ПЕРЕДМОВА

Випуск дайджесту присвячено проблемам використання мікрофільмів та електронних інформаційних технологій установами світу.

У публікації «Обеспечение доступности информации в системах современного документооборота» аналізуються переваги і недоліки зберігання документації за допомогою мікрографічних архівів. Розглянуті питання збереження якості інформації, яка сканується.

У публікації «Построение системы информационной безопасности предприятия» розглядаються наступні етапи побудови системи інформаційної безпеки підприємства: визначення цілей створення інформаційної безпеки, аналіз джерел проблем, ідентифікація вражень, оцінка ризику, ухвалення рішення.

У публікації «Недокументируемые особенности оборудования (Scanstation RS 150) и поставляемого с ним программного обеспечения» наведено результати вивчення технологічних можливостей сканера рулонних мікрофільмів Scanstation RS 150 фірми Wicks and Wilson (Великобританія).

У публікації «Разработка способа ускоренных испытаний качества и сохраняемости микрофильмов» наведено розроблений спосіб прискорених випробувань якості і прогнозування граничних термінів зберігання мікрофільмів із заданим рівнем збереження визначального параметра якості.

У публікації «Верховная Рада приняла закон о стандартизации» розповідається про нову редакцію закону, яка спрямована на формування і реалізацію державної політики у сфері стандартизації.

У публікації «Евросоюз вскоре обновит законодательство об электронных подписях» розповідається про проект нового закону Євросоюзу про електронний підпис.

У публікації «Открыто публичное обсуждение стратегического плана Международной организации по стандартизации на 2016-2020 годы» розповідається про проект плану стандартизації ІСО на 2016-2020 роки.

У публікації «Документ умер, да здравствует документ!» розповідається про погляди на питання – «Що таке документ?».

У публікації «Италия: Что обсуждают коллеги? Конференция DIG.Eat 2014» розповідається про питання електронного збереження, які було розглянуто на конференції.

У публікації «Проект Основ государственной культурной политики: Что говорится об архивах?» надано до обговорення проект «Основ державної культурної політики» Російської Федерації.

У публікації «Риски облачных вычислений: Сбой сервиса хранения данных отбросил назад исследовательские проекты» розповідається про наслідки технічного збою сервісу зберігання даних, компанії Socio Cultural Research Consultants, унаслідок чого багато дослідників втратили плоди великих зусиль, вкладених в наукові дослідження.

ОБЕСПЕЧЕНИЕ ДОСТУПНОСТИ ИНФОРМАЦИИ В СИСТЕМАХ СОВРЕМЕННОГО ДОКУМЕНТООБОРОТА

Авторы: А. К. Талалаев, д-р. техн. наук, проф., зав. кафедрой, О. В. Чечуга, канд. техн. наук, доц., Р. С. Череватый, канд. техн. наук, доц., (Россия, Тула, ТулГУ)

Анализируются преимущества и недостатки хранения документации с помощью микрографических архивов. Рассмотрены вопросы сохранения качества сканированной информации, построения поисковой системы, а также возможность использования композитных технологий.

Для целей фиксации информации, ее обмена и хранения используются различные носители:

- аналоговые (бумага, аудио- и видеоносители);
- цифровые (диски, оптические и магнитные устройства и т.д.).

С точки зрения использования информацию можно разделить на:

- оперативную (срок хранения до 1- 5 лет);
- среднесрочную (срок хранения от 5 до 75 лет);
- долговременную (срок хранения от 75 лет и, в идеале, неограниченно).

Основным носителем информации до сих пор является бумага, достоинствами которой являются:

- возможность использования без дополнительных технических средств;
- факсимильность;
- относительная дешевизна.

К недостаткам бумажного носителя можно отнести:

- потерю физических свойств с течением времени и в зависимости от условий хранения;
- большие площади, занимаемые под хранение документов;
- ручной поиск и трудности передачи информации по каналам связи.

Для целей сохранности бумажных документов в настоящее время используется технология микрофильмирования, которая позволяет:

- обеспечить сохранность информации до 300 - 500 лет, при условии соблюдения стандартов по съемке и хранению;
- сократить площади, занимаемые под хранение документации, в 10 – 20 раз;

использовать микрофильм в качестве подлинника при решении различного рода юридических вопросов (ГОСТ 13.1.101-93. «Микрофильм на правах подлинника»).

К недостаткам можно отнести трудности с оперативным доступом к информации на микрофильме и ее передачи по каналам связи.

В связи с бурным развитием средств вычислительной техники значительные объемы информации (базы данных, программные средства и др.) хранятся в электронной (цифровой) форме. Для хранения цифровой информации используются различного рода магнитные, магнитно-оптические, оптические и др. носители информации.

К преимуществам хранения информации в цифровой форме относятся:

- оперативный, многопользовательский доступ к информации по каналам связи;
- копирование информации без потери качества в каждом поколении копии;
- автоматическая индексация и поиск информации;
- возможность редактировать информацию с использованием компьютера.

К недостаткам можно отнести:

- неопределенность в сроках сохранности информации (по некоторым данным от 2…3 лет до 20…30 лет и более);
- большую стоимость оборудования и сетевой инфраструктуры, требующих специалистов для работы с ними;
- необходимость замены новыми продуктами и методами средств, процессов, программ для записи и хранения информации с регулярностью раз в 3…5 лет;
- трудности юридических аспектов использования цифровой информации.

Вопросы сохранности информации в настоящее время являются очень актуальными. По данным International Data Corporation и журнала «Document Management», в мире насчитывается более 8 млрд чертежей и только 15 % из них находится в CAD-формате (т.е. пригодны для работы в CAD-системах) (без учета данных по России).

Большие массивы документации хранятся на бумажных носителях в государственных архивах, архивах министерств и ведомств, хранилищах страхового фонда, библиотек, музеев, предприятий и т. д. Оценка хранимых объемов документации затруднительна (например, только в Российской национальной библиотеке хранится около 40 миллионов ед.).

В связи с тем, что для долговременного хранения документации в настоящее время основной остается технология микрофильмирования, большие объемы информации хранятся в виде микроформ.

Доступность информации определяется двумя факторами:

- возможностью найти источник хранения информации;
- возможностью доступа к соответствующему источнику.

В традиционной технологии с использованием бумажных носителей первую задачу решают различного рода каталоги и информационно-поисковые системы. Вторая задача решается путем поиска необходимого

документа в хранилище архива (библиотеки, организации) и выдачи его или его копии (на бумаге, микрофильме) потребителю.

Этой технологии присущи определенные недостатки:

- неоперативный доступ (off-line) к информации; длительное время поиска требуемого источника данных;

- упрощенный поисковый аппарат; значительные трудности при последующей обработке полученых данных с использованием вычислительной техники.

Современное состояние средств вычислительной техники позволяет устранить многие из вышеперечисленных недостатков, однако требует предварительного перевода документа в электронную форму и предъявляет определенные требования к качеству сканированного изображения документа.

С точки зрения качества изображения сканированного документа можно выделить три уровня представления.

1. Уровень просмотра, когда можно определить сущность хранимой информации, однако при этом может быть потеряно много мелких и важных деталей. Этот уровень характерен для работы на персональном компьютере в локальной сети учреждения или сети Интернет и характеризуется разрешением отображения 70…100 dpi с некоторой потерей полутонов (уровень разрешения стандартного монитора персонального компьютера). Основными ограничениями в этом случае являются объем и время передачи данных по сети (чем выше разрешение, тем больше объем файла изображения. Увеличение разрешения в 2 раза влечет увеличение файла в 4 раза).

2. Уровень детализации. Этот уровень характеризуется возможностью отображения большинства мелких деталей изображения и требует разрешения не менее 600 dpi, однако для большеформатных изданий (чертежи, газеты) может потребоваться разрешение более 600 dpi.

3. Уровень факсимильности. Этот уровень характеризуется адекватной передачей всех деталей документа и требует высокого разрешения и качества воспроизведения полутонов.

Сканирование документов с целью обеспечения возможности последующего использования и обработки средствами вычислительной техники дает на выходе изображение в растровой (цифровой) форме с качеством, соответствующим рассмотренному выше уровню детализации (в основном). Это позволяет осуществлять визуальный просмотр документа, хранение, обработку и передачу его по каналам связи. Существенными недостатками подобного способа представления информации являются:

- невысокое качество получаемого изображения;

- большие объемы получаемых данных;

- невозможность проводить поиск информации внутри файла изображения.

Для обеспечения возможности работы с текстовой информацией, хранящейся в файле изображения, необходимо осуществить ее выделение и преобразование в текстовую форму. Подобное преобразование осуществляется программами распознавания текста (программа оптического распознавания символов, или OCR).

В настоящее время существует широкая номенклатура систем OCR, обеспечивающих точность распознавания кириллических текстов до 99,5 % в зависимости от качества исходного изображения. Подобные системы требуют сканирования текстов с разрешением от 200 до 600 dpi, что определяется минимальным размером используемого в документе шрифта. В качестве примера подобных систем, хорошо зарекомендовавших себя на российском рынке, можно привести программу CuneiForm фирмы «Cognitive Technologies Ltd» (Россия), FineReader фирмы «Bit Software» (Россия). Преобразование цифрового изображения документа в текстовую форму позволяет проводить его просмотр и обработку широко распространенными стандартными текстовыми редакторами, а также выполнять поиск информации внутри такого документа с помощью различных поисковых систем.

