокопировании документов с текстом, выполненным анилиновыми чернилами или цветной типографской краской, следует учитывать сохранность, экземплярность, ценность документов. Решение о ксерокопировании в каждом случае принимается индивидуально.

Рекомендации по сканированию документов

1. Следует сортировать материал по типу и формату. Это значительно облегчает процесс ввода информации, и позволяет избегать частой смены настроек оборудования.

2. Документы должны быть распакованы и подготовлены в определенной зоне, предпочтительно в другой комнате, для того чтобы избежать образования пыли в зоне сканирования и на сканере.

3. Перед оцифровкой документа может возникнуть потребность в его стабилизации, очистке или каких-либо других работах, например, выравнивании. Однако такие работы должны выполняться только специалистом по консервации.

4. При перемещении документов из хранилища в зону оцифровки следует соблюдать аккуратность для минимизации изменений температуры и влажности. Если документы хранятся при низких температурах, то их акклиматизация обязательна.

5. При использовании цифровых камер следует осуществлять мониторинг света и генерации тепла для гарантии того, что условия окружающей среды не создают риска повреждения оригинала, т. к. в этом случае время экспозиции более длительное и весь объект освещается целиком. Источники освещения не должны располагаться близко к объекту до тех пор, пока не наступит реальный момент ввода информации. Время, в течение которого объект находится в освещенной зоне, должно быть сведено до минимума.

6. Установка для сканирования должна располагаться в отдельном помещении, не используемом для других целей, защищена от пыли. Пыль вредна не только для документа, но и влияет на качество сканирования.

7. Подложка для сканера должна быть сухой и чистой. Очистку рекомендуется проводить бумагой, смоченной раствором спирта.

8. Необходимо избегать в помещении попадания прямых солнечных лучей, т. к., во-первых, они вредны для документа, во-вторых, затрудняют проверку качества изображений на экране монитора.

9. Следует предусмотреть определенное количество чистого пространства на столе для размещения документов и их относительного легкого перемещения. Работа в ограниченном пространстве затруднительна и может привести к различным экстраординарным ситуациям.

10. Скорость сканирования – важный фактор не только с точки зрения производительности, но и сохранности документа.

11. Цифровые копии документов создают архивные коллекции, требующие постоянной поддержки. Условия для улучшения такой коллекции должны быть созданы в начале проекта. Это необходимо для избегания ситуации, когда цифровая коллекция может стать недоступной.

12. Работать с документом целесообразно в защитных перчатках.

Если сформулировать требования к идеальному съемочному приспособлению, то они таковы – отсутствие риска для книги, максимально приближенное к оригиналу воспроизведение текста или изображения. Следует учитывать и скорость съемки. Порядок приоритетов при переводе документов в цифровую форму следующий: сохранность оригинала, качество съемки, скорость съемки.

КОМПАНИЯ БАЛТНЕТ TIER 3 ДАТА ЦЕНТР

Источник: http://www.balt.net/kolokatsiya-v-tsod/infrastruktura/?gclid=CNWerdveq8ECFcICcwodmw0Ahg

Baltneta - самая инновационная компания информационных технологий и услуг передачи данных в Литве. Предоставляем комплексные услуги дата-центра, Интернета, технического обслуживания ИТ и телефонии для современного бизнеса.

Компания основана в 1996 году.

В чем наше отличие?

Компания Baltneta предоставляет своим клиентам комплексные решения из одного источника.

Будучи профессионалами в области ИТ и передачи данных, мы стремимся удовлетворять потребности не только бизнеса, но и работающих там людей. Каждый бизнес уникален, независимо от его размера и сферы деятельности. Поэтому каждая отдельная компания заслуживает индивидуальных, соответствующих ее бизнес-логике решений.

Нам доверяют и нашими услугами пользуются более четырех тысяч организаций в Литве и за рубежом.

Почему выбирают услуги наших Центров Обработки Данных?

- Удобное географическое расположение ЦОД в Европе (Литва, г. Вильнюс).
- Безопасность данных клиентов в ЦОД Евро Союза.
- Два собственных Центра Обработки Данных TIER3 и TIER2.
- Центры Обработки Данных – собственность Baltneta.
- Первый в Прибалтике и единственный сертифицированный ЦОД TIER3 в Литве.
- Опыт работы с 1996 г., более 130 сотрудников, 60 из которых инженеры.
- Многолетний опыт работы в области ЦОД и IAAS. Опыт работы в странах СНГ. Представительства в Москве, Минске и Киеве.
- Baltneta – единственный партнер VMware в Прибалтике, имеющий статус vCloud Powered. Статус vCloud Powered присваивается только партнерам с большим опытом в решениях облачных вычислений и имеющим уровень VMware Enterprise Service provider.
- Русскоязычная поддержка в круглосуточном режиме (24/7/365).
- Быстрый и надёжный канал связи до М9 в Москве (пинг ~24 мсек).
- Сертификаты ISO 20000, ISO 27000.

Baltneta владеет двумя Центрами Обработки Данных: один был запущен в конце августа 2012 г., данный ЦОД является первым и единственным в стране на сегодняшний день класса Tier 3 (максимальный Tier 4) по классификации Tia942, в 2007 г. в соответствии с максимальными требованиям стандартов безопасности был запущен второй Центр обработки класса Tier 2. Последний занимает 150м2 площади и в нем может быть размещено до 1500 серверов. В Дата Центре класса Tier 3 находится более 100 серверных шкафов, в которые можно разместить до 4400 серверов. Ниже представлена спецификация Дата Центра класса Tier 3.

Территория и здание

- Вся территория является собственностью компании Baltneta.
- На территории не осуществляется никакая другая деятельность.
- Расстояние от ограды до здания >15 м (согласно Tia 942 Tier 3 – мин. 9,8 м).
- Отдельный въезд, автостоянка для сотрудников и гостей.
- Въездные ворота контролируются с поста охраны.
- Здание готово выдерживать электромагнитные волны.
- Серверные помещения, помещения связи и электроснабжения оборудованы по принципу «здание в здании».
- В серверном помещении фальшпол (50 см).
- Фальшпол выдерживает статическую нагрузку 4 т/м2.
- Отдельные помещения для серверов, электроснабжения, связи.
- Доступ во внутренние помещения организуется с поста охраны.

Электричество

- На территории центра обработки данных установлены 2 новые трансформаторные. Общая мощность 3 МВт. Дублирование 2N.
- Дублирование блоков распределения электропитания 2N. Производство Schneider Electric.
- Дублирование автономных дизельных генераторов N+1. Общая мощность 2 МВт. Генераторы спроектированы выдерживать при полной нагрузке центра обработки данных 48 часов работы без дозаправки топливных баков. Производство Caterpillar.
- Источники непрерывного питания (UPS) APC Symmetra PX. Лучшие в своем классе UPS. Коэффициент эффективности 96 %. Модульное расширение. Простое обслуживание. Надежность. Элементы питания готовы снабжать электричеством работающий с полной нагрузкой центр обработки данных в течение 10 мин. Дублирование 2(N+1). Производство Schneider Electric (APC).
- В серверных шкафах устанавливаются блоки розеток (PDU), каждая розетка может управляться с удаленного расстояния (reboot/turnon/turnoff). Внедрен отдельный учет электричества в каждой розетке. Производство Schneider Electric (APC).