Существующие поисковые системы условно можно разделить на следующие классы:

1. Построенные по классификационному принципу.
2. Использующие ключевые слова.
3. С возможностью полнотекстового поиска.
4. С использованием гипертекстовых ссылок.

Первый класс обеспечивает доступ к документации по строго регламентированным классификационным признакам, набор которых может варьироваться от системы к системе, но внутри каждой из них они фиксированы. Примером подобной системы может служить организация библиотечных фондов, архивов и т.п. Существенный недостаток – для успешного поиска документа необходимо знать все его классификационные признаки.

Поисковые системы второго класса позволяют искать информацию по комбинации признаков (ключевых слов), которые, по мнению составляющего запрос, содержатся в искомом документе (или группе документов). Ключевые слова в запросе могут объединяться с помощью операторов булевой алгебры. Ключевые слова могут быть заданы не полностью, что расширяет область поиска и особенно ценно в русских текстах. Основными достоинствами подобных систем являются компактность базы ключевых слов и высокая скорость поиска. Недостатки – необходимость предварительного создания базы ключевых слов и соответственно невысокая точность поиска.

В системах третьего класса поиск документа проводится путем задания в запросе «образцов» – слов, частей слов или целых понятий, которые ищутся в теле документа. Основные достоинства подобных систем – высокая

точность поиска и гибкость языка запросов. Недостатки – значительное время реакции системы и возможный высокий информационный «шум» в результатах поиска, а также необходимость наличия полных текстов документов в электронной форме (как следствие, высокая трудоемкость выделения текстов из бумажных документов, значительные объемы хранимой информации).

Поисковые (справочные) системы четвертого класса используются при построении энциклопедий, справочников, словарей. Особенно часто они стали использоваться при появлении мультимедийных энциклопедий на CD-ROM и широко применяются в сети Интернет. Они характеризуются возможностью гипертекстовых (надтекстовых) переходов между частями текста, связанными каким-либо общим понятием или признаком.

Достоинством систем четвертого класса является удобство использования. Недостатки: сложность организации гипертекстовых связей.

Особый интерес для применения в рассматриваемой области могут представлять так называемые двухконтурные информационно-поисковые системы, в которых функции поиска и хранения информации разделены.

Для поиска информации используются базы данных, организованные по одному или нескольким рассмотренным выше способам. Просмотр документов осуществляется с использованием второго контура, в котором хранятся факсимильные изображения документов. Второй контур может быть организован на базе средств микрографии или вычислительной техники, т.е. изображения документов могут быть замикрофильмированы или сканированы и записаны в архивы цифровых изображений на компьютерных носителях.

Перспективно использование композитных технологий, когда долговременное хранение документов организовано средствами микрографии, а для оперативного доступа и обработки информации используются электронные архивы цифровых изображений.

ПОСТРОЕНИЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Авторы: В. А. Селищев, канд. техн. наук, доц., О. В. Чечуга, канд. техн. наук, доц., М. Н. Наседкин, канд. техн. наук, доц., (Россия, Тула, ТулГУ)

Рассматриваются следующие этапы построения системы информационной безопасности предприятия: определение целей создания информационной безопасности, анализ источников проблем, идентификация уязвимостей, оценка рисков, принятие решения.

Определение целей создания информационной безопасности

Специалисты в области защиты информации в своей практике сталкиваются с решением большого количества вопросов, самым первым из которых является определение цели. Можно попытаться при помощи руководства и работников организации понять, что же на самом деле нужно защищать и от кого. С этого момента начинается специфическая деятельность на стыке технологий и основного бизнеса, которая состоит в определении того направления деятельности и (если возможно) целевого состояния обеспечения информационной безопасности (ИБ), которое будет сформулировано одновременно и в бизнес-терминах, и в терминах ИБ. В этом аспекте процесс анализа рисков является хорошо зарекомендовавшим себя инструментом, с помощью которого можно определить цели построения ИБ, оценить основные критичные факторы, негативно влияющие на ключевые бизнес-процессы компании, и выработать осознанные, эффективные и обоснованные решения для их контроля или минимизации.

Цель построения ИБ заключается в сохранении конфиденциальности, целостности и доступности информации. Вопрос только в том, какую именно информацию необходимо охранять и какие усилия прилагать для обеспечения ее сохранности.

Анализ источников проблем

После определения целей создания ИБ следует проанализировать проблемы, которые мешают приблизиться к целевому состоянию. На этом уровне процесс анализа рисков спускается до информационной инфраструктуры и традиционных понятий ИБ -злоумышленников, угроз и уязвимостей.

Построение модели злоумышленника

В процессе анализа рисков необходимо оценить мотивированность злоумышленников при реализации угроз. При этом под злоумышленником подразумевается не абстрактный внешний хакер или инсайдер, а сторона, заинтересованная в получении выгоды путем нарушения безопасности актива.

Первоначальную информацию о модели злоумышленника, как и в случае с выбором изначальных направлений деятельности по обеспечению ИБ, целесообразно получить у высшего менеджмента, представляющего себе положение организации на рынке, имеющего сведения о конкурентах и о том, каких методов воздействия можно от них ожидать. Сведения, необходимые для разработки модели злоумышленника, можно получить и из специализированных исследований по нарушениям в области компьютерной безопасности в той сфере бизнеса, для которой проводится анализ рисков. Правильно проработанная модель злоумышленника дополняет цели обеспечения ИБ, определенные при оценке активов организации.

Построение модели угроз

Разработка модели угроз и идентификация уязвимостей неразрывно связаны с инвентаризацией окружения информационных активов

организации. Сама собой информация не хранится и не обрабатывается. Доступ к ней обеспечивается при помощи информационной инфраструктуры, автоматизирующей бизнес-процессы организации. Важно понять, как информационная инфраструктура и информационные активы организации связаны между собой. С позиции управления ИБ значимость информационной инфраструктуры может быть установлена только после определения связи между информационными активами и инфраструктурой. В том случае, если процессы поддержания и эксплуатации информационной инфраструктуры в организации регламентированы и прозрачны, сбор информации, необходимый для идентификации угроз и оценки уязвимостей, значительно упрощается.

В модель угроз следует включить все угрозы, выявленные по результатам смежных процессов функционирования ИБ, таких как, управление уязвимостями и инцидентами. Нужно помнить, что угрозы необходимо будет ранжировать друг относительно друга по уровню вероятности их реализации. Для этого в процессе разработки модели угроз для каждой угрозы необходимо указать наиболее значимые факторы, существование которых оказывает влияние на ее реализацию.

На этапе построения модели угроз следует обратить внимание на рекомендации имеющих большой опыт работы в этой области организаций, например британского МВД, НИЦ «Охрана» и т.д.

Приведем классификацию угроз в рекомендациях британского МВД:

Класс 1 – низкий риск. Для объектов, на которых вероятный преступник мало знаком с охранными системами. В частности, такое предположение характерно для объектов с незначительной стоимостью хранящегося там товара, без ценных в глазах преступников товаров, и не несущие угрозы безопасности для окружающих людей.

Класс 2 – риск средний низкий. Для объектов, на которых вероятный преступник предполагается с некоторым знанием охранных систем, но лишь с обычными инструментами широкого применения. Такое предположение характерно для объектов со средним объемом ценностей.

Класс 3 – риск средний высокий. Для объектов со значительным объемом ценностей, наркотическими веществами или объектов, представляющих угрозу для окружающих людей. Предполагаемый преступник оснащен всеми необходимыми инструментами и портативным электронным оборудованием.

Класс 4 – риск высокий. Для объектов с особо высоким объемом ценностей или с особо высоким уровнем риска для окружающего населения. Предполагаемый преступник считается тщательно подготовившимся, имеющим знания об охранной системе на этом объекте и имеющим образцы оборудования, аналогичного установленному на объекте.

Аналогом британских рекомендаций в нашей стране являются ведомственные Р (рекомендации) и РД (руководящие документы), выпускаемые НИЦ «Охрана» и другими организациями.

РД 78. 36.003-2002 «Технические средства охраны, требования и нормы проектирования по защите объектов от преступных посягательств» вводит аналогичную классификацию объектов на 4 группы – А1 (особо важные объекты высокой ценности или высокой опасности), А2 (собственно наиболее опасные помещения на этих объектах), Б1 (объекты розничной торговли и т. д.), Б2 (объекты категории Б, содержащие алкогольную продукцию или наиболее компактные легкосбываемые товары – электронику, товары повседневного спроса).

Р 78.36.002-99 «Выбор и применение телевизионных систем видеоконтроля» добавляет специфики. В частности, в нем вводится собственная классификация объектов на три группы: А (особо важные), Б (существенный ущерб) и В (прочие).

Уже несколько лет мы живем по новому закону о техрегулировании, согласно которому ГОСТы, как и любые стандарты предприятий или общественных организаций, сами по себе не являются обязательными.