Охлаждение

- Решение для охлаждения серверных комнат типа IN-ROW. Решение обеспечивает стабильное охлаждение по всей высоте стойки с серверами. Простое расширение, легкая адаптация к растущей мощности ИТ-оборудования. Дублирование фанкойлов (англ. fan coil) 2N. Производство Schneider Electric (APC).
- Трубопровод охлаждения соединяет фанкойлы с охладителями (чиллерами) снаружи. Дублирование трубопровода 2N.
- Дублирование охладителей 2N. Вся система охлаждения находится под непрерывным наблюдением системы DCIM (Data Center Infrastructure management), которая не только дает оператору полное представление о текущих процессах, но также управляет оборудованием, обеспечивая тем самым непрерывную работу и стабильно низкое энергопотребление.
- Эффективность использования энергии (PUE) системы охлаждения составляет 1,12!
- Для IT-оборудования обеспечивается температура 21–25° С и поддерживается относительная влажность 45–55 %. Колебания температуры не превышают 5° С в час.

Сеть

- Для непрерывной связи с центром обработки данных через разные стены введены два оптических входа. Они присоединяются к магистральной сети Baltneta отдельными путями.
- В отдельных помещениях связи коммутированы отдельные входы.

- В центре обработки данных используется сетевое коммутационное оборудование Juniper и технология VirtualChassis, позволяющая объединить до 8 физических коммутаторов в один виртуальный, имея всего одну панель управления и мощность 8 коммутаторов. Центральный коммутатор имеет порты 40 Гбит для объединения и порты 10 Гбит для распределения. Распределенные коммутаторы имеют порты 10 Гбит для объединения и порты 1 Гбит для распределения.
- Сетевую маршрутизацию выполняют маршрутизаторы Brocade.
- В центр обработки данных разными путями подведено более 200 волокон (с расширением до 600 шт.) для прямого подключения к офисам клиентов.

Пожаротушение

- Автоматическое пожаротушение инертным газом (азот и аргон, 1:1).
- Все помещения оборудованы как отдельные зоны пожара.
- Дублирование баллонов 2N (возможность тушить пожар, пока наполняются израсходованные баллоны).
- Резервные баллоны – всегда включены в систему.
- Инертный газ безвреден для IT-оборудования.
- Оборудована система сброса давления.

Физическая охрана

- Помещения для серверов и инфраструктуры оборудованы по принципу «здание в здании».
- Наблюдение за территорией и помещениями осуществляется 36 видеокамерами.
- Вся территория и здания являются собственностью компании Baltneta – никаких арендаторов, никакой иной деятельности.
- Вооруженный сотрудник охраны дежурит 24 час. в сутки.
- Дополнительная бригада охраны приезжает в течение менее 10 мин.
- Авторизация на контрольно-пропускном пункте с помощью карточки и PIN-кода.
- На территорию допускаются только имеющие разрешение лица.
- Отдельные автостоянки для сотрудников и гостей.
- Центр обработки данных огражден от общественного пространства на расстоянии 15 метров.
- Отдельные зоны обслуживания (электричество, газ, связь) и коллокации.
- Детекторы открывания серверных шкафов.
- Регистрация вносимого и выносимого оборудования. Процедуры безопасности в соответствии с ISO 27000.

Серверные шкафы

- Серверные шкафы 42U APC AR3150 750 x 1070 мм.
- Перфорированные двери шкафов с замками.
- Все шкафы закрыты боковыми панелями.
- Шкафы устанавливаются в ряд, формируя «горячий» проход (англ. hot aisle).
- В «горячем» проходе оборудованы потолок и двери.
- Всего 96 шт. серверных шкафов и 12 шт. шкафов с коммутационным оборудованием.
- В каждый шкаф можно установить 4 шт. PDU.
- Дополнительно шкаф может быть снабжен детекторами открывания–закрывания, веб-камерами, датчиками удара и вибрации, мониторами, щетками для кабелирования.

Система DCIM

- Система DCIM (англ. Data Center Infratructure Management) обеспечивает мониторинг, сбор, управление данными, планирование ресурсов (англ. capacity management).
- Благодаря упреждающему мониторингу центра обработки данных удается избежать незапланированного простоя, обеспечивается равномерное расширение, мониторинг изменения микроклимата или электроснабжения.
- Система DCIM также дает возможность Клиенту подключаться к системе с помощью выделенных ему данных для подключения и просматривать изображение со встроенной в шкафу камеры, следить за электроснабжением и охлаждением серверов, энергопотреблением и проч.

Аренда площади в центре обработки данных

Поместите свой сервер в самом безопасном центре обработки данных!

Услуга аренды пространства в центре обработки данных (колокация серверов) предназначена для клиентов, которые уже имеют свои собственные серверы и хотят обеспечить бесперебойный доступ к этим серверам, разместив их в самом безопасном центре обработки данных в Литве. Перенесите свои серверы к нам, и мы позаботимся об электроэнергии, охлаждении, подключении к интернету, физической безопасности, застрахуем ваше оборудование, предложим дополнительные услуги, обеспечим и будем поддерживать оговоренный уровень качества оказания услуги (SLA). Мы предлагаем аренду общих серверных шкафов от 1U и аренду выделенных шкафов 42U.

✓Экономия	✓Безопасность	✓Рост
Во многих случаях аренда двух или нескольких шкафов более выгодна с финансовой точки зрения, чем собственная серверная комната.	Серверы, которые размещены в нашем центре обработки данных, защищены от наводнения, пожара, скачков напряжения, кражи или подобных угроз.	Расширяйте свою серверную инфраструктуру в том объеме, который необходим для вашего растущего бизнеса. Мы никогда не откажем в предоставлении любого объема нужных Вам ресурсов

Планы аренды площадей Дата Центра

	1U - Tier 3	**2U - Tier 3**	**42U - Tier 3**
Тип стоечного шкафа	Общий шкаф	Общий шкаф	Выделенный шкаф
Скорость выделенного интернет-канала	10 Mbps	10 Mbps	По необходимости
Количество портов коммутатора	1	1	По необходимости
Количество управляемых розеток	1	1	По необходимости
Услуга по установке (разовый платеж)	59 EUR	59 EUR	145 EUR
Цена (EUR, без НДС)	**55 EUR/мес.**	**69 EUR/мес.**	**от 546 EUR/мес.**

Центры обработки данных (ЦОД) распределяются по 4 категориям – Tier 1, Tier 2, Tier 3 ir Tier 4 (Tier 4 – наивысшая категория). Соответствие той или иной категории описывает уровень установленной технолгии резервации, решения физческой безопасности, особенности здания и территории. Официальное соответствие категории подтверждает Uptime Institute или TIA (Telecommunications Industry Association).

	Tier1	**Tier2**	**Tier3**	**Tier4**
Активное оборудование	N	N+1	N+1	2N
Распределенные потоков	1	1	2	2
Взожность ослуживания ЦОД без остановки	НЕТ	НЕТ	ДА	ДА
Годовой простой, час.	28,8	22	1,6	0,4
Пригодность инфраструктуры, %	99,671	99,749	99,982	99,995
Вероятность остановки в течении 5 лет, %	37,17	31,37	25,91	2,14

Tier 1: базовая серверная	*Tier 2: дублирование активного оборудования N+1*
Центр данных, соответствующий уровню Tier 1, не имеет никаких дублирующих активных компонентв и распределения потоков. Плановые работы возможны только при остановке ЦОД.	У ЦОД есть дополнительные копненты (N+1 резервация) активного оборудования (UPS, кондиционеры, сетевое оборудование) и только один поток распредления. Во время проведения профиактических работ ЦОД должен быть отключен.
Tier 3: возможность обслуживания ЦОД без остановки	***Tier 4: двойная инфроструктура***
Актное оборудование дублируется по приципу N+1. Дублируется распределение потоков: трубопроводы охлаждения, каналы связи в здание, электроинстоляция. Выполняя профилактические работы нет необходиости отключения ЦОД. Центр находится в отдельном выделенном здании, территория – огорожена.	Как активное оборудование, так и распределение потоков дублируются. ЦОД выдерживает непланированный отказ. Активное оборудование (UPS, кондиционеры, сетевое оборудование). Выделенное здание. ЦОД Tier 4 комерческой направленности в странах Балтии нет. Чаще всего он строится как выделенный ЦОД для большой корпорации или государственый ЦОД.

Особенность	**Tier 2**	**Tier 3**
Дублированные, не мене 20 метров друг от друга отдельные телекоммуникационные помещния	НЕТ	ДА
Дублированный каналов связи и IT оборудования Клиента	НЕТ	ДА
Минимальное расстояние от железной дороги или автосрады – 0,8 км, до аэропорта, водной среды – 0,4 км	НЕТ	ДА
Минимальное расстояние до общественной зоны – 9,8 метра	НЕТ	ДА
Отдельная автомбильная стоянка для работников и гостей на минимальном расстоянии 9,1 метра	НЕТ	ДА
Отдельный заезд на территорию для работников и гостей	НЕТ	ДА
Выделенное здание	НЕТ	ДА
Отдельные физические зоны для распаковки оборудования, настройки, охраны	НЕТ	ДА
Серверные комнаты от других помещений отделены стенами, выдерживающими огонь не менее 1 часа	НЕТ	ДА

Самые популярные ЦОД комерческой направленности – это Tier 2 и Tier 3. У Tier 1 отсутствуют уровни резервирования, а Tier 4 чаще всего является частным ЦОДом. Помимо уровней резервирования и пригодности, ЦОД'ы Tier 2 ir Tier 3 уровня различаются еще и наличием собственной территории, здания, других особенностей.

Стандартные планы

Подробнее о ценах

Windows SSD Linux SSD Windows HDD Linux HDD

	IaaS - 4 - SSD	**IaaS - 8 - SSD**	**IaaS - 16 - SSD**	**IaaS - 32 - SSD**	**IaaS - 64 - SSD**
Операционная система	Windows Server Datacenter	Windows Server Datacenter	Windows Server Datacenter	Windows Server Datacenter	Windows Server Datacenter
RAM	4 GB	8 GB	16 GB	32 GB	64 GB
vCPU	2 vCPU	4 vCPU	6 vCPU	8 vCPU	16 vCPU
Объем SSD	50 GB	100 GB	150 GB	200 GB	250 GB
Гарантированная производитель-ность SSD	500 IOPS	1000 IOPS	1500 IOPS	2000 IOPS	2500 IOPS
Резервные копии данных	Каждые 7 дней по 1 копии	Каждые 7 дней по 1 копии	Каждые 24 час. 3 копии	Каждые 24 час. 3 копии	Каждые 24 час. 3 копии
Скорость выделенного интернет-канала	10 Mbps	20 Mbps	40 Mbps	60 Mbps	80 Mbps
IP-адреса	5	5	8	8	16
Услуга по установке (разовый платеж)	89 EUR	89 EUR	89 EUR	89 EUR	89 EUR
Цена (EUR, без НДС)	**81 EUR/мес.**	**185 EUR/мес.**	**321 EUR/мес.**	**516 EUR/мес.**	**797 EUR/мес.**

Baltneta - самая инновационная компания информационных технологий и услуг передачи данных в Литве. Предоставляем комплексные услуги дата-центра, Интернета, технического обслуживания ИТ и телефонии для современного бизнеса.

Компания основана в 1996 году.

В чем наше отличие?

Компания Baltneta предоставляет своим клиентам комплексные решения из одного источника.

Будучи профессионалами в области ИТ и передачи данных, мы стремимся удовлетворять потребности не только бизнеса, но и работающих там людей. Каждый бизнес уникален, независимо от его размера и сферы деятельности. Поэтому каждая отдельная компания заслуживает индивидуальных, соответствующих ее бизнес-логике решений.

Нам доверяют и нашими услугами пользуются более четырех тысяч организаций в Литве и за рубежом.

Почему выбирают услуги наших Центров Обработки Данных?

- Удобное географическое расположение ЦОД в Европе (Литва, г. Вильнюс).
- Безопасность данных клиентов в ЦОД Евро Союза.
- Два собственных Центра Обработки Данных TIER3 и TIER2.
- Центры Обработки Данных – собственность Baltneta.
- Первый в Прибалтике и единственный сертифицированный ЦОД TIER3 в Литве.
- Опыт работы с 1996 г., более 130 сотрудников, 60 из которых инженеры.
- Многолетний опыт работы в области ЦОД и IAAS. Опыт работы в странах СНГ. Представительства в Москве, Минске и Киеве.
- Baltneta – единственный партнер VMware в Прибалтике, имеющий статус vCloud Powered. Статус vCloud Powered присваивается только партнерам с большим опытом в решениях облачных вычислений и имеющим уровень VMware Enterprise Service provider.
- Русскоязычная поддержка в круглосуточном режиме (24/7/365).
- Быстрый и надёжный канал связи до M9 в Москве (пинг ~24 мсек).
- Сертификаты ISO 20000, ISO 27000.

Характеристики услуги

Гарантированная связь с серверами

Бесперебойную работу серверов в центре обработки данных обеспечивают дублированные системы электроснабжения, охлаждения, доступа в Интернет.

Стандартная работа с серверами

Работать с серверами, размещенными на удаленной площадке в центре обработки данных, также комфортно, как если бы они находились локально в своем помещении.

Дополнительные услуги

Резервные копии и восстановление данных, аварийное восстановление, мониторинг сервера, услуга «удаленные руки» и др.

Управление удаленными серверами

Устройства IP KVM и управляемые розетки позволяют удаленно выполнять большинство заданий на серверах.

Неограниченный доступ к серверам

Клиентам центра обработки данных всегда предоставляется возможность в удобное для них время (24/7) выполнять работы, физически находясь около сервера.

Страхование оборудования клиента

Все клиентское ИТ-оборудование, размещенное в центре обработки данных, застраховано от любых возможных физических повреждений.

УГРОЗЫ БЕЗОПАСНОСТИ В ОБЛАКЕ

Источник: http://www.tadviser.ru/index.php

Cloud Security Alliance (CSA), некоммерческая отраслевая организация, продвигающая методы защиты в облаке, недавно обновила свой список главных угроз в отчете, озаглавленном «Облачное зло: 9 главных угроз в облачных услугах в 2013 году».

CSA указывает, что отчет отражает согласованное мнение экспертов о наиболее значительных угрозах безопасности в облаке и уделяет основное внимание угрозам, проистекающим из совместного использования общих облачных ресурсов и обращения к ним множества пользователей по требованию.