Обязательными являются лишь техрегламенты, которые принимаются только по основным вопросам безопасности. Например, экологической безопасности, безопасности дорожного движения и т. д. В области противокриминальной защиты также предполагается технический регламент, в первую очередь описывающий классификацию объектов в зависимости от предполагаемых угроз, а затем уже рекомендующий разные уровни защиты в зависимости от уровня угрозы. Основные положения:

«В зависимости от степени потенциальной опасности, а также возможных последствий в случае реализации криминальных угроз объекты, их помещения и территории подразделяются на три основные группы:

- критически важные и потенциально опасные объекты;
- социально значимые объекты;
- объекты сосредоточения материальных ценностей.

Кроме того, в зависимости от вида и размеров ущерба, который может быть нанесен объекту, находящимся на нём людям и имуществу в случае реализации криминальных угроз все объекты подразделяются на следующие классы:

- Класс I (высокая значимость) – ущерб в результате реализации криминальных угроз приобретет федеральный или межрегиональный масштаб;
- Класс II (средняя значимость) – ущерб в результате реализации криминальных угроз приобретет региональный или межмуниципальный масштаб;
- Класс III (низкая значимость) – ущерб в результате реализации криминальных угроз приобретет муниципальный или локальный масштаб.

В зависимости от класса объекта и вида находящегося (хранящегося) на нем имущества устанавливают классы защиты объектов».

От результатов актуализации модели угроз зависят состав и стоимость работ по защите информации. Модель угроз создается не исходя из своего

опыта и здравого смысла, а на основании базовой модели, утвержденной ФСТЭК и по методике того же ведомства. От того, типовая у вас система или специальная, какие требования вы к ней выдвигаете, зависит, какие конкретно средства защиты придется использовать для обеспечения безопасности.

Идентификация уязвимостей

Соответственно после разработки модели угроз необходимо идентифицировать уязвимости в окружении активов. Идентификация и оценка уязвимостей может выполняться в рамках еще одного процесса управления ИБ -аудита. Для проведения аудита ИБ необходимо разработать критерии, которые могут быть разработаны на основании модели угроз и модели злоумышленника.

По результатам разработки модели угроз, модели злоумышленника и идентификации уязвимостей можно говорить о том, что определены причины, влияющие на достижение целевого состояния информационной безопасности организации.

Оценка рисков

Полученные результаты необходимо оценить, агрегировать, классифицировать и отобразить. Так как ущерб определяется на этапе идентификации и оценки активов, необходимо оценить вероятность событий риска. Как и в случае с оценкой активов, оценку вероятности можно получить на основании статистики по инцидентам, причины которых совпадают с рассматриваемыми угрозами ИБ, либо методом прогнозирования – на основании взвешивания факторов, соответствующих разработанной модели угроз.

Хорошей практикой для оценки вероятности станет классификация уязвимостей по выделенному набору факторов, характеризующих простоту эксплуатации уязвимостей. Прогнозирование вероятности угроз проводится уже на основании свойств уязвимости и групп злоумышленников, от которых исходят угрозы.

В процессе идентификации и оценки уязвимостей очень важен экспертный опыт специалистов по ИБ, выполняющих оценку рисков, и используемые статистические материалы и отчеты по уязвимостям и угрозам в области информационной безопасности.

Величину (уровень) риска следует определить для всех идентифицированных и соответствующих друг другу наборов «актив-угроза». При этом величина ущерба и вероятности не обязательно должны быть выражены в абсолютных денежных показателях и процентах; более того, как правило, представить результаты в такой форме не удается. Причина этого – используемые методы анализа и оценки рисков информационной безопасности: сценарный анализ и прогнозирование.

Очень важный вопрос – политика управления рисками организации

Политика задает правила обработки рисков. Например, в политике может быть сказано, что риски потери репутации следует снижать в первую очередь, а снижение рисков средней значимости, не подтвержденных инцидентами ИБ, откладывается на конец очереди. Политику управления рисками может определять подразделение, занимающееся корпоративным управлением рисками.

Политика обработки рисков может пояснять вопросы страхования рисков и реструктуризации деятельности в том случае, если потенциальные риски превышают приемлемый уровень. Если политика не определена, то последовательность работ по снижению рисков должна базироваться на принципе максимальной эффективности, но определять ее все равно должно высшее руководство.

Принятие решения

На основе полученных результатов следует разработать простой и наглядный отчет об анализе рисков, основной целью которого будет презентация собранной информации о значимости и структуре рисков ИБ в организации. Отчет следует представить высшему руководству организации.

Распространенная ошибка состоит в том, что вместо выводов высшему руководству представляют промежуточные результаты. Несомненно, все выводы должны быть подтверждены аргументами к отчету необходимо приложить все промежуточные выкладки.

Для наглядности отчета риски необходимо классифицировать в привычных для организации бизнес-терминах, сходные риски – агрегировать. В целом классификация рисков может быть многогранной.

С одной стороны, речь идет о рисках информационной безопасности, с другой – о рисках ущерба для репутации или потери клиента. Классифицированные риски необходимо ранжировать по вероятности их возникновения и по значимости для организации.

Отчет об анализе рисков отражает следующие сведения:

- наиболее проблемные области обеспечения ИБ в организации;
- влияние угроз ИБ на общую структуру рисков организации;
- первоочередные направления деятельности отдела ИБ по повышению эффективности обеспечения ИБ.

На основании отчета об анализе рисков руководитель отдела ИБ может разработать план работы отдела на среднесрочный период и заложить бюджет исходя из характера мероприятий, необходимых для снижения рисков.

В процессе создания систем информационной безопасности предприятия особое внимание необходимо уделять автоматизированным системам обработки персональных данных согласно Федеральному закону Российской Федерации № 152-ФЗ «О персональных данных» (от 27 июля 2006 года), в котором определены общие требования безопасности. Защитные механизмы в значительной степени уточнены в постановлении Правительства 2007 г. №

781. А конкретные требования по нейтрализации выявленных угроз безопасности и конкретные функциональные требования к защитным механизмам определяются после классификации системы и актуализации модели угроз на основании методических документов ФСТЭК и ФСБ.

Необходимо подчеркнуть, что требований этих достаточно много, и они весьма жесткие. Так, для информационных систем персональных данных (ИСПД) класса 2 они в основном (но не полностью) повторяют требования по предотвращению несанкционированного доступа для многопользовательских автоматизированных систем класса 1Г, а для ИСПД класса 1 – для АС класса 1В. Выдвигаются и дополнительные требования, которых в руководящих документах ФСТЭК ранее не было, например по уровню защищенности межсетевых экранов, функциональности систем выявления вторжений, противодействия программно-математическим воздействиям и др.

Конкретные механизмы защиты и их функционал в рамках данной статьи рассмотреть не представляется возможным, но необходимо отметить, что обладатели информационных систем класса 1 и 2 должны будут впоследствии провести валидацию выполнения требований путем аттестации или сертификации ИСПД, так что уклонение от реализации каких-либо из предъявляемых требований будет чревато проблемами при проведении аттестационных испытаний.

Важно понимать, что в силу изложенных причин защищать придется всю информационную систему предприятия или, в лучшем случае, сегменты, разграниченные сертифицированными межсетевыми экранами.

Строить подсистему безопасности необходимо не с нуля, а интегрируя в существующую систему дополнительные средства защиты, что существенно усложняет задачу как проектирования, так и внедрения. Для функционирования защитных механизмов могут потребоваться дополнительные вычислительные мощности, более высокая пропускная способность сетевого оборудования и каналов передачи данных, мониторинг и обслуживание новых подсистем и средств.

Заключение

Создание систем информационной безопасности предприятия – длительная, затратная и сложная работа, требующая специальных знаний и навыков, материальных средств и подготовленных специалистов. В этих условиях неизбежно возрастает значение аутсорсинга информационной системы как при проектировании и вводе в эксплуатацию средств и систем защиты информации, так и на этапе ее сопровождения, в том числе с использованием современных средств, например центров управления безопасностью (SOC).

Анализ рисков, управление инцидентами и аудит ИБ неразрывно связаны друг с другом, поскольку связаны входы и выходы выше перечисленных процессов. Разработку и внедрение процесса управления

рисками необходимо вести с оглядкой на управление инцидентами и аудитами ИБ.

Установленный процесс анализа рисков – это обязательное требование стандарта СТО-БР ИББС-1.0-2006 по обеспечению информационной безопасности в банковской сфере.

Постановка процесса анализа рисков необходима организации, если в ней принято решение о прохождении сертификации на соответствие требованиям международного стандарта ISO/IEC 27001:2005.

Установление режима защиты коммерческой тайны и персональных данных неразрывно связано с анализом рисков, так как все перечисленные процессы используют сходные методы идентификации и оценки активов, разработки модели нарушителя и модели угроз.

Список литературы:

1. Суханов А. Анализ рисков в управлении информационной безопасностью// Байт. 2008. № 11. С. 25-29.

2. Омельянчук А. Анализ угроз при проектировании систем технических средств охраны// Технологии защиты. 2008. №3. С. 37-41.

3. Емельянников М. Информационные системы персональных данных // Журнал «CIO». 2008. № 10. С. 17-20.

4. Разувайкин В. Что делать с персональными данными? // Инсайд. 2008. № 3. С. 45-49.

5. Эмм М., Зосимовская Н. Стандарт PCI DSS: Основные несоответствия и как с ними бороться // Плас. 2008. № 1. С. 32-37.