Опубликованный отчет имеет целью помочь пользователям облака и поставщикам облачных услуг внедрить лучшие стратегии снижения риска.

Итак, главные угрозы…

Кража данных

Кража конфиденциальной корпоративной информации - всегда страшит организации при любой ИТ-инфраструктуре, но облачная модель открывает «новые, значительные магистрали атак», указывает CSA. «Если база данных облака с множественной арендой не продумана должным образом, то изъян в приложении одного клиента может открыть взломщикам доступ к данным не только этого клиента, но и всех остальных пользователей облака», - предупреждает CSA.

Потеря данных

Данные, хранящиеся в облаке, могут быть украдены злоумышленниками или потеряны по другой причине, пишет CSA. Если

поставщик облачных услуг не внедрит должные меры резервного копирования, данные случайно может удалить сам провайдер или они пострадают при пожаре или стихийном бедствии. С другой стороны, заказчик, который шифрует данные до того, как выгрузить их в облако, вдруг потерявший шифровальный ключ, также утратит свои данные, добавляет CSA.

Кража аккаунтов / Взлом услуг

В облачной среде взломщик может использовать украденную регистрационную информацию, чтобы перехватывать, подделывать или выдавать искаженные данные перенаправлять пользователей на вредоносные сайты, пишет CSA. Организациям следует запретить раздачу своих регистрационных данных другим служащим и использование одних и тех же паролей для всех сервисов. Нужно также внедрить надежную, двухфакторную аутентификацию для снижения риска, рекомендует CSA.

Незащищенные интерфейсы и API

Слабые интерфейсы ПО или API, используемые заказчиками для управления и взаимодействия с облачными услугами, подвергают организацию целому ряду угроз, пишет CSA. Эти интерфейсы должны быть правильно спроектированы и обязательно включать аутентификацию, управление доступом и шифрование, чтобы обеспечить необходимую защиту и готовность облачных услуг.

CSA добавляет также, что организации и сторонние подрядчики часто используют облачные интерфейсы для предоставления дополнительных услуг, что делает их более сложными и увеличивает риск, поскольку может потребоваться, чтобы заказчик сообщил свои регистрационные данные такому подрядчику для упрощения предоставления услуг.

DoS-атаки

На облако могут быть предприняты атаки типа «отказ в обслуживании», которые вызывают перегрузку инфраструктуры, заставляя задействовать огромный объем системных ресурсов и не давая заказчикам пользоваться этой услугой. Внимание прессы чаще всего привлекают распределенные, или DDoS-атаки, но есть и другие типы DoS-атак, которые могут блокировать облачные вычисления, пишет CSA. К примеру, злоумышленники могут запустить асимметричные DoS-атаки прикладного уровня, используя уязвимости в Web-серверах, базах данных или других облачных ресурсах, чтобы завалить приложение с очень малой полезной нагрузкой.

Злонамеренный инсайдер

В среде IaaS, PaaS или SaaS, где не обеспечен должный уровень безопасности, инсайдер, имеющий неблаговидные намерения (например, системный администратор), может получить доступ к конфиденциальной информации, которая ему не предназначена, предупреждает CSA.

Системы, которые в обеспечении безопасности полагаются только на поставщика облачных услуг, подвергают себя большому риску, пишет CSA. «Даже если внедрено шифрование, если ключи не хранятся только у

заказчика, будучи доступны лишь на время пользования данными, то система всё еще подвержена злонамеренным действиям инсайдера», - указывает CSA.

Использование облачных ресурсов хакерами

Облачные вычисления дают возможность организациям любого размера задействовать огромную вычислительную мощь, но кто-то может захотеть сделать это с неблаговидными намерениями, предупреждает CSA. К примеру, хакер может использовать совокупную мощь серверов облака, чтобы взломать шифровальный ключ в считанные минуты.

Поставщики облачных услуг должны продумать, как они будут отслеживать людей, использующих мощь облачной инфраструктуры во вред, каким образом будут выявляться и предотвращаться такие злоупотребления, пишет CSA.

Недостаточная предусмотрительность

В погоне за снижением затрат и другими преимуществами облака некоторые организации спешат использовать облачные услуги, не понимая до конца все последствия этого шага, пишет CSA. Организации должны провести обширную, тщательную проверку своих внутренних систем и потенциального поставщика облака, чтобы полностью уяснить все риски, которым они себя подвергают, переходя на новую модель.

Смежная уязвимость

В любой модели облачной доставки существует угроза уязвимости через общие ресурсы, указывает CSA. Если ключевой компонент совместно используемой технологии - например, гипервизор или элемент общей платформы - будет взломан, то это подвергает риску не только пострадавшего заказчика: уязвимой становится вся среда облака.

2014: Ponemon: ИТ-подразделения проигрывают битву за безопасность в облаке

Большинство ИТ-организаций находятся в неведении относительно того, каким образом осуществляется защита корпоративных данных в облаке – в результате компании подвергают рискам учетные записи и конфиденциальную информацию своих пользователей. Таков лишь один из выводов недавнего исследования осени 2014 года, проведённого институтом Ponemon по заказу SafeNet. В рамках исследования, озаглавленного "Проблемы управления информацией в облаке: глобальное исследование безопасности данных", во всём мире было опрошено более 1800 специалистов по информационным технологиям и ИТ-безопасности.

В числе прочих выводов, исследование показало, что хотя организации всё активнее используют возможности облачных вычислений, ИТ-подразделения корпораций сталкиваются с проблемами при управлении данными и обеспечении их безопасности в облаке. Опрос показал, что лишь в 38% организаций четко определены роли и ответственности за обеспечение защиты конфиденциальной и другой чувствительной информации в облаке. Усугубляет ситуацию то, что 44% корпоративных данных, хранящихся в облачном окружении, неподконтрольны ИТ-подразделениям и не управляются ими. К тому же более двух третей (71%) респондентов

отметили, что сталкиваются с всё новыми сложностями при использовании традиционных механизмов и методик обеспечения безопасности для защиты конфиденциальных данных в облаке.

С ростом популярности облачных инфраструктур повышаются и риски утечек конфиденциальных данных Около двух третей опрошенных ИТ-специалистов (71%) подтвердили, что облачные вычисления сегодня имеют большое значение для корпораций, и более двух третей (78%) считают, что актуальность облачных вычислений сохранится и через два года. Кроме того, по оценкам респондентов около 33% всех потребностей их организаций в информационных технологиях и инфраструктуре обработки данных сегодня можно удовлетворить с помощью облачных ресурсов, а в течение следующих двух лет эта доля увеличится в среднем до 41%.

Однако большинство опрошенных (70%) соглашается, что соблюдать требования по сохранению конфиденциальности данных и их защите в облачном окружении становится всё сложнее. Кроме того, респонденты отмечают, что риску утечек более всего подвержены такие виды хранящихся в облаке корпоративных данных как адреса электронной почты, данные о потребителях и заказчиках и платежная информация.