НЕДОКУМЕНТИРУЕМЫЕ ОСОБЕННОСТИ ОБОРУДОВАНИЯ (SCANSTATION RS 150) И ПОСТАВЛЯЕМОГО С НИМ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Авторы: Р. С. Череватый, канд. техн. наук, доц., О. В. Чечуга, канд. техн. наук, доц., Е. И. Струкова, канд. техн. наук, доц., (Россия, Тула, ТулГУ)

Приведены результаты изучения технологических возможностей сканера рулонных микрофильмов Scanstation RS 150 фирмы Wicks and Wilson (Великобритания) в серии производственных экспериментов.

Активно предлагаемые сегодня гибридные системы представляют собой совмещенные комплекты оборудования сканирования документов (получение электронного образа) и печати микрофильмов. Такие системы, как правило, пишут на 16/35-мм рулонный фильм с достаточно высокой

скоростью ввода для документов всех форматов от А0 до А6. Гибридные системы решают одновременно проблемы создания архивов для оперативного и долговременного хранения информации[1].

Используемая для целей сохранности бумажных документов технология микрофильмирования позволяет:

- обеспечить сохранность информации до 300 - 500 лет при условии соблюдения стандартов по съемке и хранению;

- сократить площади, занимаемые под хранение документации, в10 - 20 раз;

- использовать микрофильм в качестве подлинника при решении различного рода юридических вопросов (ГОСТ13.1.101-93. «Микрофильм на правах подлинника»).

Современное состояние средств вычислительной техники позволяет переводить документ из аналоговой формы в электронную и обратно с заданными требованиями к качеству изображения документа.

Так, с появлением сканеров рулонных микрофильмов технология микрофильмирования получила дополнительные возможности. Сегодня для любого пользователя не составит проблем перевести в электронный вид даже очень старые документы, записанные на микропленку. Многие конструкторские бюро восстанавливают старые архивы, переводя их на электронные носители [1]. Учитывая фактор востребованности и большие сроки хранения микрофильмов, такие работы можно проводить постепенно, что еще раз подтверждает экономическую эффективность микрографических архивов.

С точки зрения качества сканированного изображения документа можно выделить три уровня представления:

- уровень просмотра;

- уровень детализации;

- уровень факсимильности.

Сканер Scanstation RS 150 фирмы «Wicks and Wilson» представляет собой полнофункциональную систему сканирования, позволяющую работать с рулонными микропленками 16 мм и 35 мм с коэффициентом уменьшения от 7.5 до 50. Отсканированные данные можно просмотреть, распечатать или сохранить в файле в черно-белом формате либо в градациях серого – 256 градаций [2].

Сканер обладает всеми функциями, необходимыми для сканирования отдельных кадров рулонных микропленоклибо для последовательного сканирования всей пленки. В результате сканирования создаются файлы изображений наилучшего возможного качества. Программное обеспечение сканера работает под управлениемоперационной системы Windows. Системным интерфейсом сканера является сеть, по которой изображения передаются на «файл сервер хост» системы (указанной в качестве удаленного узла сети) напрямую или через буферный каталог. Кроме того, данные можно хранить надисковых накопителях, указав в качестве доступак данным

локальный контроллер. Такой подход позволяет сохранять данные на дискетах, оптических дисках, магнитной ленте и т.д.

Станция сканирования управляется с помощью полнофункционального, простого в использовании и достаточно мощного программного обеспечения Rollfilm RS l.0 q, входящего в состав системы.

Система Scanstation может работать в следующих режимах: SINGLE SCAN, AUTO ADVANCE, BATCH SCAN и MANUAL SCAN [2].

Режим пакетного сканирования позволяет спомощью команды SCAN последовательно сканировать кадры пленки до тех пор, пока не будет достигнут конец пленки или процесс не будет прерван оператором. В данном режиме сканирование выполняется по всей ширине пленки. Программное обеспечение определяет расположение каждого кадра, который затем сканируется и отображается в соответствии с выбранным режимом просмотра. Программа автоматически принимает изображение и переходит к следующему кадру. Таким образом, процесс продолжается без вмешательства оператора. В любой момент процесс сканирования можно приостановить, при этом можно просмотреть текущее изображение, изменить параметры сканирования или продолжить обработку.

Параметры обнаружения краев можно ввести вручную в соответствующие поля или с помощью мастера «Функцияобнаружения краев кадров» можно настроить независимо для обоих краев кадра. При этом край кадра определяется в соответствии с долей белых пикселей в процентах, указываемой в соответствующихполях.

Можно настроить ширину пленки для сканирования (например, отдельное сканирование верхнего и нижнего ряда изображений на дуплексной пленке), а также длину пленки для сохранения в каждом файле (рис. 1-3).

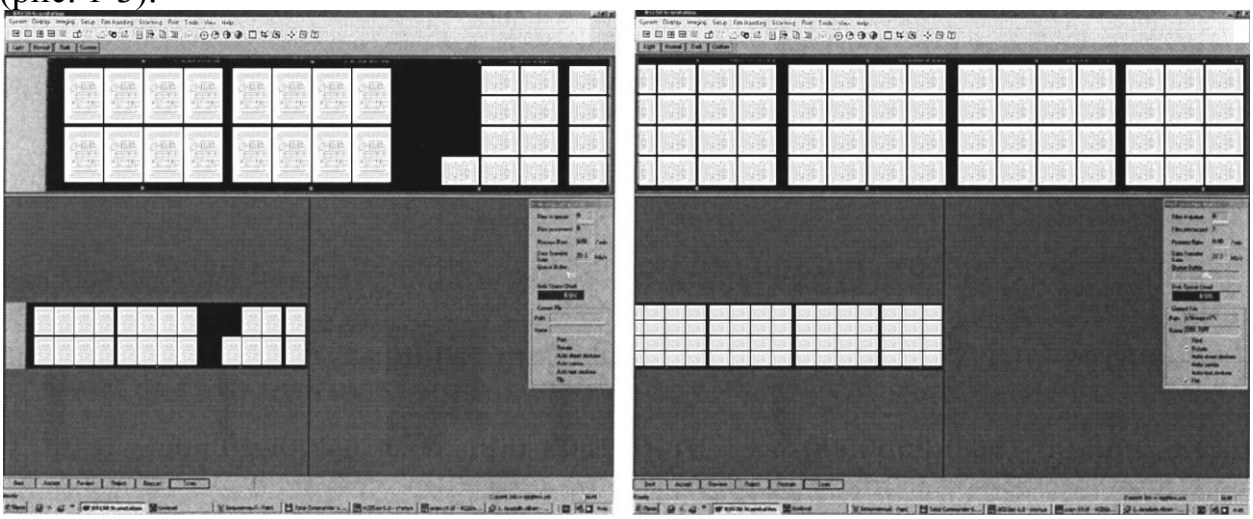


Рис. 1. Сканирование в пакетном режиме рулонного микрофильма по всей его ширине за один проход

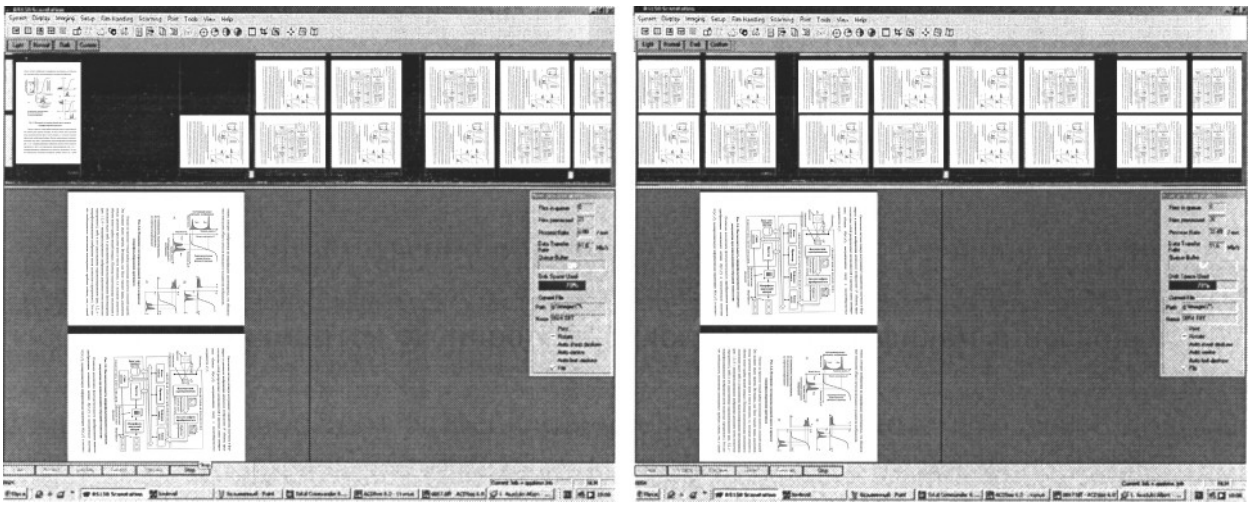
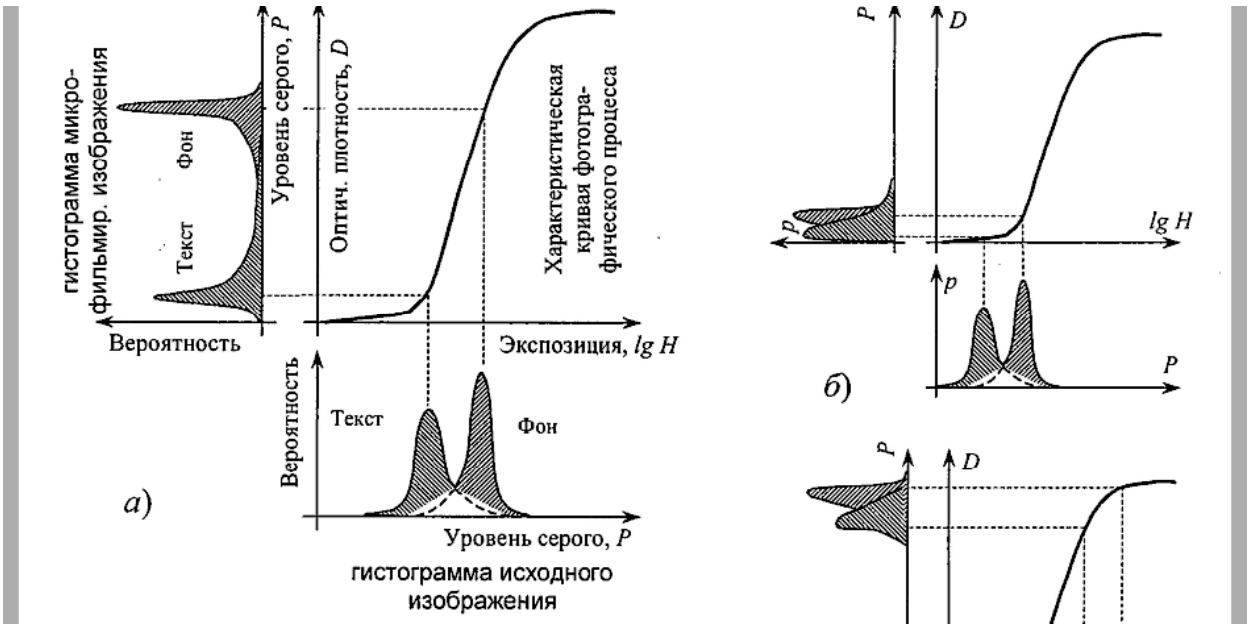


Рис. 2. Сканирование в пакетном режиме рулонного микрофильма за два прохода по всей его ширине

При сканировании рулонного микрофильма в градациях серой шкалы в зависимости от требуемой кратности изображения оборудование ограничивает выбор значений разрешающей способности сканирования целого (по ширине пленки) изображения. Для формата A0 и кратности 29.7 максимальное разрешение составляет 200 dpi, при котором обеспечивается сканирование полной ширины микрофильма, для формата A1 и кратности 21 – 300 dpi и только для формата A2 при кратности 14.8 обеспечивает полное оптическое разрешение 400 dpi.

Для того чтобы при заданной кратности 29.7 и 21 и при формате изображения A0 и A1 соответственно получить более высокие значения разрешающей способности приходится сканировать рулонный микрофильм в несколько проходов и в зависимости от разрешения число проходов может возрасти до 3 (для формата A0).



а) нормальное экспонирование;
б) недоэкспонирование;
в) переэкспонирование

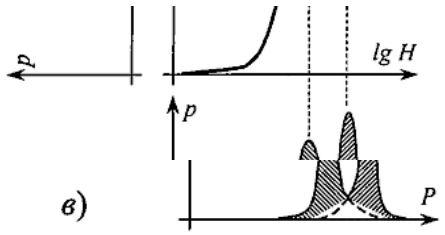


Рис. 3. Результат сканирования за два прохода в дуплексном режиме при автоматическом определении краев кадра.

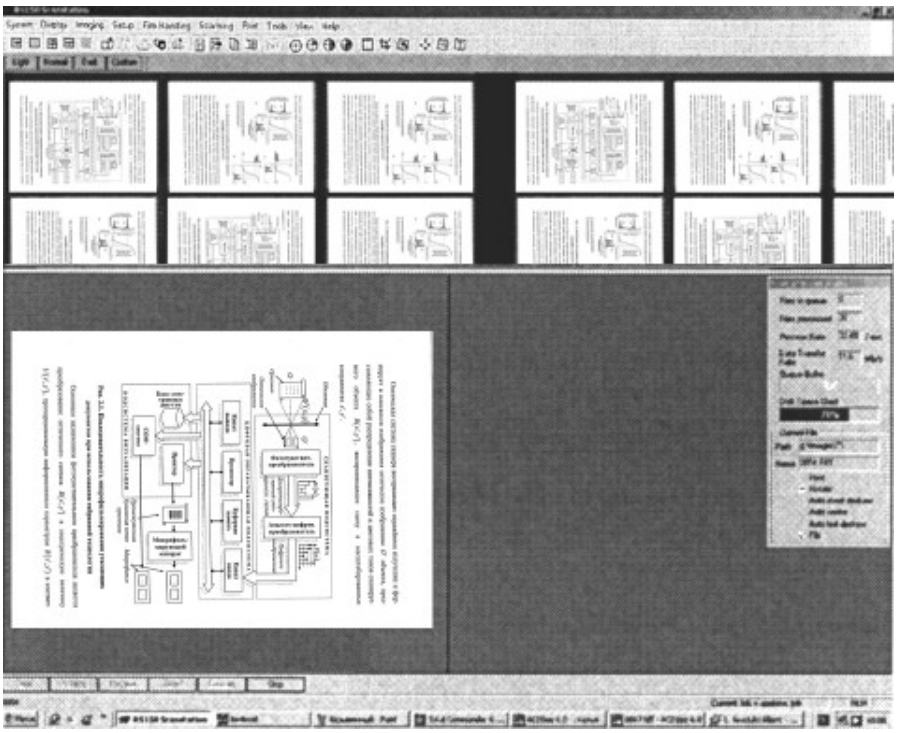
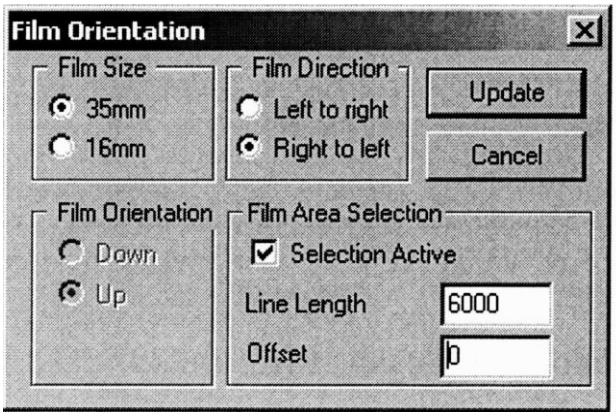


Рис. 4. Сканирование микрофильма за более чем два прохода (сканирование участка меньше 1/2 ширины микрофильма).

При количестве числа проходов более 2х, приходится использовать смещение области сканирования по высоте микрофильма, используя поле Film Area Selection/Offset во вкладке Film Handing/Film Orientation (рис. 5).



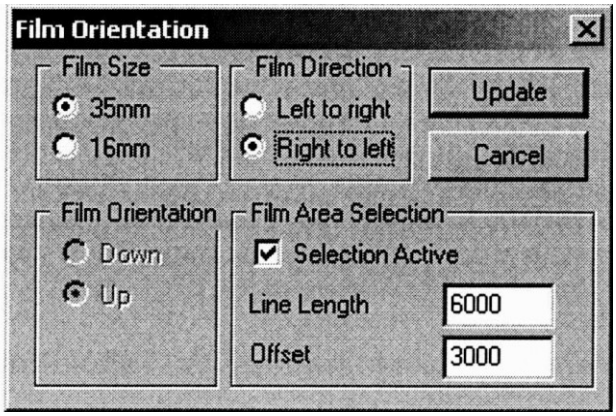


Рис. 5. Вкладка Film Handing/Film Orientation

Сканирование микрофильма за несколько проходов удобно применять, если микрофильм был записан в режиме Office 0 (несколько отдельных изображений на одном кадре), в противном случае придется составлять изображения, что при сканировании рулонного микрофильма трудоемко.

Таким образом, выявлены некоторые недокументированные возможности при изучениитехнологиисканера рулонных микрофильмов Scanstation RS 150 фирмы «Wicks and Wilson» (Великобритания) в серии производственных экспериментов, позволяющие при большей плотности записанных изображений получать более качественные сканированные изображения с более высоким значением разрешающей способности.

Список литературы

1. Иванов Р.Н. Репрография. М: Экономика, 1986. 335 с.

2. RS200 RS150 RS100 Rollfilm Scanstation User Guide v1.0 // Electronic Letters. 2003. 166 с.

РАЗРАБОТКА СПОСОБА УСКОРЕННЫХ ИСПЫТАНИЙ КАЧЕСТВА И СОХРАНЯЕМОСТИ МИКРОФИЛЬМОВ

Авторы: А. К. Талалаев, д-р техн. наук, проф., Р. Г. Панфилов, канд. техн. наук, доц., (Россия, Тула, ТулГУ)

Разработан способ ускоренных испытаний качества и прогнозирования предельных сроков хранения микрофильмов с заданным уровнем сохранности определяющего параметра качества. Приведен пример расчета сроков хранения микрофильмов, изготовленных без применения тиосульфата натрия при химико-фотографической обработке.