Безопасность в облаке, теневые ИТ и потребность в более прозрачной отчетности

В среднем, внедрение более половины всех облачных сервисов на предприятиях осуществляется силами сторонних департаментов, а не корпоративными ИТ-отделами, и в среднем около 44% корпоративных данных, размещенных в облаке, не контролируется и не управляется ИТ-подразделениями. В результате этого, только 19% опрошенных могли заявить о своей уверенности в том, что знают обо всех облачных приложениях, платформах или инфраструктурных сервисах, используемых в настоящий момент в их организациях.

Наряду с отсутствием контроля за установкой и использованием облачных сервисов, среди опрошенных отсутствовало единое мнение относительно того, кто же на самом деле отвечает за безопасность данных, хранящихся в облаке. Тридцать пять процентов респондентов заявили, что ответственность разделяется между пользователями и поставщиками облачных сервисов, 33% считают, что ответственность целиком лежит на пользователях, и 32% считают, что за сохранность данных отвечает поставщик сервисов облачных вычислений.

Шифрование и многофакторная аутентификация как убедительная альтернатива традиционным средствам обеспечения безопасности данных

Более двух третей (71%) респондентов отметили, что защищать конфиденциальные данные пользователей, хранящиеся в облаке, с помощью традиционных средств и методов обеспечения безопасности становится всё сложнее, и около половины (48%) отмечают, что им становится всё сложнее контролировать или ограничивать для конечных пользователей доступ к облачным данным. В итоге более трети (34%) опрошенных ИТ-специалистов

заявили, что в их организациях уже внедрены корпоративные политики, требующие в качестве обязательного условия для работы с определёнными сервисами облачных вычислений применения таких механизмов обеспечения безопасности как шифрование. Семьдесят один (71) процент опрошенных отметили что возможность шифрования или токенизации конфиденциальных или иных чувствительных данных имеет для них большое значение, и 79% считают, что значимость этих технологий в течение ближайших двух лет будет повышаться.

Отвечая на вопрос, что именно предпринимается в их компаниях для защиты данных в облаке, 43% респондентов сказали, что в их организациях для передачи данных используются частные сети. Примерно две пятых (39%) респондентов сказали, что в их компаниях для защиты данных в облаке применяется шифрование, токенизация и иные криптографические средства. Еще 33% опрошенных не знают, какие решения для обеспечения безопасности внедрены в их организациях, и 29% сказали, что используют платные сервисы безопасности, предоставляемые их поставщиками услуг облачных вычислений.

Респонденты также считают, что управление корпоративными ключами шифрования имеет важное значение для обеспечения безопасности данных в облаке, учитывая возрастающее количество платформ для управления ключами и шифрования, используемых в их компаниях. В частности, 54% респондентов сказали, что их организации сохраняют контроль над ключами шифрования при хранении данных в облаке. Однако 45% опрошенных сказали, что хранят свои ключи шифрования в программном виде, там же, где хранятся и сами данные, и только 27% хранят ключи в более защищенных окружениях, например, на аппаратных устройствах.

Что касается доступа к данным, хранящимся в облаке, то шестьдесят восемь (68) процентов респондентов утверждают, что управлять учетными записями пользователей в условиях облачной инфраструктуры становится сложнее, при этом шестьдесят два (62) процента респондентов сказали, что их в организациях доступ к облаку предусмотрен и для третьих лиц. Примерно половина (46 процентов) опрошенных сказали, что в их компаниях используется многофакторная аутентификация для защиты доступа сторонних лиц к данным, хранящимся в облачном окружении. Примерно столько же (48 процентов) респондентов сказали, что в их компаниях применяются технологии многофакторной аутентификации в том числе и для защиты доступа своих сотрудников к облаку.

Основные рекомендации по обеспечению безопасности данных в облаке

- Роль ИТ-подразделений постепенно меняется: перед ними стоит задача приспособиться к новым реалиям облачных ИТ. ИТ-подразделения должны рассказывать сотрудникам о проблемах безопасности, разрабатывать комплексные политики по управлению данными и по соблюдению законодательных требований, разрабатывать рекомендации по внедрению

облачных сервисов и устанавливать правила относительно того, какие данные можно хранить в облаке, а какие – нет.

- ИТ-подразделения способны выполнить поставленную перед ними миссию по защите корпоративных данных и одновременно выступать в роли инструмента в реализации "Теневых ИТ", реализуя меры по обеспечению безопасности данных, например, внедряя подход `encryption-as-a-service` ("шифрование в виде сервиса"). Подобный подход позволяет ИТ-отделам централизованно управлять защитой данных в облаке, обеспечивая другим подразделениям компании возможность самостоятельно находить и пользоваться облачными сервисами по необходимости.
- По мере того, как всё больше компаний хранят свои данные в облаке, а их сотрудники всё активнее пользуются облачными сервисами, ИТ-подразделениям необходимо уделять больше внимания реализации более эффективных механизмов для контроля за пользовательским доступом, таких как многофакторная аутентификация. Это особенно актуально для компаний, которые обеспечивают третьим лицам и поставщикам доступ к своим данным в облаке. Решения многофакторной аутентификации могут управляться централизованно и обеспечивать более защищенный доступ ко всем приложениям и данным, где бы они ни размещались – в облаке, или на собственном оборудовании компании.

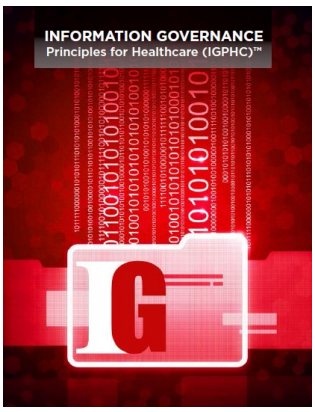
Использованы материалы: Марсия Сэвидж, CRN/США

АССОЦИАЦИЯ ARMA INTERNATIONAL ОДОБРИЛА «ПРИНЦИПЫ УПРАВЛЕНИЯ ИНФОРМАЦИЕЙ В ЗДРАВООХРАНЕНИИ»

Источник: http://rusrim.blogspot.com/2014/10/arma-international.html

Данная заметка была опубликована 2 октября 2014 года на сайте международной ассоциации специалистов по управлению документами и информацией ARMA International.

Авторитетная в области полномасштабного управления информацией (information governance), международная ассоциация ARMA International 2 октября 2014 года объявила о своей поддержке «Принципов управления информацией в здравоохранении» (Information Governance Principles for Healthcare, IGPHC™), разработанных Американской ассоциацией по управлению информацией в здравоохранении (American Health Information Management Association, AHIMA).



Этот документ объёмом 21 стр. можно скачать по адресу http://arma.org/docs/default-document-library/ig_principles-ahima.pdf

Как отмечается во введении в документ, ассоциация AHIMA привлекла лидеров и заинтересованные стороны из медицинской отрасли, а также экспертов в области управления информацией из других отраслей, для того, чтобы сформулировать Принципы IGPHC, адаптировав для этой цели «Общепринятые принципы делопроизводства» (Generally Accepted Recordkeeping Principles, GARP, *о них см.* http://rusrim.blogspot.ru/2009/06/arma-international-garp.html - *Н.Х.*) ассоциации ARMA International.

Ведущие эксперты ARMA International также приняли участие в разработке Принципов IGPHC: Президент ARMA International Фред Пульцелло (Fred Pulzello) и бывший президент ассоциации д-р Галина Дацковски (Galina Datskovsky) входили в состав консультативной экспертной группы AHIMA, отвечавшей за адаптацию GARP к потребностям членов ассоциации AHIMA.