Обеспечение сохранности документов, в частности на бумажных носителях, является важнейшей государственной задачей и в значительной степени осуществляется созданием Российского страхового фонда документации, представляющего собой совокупность функционально ориентированных и упорядоченных массивов специально изготовленных на микрофильмах страховых копий необходимых документов, хранимых в специальных хранилищах [1].

Микрографическая форма представления документации обладает целым рядом важных достоинств [2]. Качество изготавливаемых микрофильмов, оптическая плотность и читаемость зависят от многих

факторов: свойств используемого фотоматериала, условий его последующей химико-фотографической обработки (ХФО) для визуализации изображения и хранения готового микрофильма.

Проблема прогнозирования поведения полимерных материалов, в частности используемых для микрофильмирования, во времени изучена недостаточно. Для удовлетворительного прогнозирования жизненного ресурса микроизображений необходимо иметь простые и надежные соотношения между кинематическими параметрами физико-химических процессов старения и макро-свойствами материала, определяющими их эксплуатационную пригодность. Наиболее сильное воздействие на деструктивные процессы оказывают повышенные температурно-влажностные условия при хранении микрофильмов.

Результаты исследований многих отечественных и зарубежных ученых позволили сформулировать основные принципы оценки долговечности различных архивных материалов, так как закономерности изменений свойств материалов, изготовленных с применением разных полимерных основ, качественно совпадают.

Изменения в изображении на галогенидосеребряных микрофильмах известны под названием обесцвечивания или выцветания элементов изображения, следствием чего является снижение оптической плотности и контраста этого микроизображения. В значительной степени это происходит из-за присутствия в эмульсионном слое тиосульфата натрия по завершении окончательной промывки микрофильма, за счет известных химических реакций разложения комплексных солей тиосульфата натрия. Содержание остаточного тиосульфат-иона в микрофильмах долговременного хранения после их ХФО должно быть не более 0,0007 мг/л [3], что является очень жесткой нормой.

Обобщение теоретических и экспериментальных исследований позволило разработать обоснованные режимы хранения, обеспечивающие физико-химическую сохранность микрофильмов. Испытания на стабильность фотографического изображения согласно международным стандартам
ISO 4331 и ISO 4332 предусматривают воздействие на микрофильмы окружающего воздуха в течение 30 дней при температуре (60 ± 2) ºС и (60 ± 2) % относительной влажности. После выдержки в указанных условиях образцы микрофильмов сравнивают визуально с контрольным образцом, который хранился при комнатной температуре и относительной влажности не более 60 %. При этом изображение не должно показывать никаких следов разрушения, препятствующих его дальнейшей эксплуатации или хранению. Проведенные по вышеуказанным стандартам испытания образцов микрофильмов, изготовленных без применения тиосульфата натрия, показали пригодность их для последующей эксплуатации и дальнейшего хранения.

В данной статье приводится результаты разработки способа ускоренных испытаний, позволяющего оценивать предельные сроки хранения микрофильмов первого поколения, изготовленных по технологии, исключающей в процессе ХФО применение тиосульфата натрия (в дальнейшем изложении - способ).

1. Объектом испытания являются рулонные негативные микрофильмы первого поколения в отрезках МО-35 [4], выполненные на неперфорированной рулонной фотопленке методом прямой съемки.

2. Испытания проводятся в 2 этапа. На первом этапе образцы подвергаются испытанию в течение 240 ч воздействию температуры 60 ºС и относительной влажности 55 %. По результатам испытаний данного этапа проводится выбор определенного параметра *П* (*D* или S_m, R_m), в наибольшей степени подверженного изменениям, для проведения испытаний второго этапа. На втором этапе образцы подвергаются испытаниям термовлажного воздействия по следующим режимам: температура 55, 60, 65 и 70 ºС при относительной влажности 55 %.

3. Способ предполагает реализацию следующих программы и алгоритма испытаний:

3.1. В процессе испытаний (на обоих этапах) необходимо фиксировать изменения показателя S_m - предела читаемости или R_m - разрешающей способности, *D* - оптической плотности фона изображения, а также физико-механическое состояние образцов микрофильмов.

3.2. Предельный срок хранения микрофильмов должен быть определен с помощью зависимости Аррениуса скорости старения микроизображения от температуры и влажности с использованием экспериментальных данных изменения выбранного (на первом этапе) определяющего параметра микроизображения в ускоренных режимах испытаний:

$$\frac{d \ln K}{dT} = \frac{E}{R \cdot T^2}, \qquad (1)$$

где *K* - константа скорости процесса старения, $с^{-1}$; *T* - температура, ºК; Е - энергия активация процесса, кал/моль; *R* - универсальная газовая постоянная, 1,987 моль К. Для обоснованного применения зависимости Аррниуса в предлагаемой методике прогноза необходимо проверять идентичность физико-химических процессов, протекающих при ускоренном старении и натурном хранении или эксплуатации. Это устанавливается проверкой отсутствия отклонения от линейности регрессионной зависимости

$$\ln \tau_{пр.исп.} = f\left(\frac{1}{T}\right), \qquad (2)$$

где $t_{исп.}$ - время проведения ускоренных испытаний для каждого выбранного значения температуры, при котором установленный на первом этапе

испытаний определяющий параметр П достигает своего предельного порога старения (например, ухудшается на 20 %); T - диапазон температурных значений, в котором проводились ускоренные испытания.

3.3. За скорость процесса старения принимается скорость изменения определяющего параметра микроизображения. Допустимое изменение величины определяющего параметра устанавливается равным 20 % от первоначального значения. За основу модельного прогноза допустимого предельного срока хранения микрофильмов по результатам ускоренных испытаний принимается идентичность произведений скорости старения на время

$$C \cdot \tau = idem = C_{исп.} \cdot \tau_{пр.исп.} = C_{хран.} \cdot \tau_{хран.}, \qquad (3)$$

где $C_{исп}$ $C_{хран}$ - скорости процесса старения соответственно в условиях испытаний и в условиях хранения; $t_{пр.исп.}$ - время испытаний, в течение которого определяющий параметр достиг установленного порога ухудшения качества; $t_{хран.}$ - прогнозируемое время хранения.

3.4. Предельный срок хранения микрофильмов с учетом результатов ускоренных испытаний определяется по соотношению, вытекающему из зависимости (1):

$$\ln\frac{\tau_{пр.исп.}}{\tau_{хран.}} = \frac{E}{R}\left(\frac{1}{T_{исп.}} - \frac{1}{T_{хран.}}\right) \text{ или } \ln\tau_{хран.} = \ln\tau_{пр.исп.} - \frac{E}{R}\left(\frac{1}{T_{исп.}} - \frac{1}{T_{хран.}}\right), \qquad (4)$$

где $T_{исп.}$ и $T_{хран.}$ - температура испытаний и хранения соответственно, ºК;
$t_{пр.исп.}$ и $t_{хран.}$ - предельное время испытаний и хранения соответственно, ч.

При этом стандартизованная температура хранения составляет
$T_{хран.} = 285$ ºК.

3.5. Испытания проводят с использованием термошкафов, шкафа переменной температуры и эксикатора. Они реализуются в следующей последовательности:

- образцы микрофильмов помещают в эксикатор, где создана относительная влажность воздуха, соответствующая данному этапу испытаний, а затем эксикатор помещают в термошкаф с заранее установленной температурой в соответствии с п. 2;

- периодически испытуемые образцы микрофильмов извлекаются из эксикаторов, выдерживаются на воздухе для акклиматизации в течение 30 мин, затем производятся замеры значений определяющего параметра (П) (контроль изменения определяющего параметра); периодичность выемки образцов устанавливается опытным путем, в зависимости от интенсивности наблюдаемых изменений и соблюдения условий репрезентативности получаемой выборки;

- результаты измерений заносятся в журнал испытаний, при этом контролируется физико-механическое состояние образцов;

- результаты изменения определяющего параметра до предельного значения аппроксимируются (например, с помощью компьютерной программы «*Table curve – 2D*») в виде регрессионной зависимости $П = f(t_{исп.})$, по которой определяются предельные значения времени испытаний $t_{пр.исп.}$, в течение которого определяющий параметр достигает своего допустимого порога ухудшения;

- установленные предельные значения $t_{пр.исп.}$ для всех режимов ускоренных испытаний используются для расчетов по п. 3.4 прогнозного срока предельного хранения микрофильмов, при котором ухудшение качества не превысит допустимого;

- на основании полученных расчетов выдается заключение о гарантированном сроке хранения микрофильмов.

Приведем пример использования разработанного способа ускоренных испытаний для оценки предельных сроков хранения.

Объектом испытаний являлись образцы микрофильма первого поколения на пленке Copex HDP 10 (Бельгия) с изображением тест-оригиналов [3] масштабом 1:14,8, полученные по технологии ХФО без применения тиосульфата натрия.

Цель испытаний – определение предельного срока хранения микрофильмов в условиях, регламентируемых государственным стандартом [5].