«Мы гордимся тем, что наработки ассоциации ARMA International играют ключевую роль в усилиях по управлению информацией различных отраслей и секторов», подчеркнул президент ARMA Фред Пульцелло. «Наши «Общепринятые принципы делопроизводства» были созданы достаточно гибкими, что позволяет адаптировать их к конкретных условиям соответствующих отраслей, а также к уникальных особенностям деятельности конкретных организаций, связанным с их размером, сложностью структуры, ресурсами и законодательно-нормативной средой».

Ассоциация AHIMA отметила, что она опиралась на определения, данные фирмой Gartner и ассоциацией ARMA International, определяя «полномасштабное управление информацией» как «охватывающую всю организацию концепцию управления информацией на протяжении всего её жизненного цикла, поддерживающую стратегию организации, её оперативную деятельности, выполнение нормативно-правовых требований и требований, связанных с рисками и окружающей средой».

Как отмечается в документе, Принципы IGPHC предназначены для применения не только в отношении информации о здоровье, но и в отношении информации всех функциональных областей организаций,

работающих в сфере здравоохранения. «Внедрение этих принципов конкретной организацией отражает её стремление укрепить у себя управление информацией и повысить его эффективность в интересах своих пациентов, заинтересованных сторон, и общества в целом».

Мой комментарий: Как и GARP, IGPHC содержит те же 8 основных принципов (в слегка измененном порядке). Это принципы:

- Подотчетность;
- Прозрачность процессов и действий;
- Обеспечение целостности и аутентичности информации и документов;
- Защита информации и документов;
- Соблюдение требований законодательства и иных обязательных требований;
- Обеспечение возможности своевременного и эффективного доступа к информации;
- Сохранение документов и информации в течение установленных сроков хранения;
- Соответствующее требованиям и защищённое уничтожение либо передача на архивное хранение документов с истекшими сроками хранения;

МЕЖДУНАРОДНЫЙ СОВЕТ АРХИВОВ: СТРАТЕГИЧЕСКИЙ ПЛАН ДЕЙСТВИЙ НА 2014-2018 ГОДЫ

Источник: http://rusrim.blogspot.com/2014/10/2014-2018.html

14 октября 2014 года в испанском городе Жирона (Girona) в рамках ежегодной конференции прошло общее собрание (генеральная ассамблея) членов Международного совета архивов (МСА).

К общему собранию руководство МСА подготовило «Стратегический план действия МСА на 2014-2018 годы» (ICA Strategic Implementation Plan 2014-2018), в котором дана оценка текущей ситуации в архивной отрасти и намечены цели на будущее. Документ готовила рабочая группа, в состав которой входили уходящий президент МСА Мартин Берендсе (Martin Berendse), избранный новый президент Дэвид Фрикер (David Fricker), вице-президент по финансам Андреас Келлерхалс (Andreas Kellerhals), вице-президент по программным вопросам Анри Зубер (Henri Zuber), руководитель совета председателей секций МСА Дебора Дженкинс (Deborah Jenkins), координатор региональных отделений Брайан Корбетт (Bryan Corbett), президент секции профессиональных объединений и ассоциаций

архивистов и специалистов по управлению документами (SPA) Фред ван Кан (Fred van Kan), при поддержке секретариата МСА во главе с генеральным секретарем Дэвидом Лейтчем (David Leitch).

В документе отмечается, что в начале 21-го века кардинально изменились условия, в которых действует Международный совет архивов. По мнению авторов документа, глобализация, снявшая многие экономические и политические барьеры между нациями, привела к созданию единого огромного рынка для создания, обмена и использования информации. По мере снижения роли национальных государств всё больше решений, влияющих на повседневную практическую деятельность архивистов и специалистов по управлению документами, принимается на международном и региональном уровне:

- В политическом плане «открытое правительство», «большие данные» и программы обеспечения доступа к информации привели к тому, что архивы оказались в центре внимания политиков;
- Всё больше признаётся важность архивов с точки зрения защиты прав граждан;
- Сегодня, как никогда ранее, хрупок и противоречив баланс между правом на доступ к информации, интересами создателей документов (частных лиц, ассоциаций, частных компаний и государственных органов) и правом гражданина на неприкосновенность частной жизни;
- В дополнение к этому, население планеты продолжает расти. Усиливается конкуренция за доступ к ограниченным ресурсам, ведущая к политической нестабильности, которая увеличивает риски для архивов;
- Текущий кризис на Украине, гражданская война в Сирии, внутренние религиозные конфликты в западной и центральной Африке, этнические и племенные столкновения в Южном Судане, атаки террористов в Сомали создают политическую неопределенность, также угрожающую архивам;
- Многие страны серьёзно пострадали от рецессии, и бюджетные сокращения повлияли на деятельность многих национальных архивов.

Влияние информационных технологий и появления электронных документов

Технологические изменения, в том числе появление облачных вычислений и социальных сетей, способствуют созданию колоссальных объёмов информации, значительная часть которой вообще никак не управляется. Быстрое развитие в большинстве регионов мира информационного общества, в котором использование постоянно изменяющихся информационно-коммуникационных технологий стало обычным делом, имело и продолжает иметь далеко идущие последствия для специалистов в области управления документами и архивного дела.

Создание в поразительных масштабах изначально-электронных документов и массовая оцифровка архивных материалов, первоначально созданных в неэлектронных форматах, фундаментальным образом изменяют взаимоотношения как между архивами и создателями документов, так и

между архивами и их пользователями из числа представителей общественности:

- Необходимо, чтобы архивисты и специалисты по управлению документами привлекались в самом начале жизненного цикла информации, ещё до создания каких-либо документов, с тем, чтобы отобранные информационно-коммуникационные технологии обеспечивали аккуратное описание документов и ответственное управление ими;
- Решения относительно долговременной ценности архивных документов на основе экспертизы их ценности должны приниматься на гораздо более ранней стадии;
- Архивные учреждения являются окончательными хранителями архивных документов, имеющих непреходящую историческую ценность, и они будут продолжать нести за них ответственность и тогда, когда сами создатели документов уже прекратят своё существование;
- В то же время архивные учреждения должны решать задачу предоставления в онлайн-режиме растущих объёмов информации посредством оцифровки созданных на традиционных носителях архивных материалов, в условиях, когда непрерывно возрастают ожидания общественности в плане быстроты и эффективности получения информации;

Меняющиеся условия требуют от учреждений архивной отрасли гибкости и умения адаптироваться, а также устанавливать новые стандарты и приоритеты. Для того, чтобы справится с проблемами, встающими перед отраслью вследствие политических, экономических и технологических изменений, необходимо четко определиться с путями и приоритетами дальнейших действий.

Стратегические цели на 2014-2018 годы

Авторы документа считают, что МСА по-прежнему должен придерживаться свои миссии и видения, как они были сформулированы в стратегическом документе 2008 года:

«Видение: Благодаря усилиям Международного совета архивов, ключевые руководители национальных и международных организаций и мировая общественность осознают, что эффективное управление документами и архивами является важнейшей предпосылкой хорошего государственного управления, верховенства права, прозрачности администрирования, сохранения коллективной памяти человечества и обеспечения доступа граждан к информации».