Материально-техническое обеспечение:

1. Съемочный аппарат Recordak Micro-File Film unit, model MCGI (зав. № 2874).
2. Аппарат химико-фотографической обработки Meolab.
3. Термошкафы ТС-80М (зав. № 43016, № 283325) и GRONLAND (зав. № 90200158).
4. Денситометр фирмы Brumac Indastries, Ins, модель МР-8 (зав. № 9405636).
5. Прибор контроля универсальный Carl Zeiss Iena (зав. № 2030).
6. Эксикатор стеклянный [6].
7. Мерный цилиндр V = 250 мл [7].
8. Кислота серная, (d = 1,83 г/л) [7].
9. Вода дистиллированная [8].

Из анализа результатов комплекса предварительных испытаний было установлено, что влага оказывает весьма существенное воздействие на состояние микроизображений, в связи с чем были тщательно подобраны водные растворы серной кислоты, обеспечивающие поддержание постоянной влажности во всем температурном и временном интервалах испытаний, и химико-фотографическая обработка на аппарате Meolab велась по режиму, приведенному в табл. 1.

Таблица 1. Режимы ХФО

№ п/п	Наименование операции	Время обработки, мин.	Температура, °С
1	Проявление	**4,0**	**28,0**
2	Промывка	**4,0**	**15,0 - 18,0**
3	Осветление	**4,0**	**28,0**
4	Промывка	**4,0**	**15,0 -18,0**
5	Отбеливание	**3,0 – 4,0**	**20,0**
6	Промывка	**4,0**	**15,0 – 18,0**
7	Чернение	**2,0**	**20,0**
8	Промывка	**8,0**	**15,0 – 18,0**

Результаты предварительных испытаний (первого этапа) подтвердили возможность выбора в качестве предельной величины определяющего параметра качественных изменений микроизображений рекомендуемое увеличение оптической плотности D (т.е. ухудшения качества микрофильма) на 20 % от первоначального значения. При этом читаемость меры шрифта S_m оставалась неизменной (не ухудшалась).

На втором этапе отобранные образцы микрофильмов (по 5 штук в каждой серии испытаний) с изображением тест-объекта помещали в эксикаторы с водными растворами серной кислоты для создания относительной влажности 55 % [5] и выдерживали в термошкафах при температурах 55, 60, 65, 70 °С. Качественные изменения микрофильмов оценивали измерением на денситометре оптической плотности фона микроизображения и определением читаемости миры шрифта тест-объекта ТО-1 с помощью прибора контроля универсального. Несмотря на значительный общий срок проведения параллельных для каждой температуры испытаний (6,5 месяцев), ни в одном случае из используемых режимов не было ухудшения качества микрофильма (увеличение оптической плотности изображения) на 20 %. В этой связи представилось возможным повысить требования к качеству сохранности микрофильмов, а именно – пороговое значение оптической плотности принять на уровне 13 %. Однако для температуры испытаний 55 °С и эта величина оказалась недостижимой за весь период испытаний, на основании чего указанная температура испытаний была признана не лимитирующей скок хранения и соответствующие данные в дальнейший расчет не принимались. В табл. 2 приведем данные изменения оптического параметра микроизображений D на пленке Copex HDF 10 при относительной влажности 55 %, неизменном контролируемом пределе читаемости $S_m = 45$.

Таблица 2. Изменение оптической плотности микроизображения D от времени ускоренного испытания исп. t по предлагаемому способу в зависимости от температуры T испытаний

Обозн. парам.	Значения параметров в отдельном испытании*														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Температура $T^0_{исп.} = 55\ ^0$C															
$\tau_{исп.}$, ч	0	15	42	61	83	153	175	199	320	388	483	507	577	669	815
D ,Б	1,424	1,466	1,482	1,490	1,488	1,488	1,496	1,492	1,490	1,498	1,486	1,494	1,492	1,502	1,501
Температура $T^1_{исп.} = 60\ ^0$C															
$\tau_{исп.}$, ч	0	15	37	60	82	153	175	198	221	243	319	487	653	723	
D ,Б	1,110	1,188	1,208	1,225	1,220	1,229	1,221	1,237	1,236	1,239	1,237	1,242	1,277	1,281	
Обозн. парам.	Значения параметров в отдельном испытании*														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Температура $T^2_{исп.} = 65\ ^0$C															
$\tau_{исп.}$, ч	0	15	38	61	136	182	225	299	465	535	628	798			
D ,Б	1,122	1,217	1,230	1,256	1,250	1,254	1,258	1,262	1,259	1,260	1,258	1,258			
Температура $T^3_{исп.} = 70\ ^0$C															
$\tau_{исп.}$, ч	0	35	75	113	225										
D ,Б	1,170	1,190	1,290	1,325	1,330										

На рис. 1 приведены соответствующие аппроксимированные зависимости. Штриховыми линиями отмечены значения параметров, соответствующие моментам достижения оптической плотностью предельного порога ухудшения качества микрофильма. Анализ полученных графических зависимостей показывает, что наиболее интенсивное увеличение оптической плотности наблюдается лишь в первые сутки ускоренных испытаний для всех режимов, а затем происходит очень незначительный прирост в течение длительного времени. Это, очевидно, объясняется завершением остаточных химических реакций.

Графическая интерпретация результатов проверки идентичности физико-химических процессов при ускоренном старении и натурном хранении или эксплуатации микрофильмов, а следовательно, при обоснованном применении уравнения Аррениуса, представлена на рис. 2.

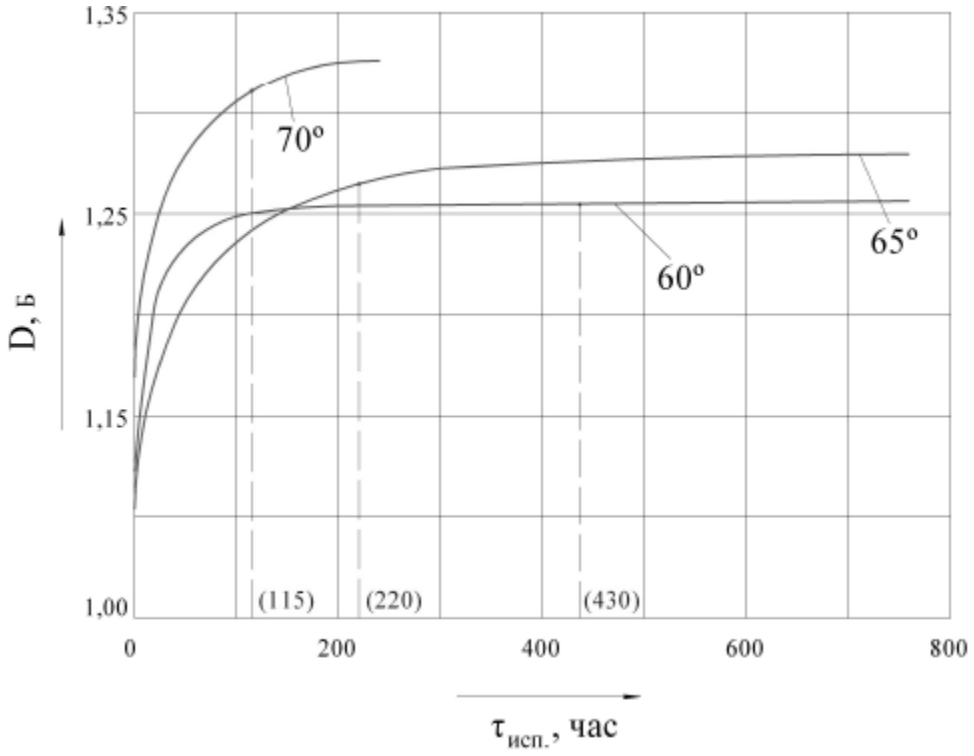


Рис. 1. Аппроксимированные регрессионные зависимости $D = f(t_{исп.})$ для различных значений температуры ускоренных испытаний

Очевидность линейности полученной зависимости подтверждает обоснованность проводимых расчетов. В случае возникновения сомнений следует провести корреляционный анализ с расчетом коэффициента корреляции и корреляционного отношения и проверкой значимости их расхождения.