На период 2014-2018 годов предлагается шесть сформулированных в Куала-Лумпуре стратегических целей сократить до трёх (а остальные три рассматривать как часть организационной деятельности). Эти цели следующие:

1. Позиционирование архивов как ключевого элемента для хорошего государственного управления, прозрачности и демократической подотчетности. Здесь нужно уделить внимание следующему:

- Повышение видимости архивной отрасли для принимающих решения лиц, потенциальных заинтересованных сторон и партнеров,

подчёркивание её важности для хорошего государственного управления, прозрачности административной деятельности и для демократической подотчётности;

- Подчёркивание (в сотрудничестве со специалистами других профессий, включая аудиторов, юристов, экономистов, ИТ-специалистов, и с компаниями-производителями программного обеспечения) роли важнейших документов в современном обществе;
- Подчёркивание (совместно с представителями других профессий) центральной роли архивов в сохранении культурно-исторического наследия различных сообществ;
- Активный поиск возможностей для участия в таких инициативах, как «Партнерство открытого правительства» (Open Government Partnership) и «Общество открытых знаний» (Open Knowledge Society);
- Четкая формулировка своей позиции по таким актуальным вопросам сегодняшнего дня, как защита и сохранение персональных данных, обеспечение доступа к информации и «большие данные».

2. Мониторинг и влияние на развитие и применение новых технологий, особенно в связи с проблемами обеспечения доступа к информации, защиты прав граждан и сохранения коллективной памяти, решение которых подразумевается в рамках управления архивами. Здесь нужно уделить внимание следующему:

- Внесение вклада в модернизацию архивной деятельности, способствуя использованию новых технологий, но при этом видя связанные с ними риски;
- Пропаганда и способствование внедрению решений, позволяющих справляться с проблемами и снижать риски, например, в таких вопросах, как обеспечение жизнеспособной электронной сохранности, надёжности и аутентичности и т.д.;
- Использование новых технологий для улучшения доступа к архивным материалам.

3. Создание в отрасли потенциала (особенно новых компетенций и навыков) позволяющего справиться с двойной проблемой управления как электронными документами, так и архивными материалами на традиционных носителях. Здесь нужно уделить внимание следующему:

- Хорошее управление;
- Управление электронными документами;
- Вопросы обеспечения долговременной сохранности;
- Вопросы доступа.

США: ПОТРАТИВ ПОЛМИЛЛИАРДА ДОЛЛАРОВ НА ОЦИФРОВКУ ДЕЛ ФБР, НЕ В СОСТОЯНИИ ОТЫСКАТЬ ИХ

Источник: http://rusrim.blogspot.com/2014/10/blog-post_13.html

Шкафы с документами в штаб-квартире ФБР /Фото: FBI

По данным внутреннего аудита ФБР, специальные агенты и технические специалисты ФБР считают, что впервые введенная в ведомстве компьютеризированная система управления следственными делами, разработка которой заняла десятилетие, замедлила проводимые ими расследования и их работу.

Компьютерное приложение «Страж» (Sentinel) было введено в эксплуатацию в 2012 году с целью облегчить поиск в делах как подсказок и улик, так и возможных взаимосвязей с другими текущими расследованиями. Ранее сотрудники ФБР обменивались информацией, утверждали документы и пополняли дела путем перемещения груд бумаг.

Согласно выпущенному 24 сентября 2014 года Генеральным инспектором ведомства (руководителем службы внутреннего аудита отчету (см. http://www.justice.gov/oig/reports/2014/a1431.pdf), большинство сотрудников считает, что данное программное обеспечение оказало «в целом положительное влияние на деятельность ФБР, укрепив способность ФБР выполнять свою миссию и осуществлять обмен информацией».

В то же время часть сотрудников, в том числе специальные агенты и технические специалисты, сообщили о том, что сохраняются связанные с новой системой причины для головной боли, такие как неэффективный поиск и обременительное индексирование.

Например, в отчете отмечается, что по мнению большинства специальных агентов, они теперь тратят больше времени на заполнение полей базы данных ради улучшения результатов поиска, и это «оставляет меньше времени для следственных действий». Процесс заполнения полей для

таких элементов, как дата рождения, псевдонимы и т.п. называется «индексированием».

Виновата глючная машина поиска

Согласно отчету, около 67% техников ФБР, отвечающих за хранение доказательств, их приём в хранилища и выдачу, считает, что «система «Страж» негативно повлияла на производительность их труда».

Индексирование и поиск, две ключевых функции системы, также раздражают и некоторых других сотрудников.

Только 42% опрошенных в процессе аудита сотрудников сказали, что они получают необходимые им результаты поиска. Проблема во многом связана с ошибками в работе фильтров машины поиска.

Как отметили представители службы аудита, «система «Страж» возвращала либо слишком большое количество результатов поиска для того, чтобы пользователи смогли их разумно проанализировать, либо вообще не выдавала никаких результатов при поиске документа, о существовании которого пользователь точно знал».

В общей массе опрошенных в ходе аудита сотрудников ФБР технические специалисты, занимающиеся хранением доказательств и электронным наблюдением, составляли небольшую часть, но при этом они представляют собой значительную часть пользователей системы. Многие из них тратят более 30 часов в неделю на работу в системе.

Теперь техникам по хранению доказательств приходится поддерживать два комплекта документации, отражающей переход доказательств из рук в руки - в бумажном и в электронном виде. Техникам приходится заполнять дела-дубликаты, так как «Страж» призван служить в качестве резервной системы на случай утраты или уничтожения бумажной документации.

Как отмечается в отчете, представители ФБР заверили аудиторов, что эффективность поиска в настоящее время повышается за счет «обучения, использования новых алгоритмов и других технических усовершенствований, позволяющих снизить частоту выдачи ложных позитивных и негативных результатов в ходе поиска».

Кроме того, ожидается, что в «Страже» версии 1.5 – это будет первая модернизация системы, проведение которой планируется на следующий месяц - будут улучшены другие функции, взаимосвязанные с поиском.

Вторая попытка оцифровки следственных дел: цена вопроса увеличивается

Это уже вторая попытка создания сетевой системы управления следственными делами ФБР. Первый проект создания системы под названием «Виртуальные следственные дела» (Virtual Case File) был начат в 2001 году, а в 2005 году ФБР махнуло на проект рукой, потеряв тем самым 170 миллионов долларов.

С момента ввода в эксплуатацию в 2012 году (см. http://www.nextgov.com/big-data/2012/07/after-decade-delays-fbi-agents-finally-get-case-management-system/57142/), бюджет системы «Страж» превысил запланированный на 100 млн. долларов, и в настоящее время система, как

ожидается, обойдётся в итоге в 551 млн. долларов. Увеличение обосновывается расходами на эксплуатацию и техническое обслуживание, а также на внедрение новых функциональных возможностей, разработанных в течение 2014 финансового года.

Однако, по мнению аудиторов, эффективно работающая система «Страж» могла бы реально сэкономить деньги в будущем.

«Если «Страж» версии 1.5 успешно поглотит ряд унаследованных систем и/или будет улучшена его интеграция с другими существующими системами, то ФБР должно получить экономию благодаря выводу из эксплуатации ряда систем и уменьшению усилий, затрачиваемых на поддержку в работоспособном состоянии других унаследованных систем», - говорится в отчете.

Реагируя на проект отчета, официальные лица ФБР признали наличие трудностей с поиском и индексированием, взяли на себя обязательство решить беспокоящие сотрудников проблемы.

Как отметил в своём письме от 12 сентября 2014 года помощник директора ФБР по инженерии информационных технологий Джеффри Джонсон (Jeffrey Johnson), «ФБР постарается наладить обратную связь от пользователей «Стража», обеспечивая, чтобы улучшения функциональных возможностей поиска эффективно отражали потребности пользователей».

Кроме того, по его словам, официальные лица ФБР изучат возможности для внесения технологических исправлений и пересмотра бизнес-процессов с тем, чтобы найти способы сокращения трудозатрат на индексирование больших неклассифицированных документов.

Представители ФБР не смогли сразу прокомментировать, на какой стадии сейчас находится процесс исправления отмеченных недостатков.

ФРАНЦИЯ: НАЧАТО ПУБЛИЧНОЕ ОБСУЖДЕНИЕ ФРАНЦУЗСКОЙ РЕДАКЦИИ ЕВРОПЕЙСКОГО СТАНДАРТА PREN 16790:2014 «ИНТЕГРИРОВАННОЕ УПРАВЛЕНИЕ БОРЬБОЙ С ВРЕДИТЕЛЯМИ В ЦЕЛЯХ ЗАЩИТЫ КУЛЬТУРНО-ИСТОРИЧЕСКОГО НАСЛЕДИЯ»

Источник: http://rusrim.blogspot.com/2014/10/pren-167902014.html

На специальном сайте французского органа по стандартизации AFNOR для обсуждения проектов стандартов 3 октября 2014 года был выложен для публичного обсуждения проект национальной адаптации европейского

стандарта **prEN 16790:2014 «Сохранение культурно-исторического наследия - Интегрированное управление борьбой с вредителями (IPM) в целях защиты культурно-исторического наследия»** (Conservation du patrimoine culturel — Gestion de lutte intégrée contre les nuisibles (IPM) pour la protection du patrimoine culturel, английское название Conservation of cultural heritage - Integrated pest management (IPM) for protection of cultural heritage) объёмом 34 страницы. Публичное обсуждение продлится до 15 декабря 2014 года.

Документу присвоено обозначение PR NF EN ISO 22313, его можно получить (при условии регистрации на сайте) на странице по адресу http://www.enquetes-publiques.afnor.org/construction-et-urbanisme/pr-nf-en-16790.html.

Как отмечается в аннотации, данный документ определяет принципы комплексной борьбы с вредителями и описывает процедурные, физические и практические методы профилактики, снижения масштабов заражения/загрязнения и обработки загрязнений материалов, относящихся к культурному наследию. Он призван обеспечить стандартизированный комплексный подход к управлению борьбой с вредителями для таких пользователей, как музеи, архивы, библиотеки, исторических здания, мест отправления культов, салоны продажи предметов искусства, аукционные дома и компании, занимающиеся перевозкой произведений искусства и оказывающие услуги коммерческого хранения. Стандарт применим в отношении коллекции, зданий, в которых они хранятся и к окружающей среде. Стандарт не распространяется на пещеры, сады и парки.

ИСО: ОПУБЛИКОВАН ТЕХНИЧЕСКИЙ ОТЧЕТ ПО ВЫБОРУ ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ ДЛЯ ДОЛГОВРЕМЕННОГО СОХРАНЕНИЯ ИНФОРМАЦИИ

Источник: http://rusrim.blogspot.com/2014/10/blog-post_62.html

23 сентября 2014 года Международная организация по стандартизации опубликовала технический отчет ISO/TR 17797:2014 «Электронная архивация – Выбор электронных носителей для долговременного сохранения информации» (Electronic archiving – Selection of digital storage media for long term preservation).

Документ объёмом 26 страниц был подготовлен техническим подкомитетом TC171/SC1. Его вводная часть доступна по адресу https://www.iso.org/obp/ui/#iso:std:iso:tr:17797:ed-1:v1:en .

Во введении в технический отчет отмечается следующее:

«Значительную часть электронной информации, создаваемой в ходе разного рода человеческой деятельности, необходимо сохранять в течение длительного периода времени, а в некоторых случаях – как можно дольше. В контексте данного Технического отчета термин «долговременное сохранение» означает срок хранения не менее ожидаемого срока службы носителя информации.

Используемые в настоящее время носители информации не изготавливались для этой цели, и их оценка с такой точки зрения не проводилась - в основном они разрабатывались с целью максимизировать скорость передачи информации, плотность её записи и сократить время доступа. В том случае, когда обеспечение долговременной сохранности является ключевым требованием и носитель используется не просто для записи резервных копий, все эти параметры должны рассматриваться в соответствующей перспективе.

В целом, существующие системы управления информацией не слишком способствуют удовлетворительному решению задачи обеспечения долговременной сохранности. Для целей долговременной сохранности нужно создавать специальные ресурсы и сложные процедуры, часто более дорогостоящие по сравнению с «нормальными» информационными системами (вследствие дублирования файлов, обновления носителей информации, резервирования оборудования, использования систем мониторинга, серьёзных усилий по техническому обслуживанию, частых и рискованных миграций, высокого потребления энергии и т.д.).

Даже в тех случаях, когда системы специально рассчитаны на обеспечение долговременной сохранности, следует принимать во внимание потребности в повседневном доступе и управлении хранимой электронной информации.

При проектировании систем для обеспечения долговременной сохранности, необходимо иметь конкретные методы отбора квалифицированных носителей информации по таким критериям, как надежность и стабильность; достигаемая тем самым жизнеспособность электронной информации позволит оптимизировать решения как в плане обеспечения сохранности, так и в плане доступности электронной информации.

В контексте требования об обеспечении долговременной сохранности электронной информации необходимо определить условия и рекомендации для специально производимых носителей информации, имеющих гарантированный потенциал стабильности и надежности.

Основные критерии, которые следует учесть при обеспечении долговременной сохранности электронной информации, можно сформулировать следующим образом:

- внутренняя стабильность носителя информации;
- стабильность физических и / или химических модификаций носителя, производимых в процессе записи информации;

- качество и надежность процесса записи;
- сохранение пути доступа к информации и метаданным;
- сохранение средств доступа (т.е. специального программного обеспечения, необходимого для использования тех электронных объектов, которые не были мигрированы в форматы, пригодные для долговременной сохранности или в стандартные форматы);
- качество информации (соблюдение спецификаций формата; целостность данных).

Только первые три критерия из данного списка рассматриваются в рамках данного Технического отчета.

Данный Технический отчет содержит рекомендации по выбору наиболее подходящих носителей для использования в решениях, обеспечивающих долговременную сохранность электронной информации. В отчете рассматриваются магнитные, оптические и «электронных» носители».

Содержание технического отчета следующее:

1 Область применения
2 Нормативные ссылки
3 Термины и определения
4 Методология
5 Выбор систем хранения / носителей информации
6 Жёсткий диск
7 Магнитная лента
8 Твердотельный диск (Solid state drive, SDD), флеш-память
9 Оптические диски (однократной записи и перезаписываемые)
10 Общие требования с обеспечения долговременной сохранности
11 Выбор носителей информации
Приложения: A. RAID и B. SMART

ЗМІСТ