Из зависимостей, представленных на рис. 1, легко установить предельные значения времени испытания пр.исп. t для каждой температуры испытаний:

$$60\ ^0C\ -\ \tau^1_{пр.исп.} = 430\ \text{ч.};\ 65\ ^0C\ -\ \tau^2_{пр.исп.} = 220\ \text{ч.};\ 70\ ^0C\ -\ \tau^2_{пр.исп.} = 115\ \text{ч.}$$

Энергия активации процесса старения микроизображения каждого температурного интервала рассчитывается по модифицированной формуле (4), в которую вместо $t_{пр.исп.}$, $t_{хран.}$ необходимо подставить $t^1_{пр.исп.}$, $t^2_{пр.исп.}$, $t^3_{пр.исп.}$, а вместо $T_{исп.}$ и $T_{хран.}$ - $T^1_{исп.}$, $T^2_{исп.}$, $T^3_{исп.}$:

$$E_1 = 33497,\ E_2 = 32438,$$

$$E_{ср} = \frac{E_1 + E_2}{2} = 32968\ \text{[ккал/моль]}.$$

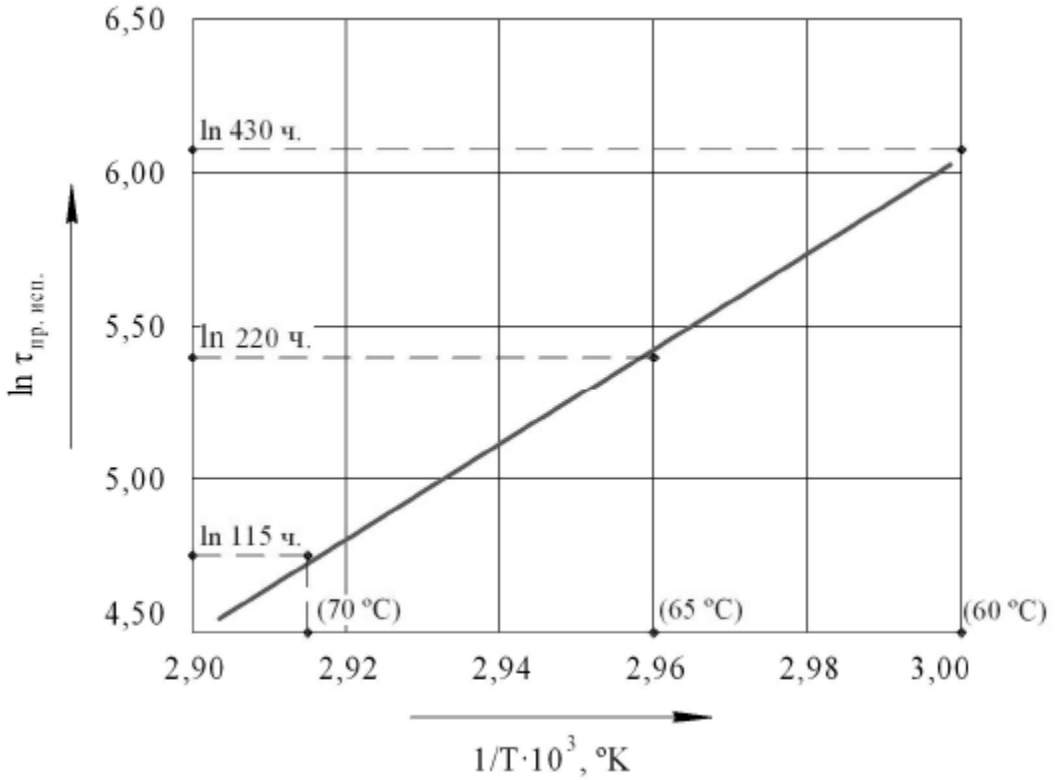


Рис. 2. Зависимость логарифма времени $t_{пр.исп.}$ достижения оптической плотностью изображения (определяющим параметром) предельного значения (ухудшения качества на 13 %) от величины, обратной температуре, при трех ее значениях, участвующих в расчетах

Подставляя полученные данные вновь в зависимость (4), получим предельное время сохранности микрофильмов, полученных без применения тиосульфата натрия при ХФО. Расчеты проведены для температур хранения 20 и 12 0С и относительной влажности 55 %.

$$\ln \tau_{хран.}^{20^0} = 12,86\,;\ \text{“}\ \tau_{хран}^{20^\circ} = 15987,5 \text{ сут.} \approx 43,8 \text{ года;}$$

$$\ln \tau_{хран.}^{12^0} = 14,52\,;\ \tau_{хран}^{12^\circ} = 84083,3 \text{ сут.} \approx 230 \text{ лет.}$$

При снижении уровня требований к качеству хранимых микрофильмов до предельного уровня снижения определяющего параметра на 20%, предельные сроки хранения значительно увеличатся.

ВЕРХОВНАЯ РАДА ПРИНЯЛА ЗАКОН О СТАНДАРТИЗАЦИИ

Источник: http://biz.liga.net/ekonomika/all/novosti/2763804-verkhovnaya-rada-prinyala-zakon-o-standartizatsii.htm

Верховная Рада Украины приняла Закон "О стандартизации" (регистр. N4585). За такое решение проголосовали 274 народных депутата.

Закон направлен на формирование и реализацию государственной политики в сфере стандартизации.

Законодательным актом определены правовые и организационные основы национальной стандартизации, направленные на приведение ее в соответствие с европейской моделью, а также созданию единого национального органа по стандартизации.

Согласно закону, *европейский стандарт* - региональный стандарт, принятый европейской организацией стандартизации; *межгосударственный стандарт* - региональный стандарт, предусмотренный Соглашением о проведении согласованной политики в области стандартизации, метрологии и сертификации от 13 марта 1992 года и принятый Межгосударственным советом по стандартизации, метрологии и сертификации; *международный стандарт* - стандарт, принятый Международной организацией по стандартизации и доступный для широкого круга пользователей; *национальная стандартизация* - стандартизация, которая осуществляется на уровне одного государства; *национальный стандарт* - стандарт, принятый национальным органом стандартизации и доступный для широкого круга пользователей.

Функции национального органа стандартизации выполняет государственное предприятие, которое не подлежит приватизации,

образованное центральным органом исполнительной власти, реализующим государственную политику в сфере стандартизации. Национальный орган стандартизации не может иметь целью получение прибыли от своей деятельности.

К полномочиям национального органа стандартизации переданы: организация и координация деятельности в сфере стандартизации; утверждение программ работ по стандартизации, принятие и отмена национальных стандартов (в том числе в сфере строительства), создание, прекращение деятельности технических комитетов стандартизации, представление интересов Украины в международных и региональных организациях стандартизации и сотрудничество с национальными органами стандартизации других государств. Согласно европейской практике выполняющий соответствующие функции национальный орган стандартизации, не является органом государственной власти.

При этом действие закона не распространяется на санитарные мероприятия безопасности пищевых продуктов, ветеринарно-санитарные и фитосанитарные мероприятия, строительные нормы, лекарственные средства, стандарты медицинской помощи, бухгалтерского учета, оценки имущества, образования и другие социальные стандарты, предусмотренные законодательством.

Согласно принятому закону, объектами стандартизации являются: материалы, комплектующие, оборудование, системы, их совместимость; правила, процедуры, функции, методы, деятельность или ее результаты, включая продукцию, персонал, системы управления; требования к терминологии, обозначению, фасовке, упаковке, маркировке, этикетировке и тому подобное.

Технические комитеты стандартизации не имеют статуса юридического лица. К работе в технических комитетах стандартизации привлекаются уполномоченные представители органов исполнительной власти, других государственных органов, органов местного самоуправления, субъектов ведения хозяйства и их общественных объединений, организаций работодателей и их объединений, научных учреждений и учебных заведений, научно-технических и инженерных обществ (союзов), общественных организаций потребителей (объединений потребителей), других общественных объединений, профессиональных союзов, ведущих научных работников и специалистов.

Определены источники финансирования: средства госбюджета; средства, предусмотренные на выполнение программ и проектов; собственные и привлеченные средства субъектов ведения хозяйства; другие, не запрещенные законодательством источники финансирования.

ЕВРОСОЮЗ ВСКОРЕ ОБНОВИТ ЗАКОНОДАТЕЛЬСТВО ОБ ЭЛЕКТРОННЫХ ПОДПИСЯХ

Автор: Наташа Храмцовская

Данная статья Марка Герлаха (Mark Gerlach) была опубликована 30 апреля 2014 года на американском сайте «Новости правовых технологий» (Law Technology News).

Ожидается, что в Евросоюзе в ближайшее время появится законодательство, регулирующее трансграничное использование электронных подписей, сопоставимое по эффективности с законом США об электронной подписи.

Европейский Союз более десятилетия потратил на формирование согласованного законодательства об электронной подписи, удовлетворяющего все его 28 стран-членов в плане технических стандартов и полноты нормативно-правовой базы. Этот процесс в настоящее время близится к завершению, и Евросоюз надеется принять закон об электронной подписи к июлю.

Согласно высказанному в интервью «Новостям правовых технологий» мнению Хью Лога (Hugh Logue), старшего аналитика научно-консультационной фирмы Outsell Inc., располагающейся в Бёрлингеме (Burlingame), штат Калифорния, «Евросоюз столкнулся с рядом препятствий при внедрении общеевропейского законодательства об электронной подписи, которое было бы равноценно американскому. Но сейчас он подтягивается».

Хью Лог пояснил, что европейская Директива 1999/93/ЕС (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999L0093) заложила правовую основу для использования электронных подписей, и к 2001 году страны-члены Евросоюза должны были привести в соответствие с ней своё законодательство. Однако страны интерпретировали Директиву по-разному, и к тому же, по словам живущего в Лондоне Лога, «у коммерческого сектора отсутствовала заинтересованность во внедрении этой модели».

Теперь, 13 лет спустя, Евросоюз готовится к завершающим усилиям по введению общеевропейской политики по этому вопросу. В начале этого месяца Евросоюз одобрил закон о европейской электронной идентификации и доверенным услугам при осуществлении электронных транзакций

("Regulation on electronic identification and trust services for electronic transactions in the internal market", *текст одобренной Европарламентом 3 апреля 2014 года редакции документа доступен по адресу* http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0282 – *Н.Х.*). Новый закон, который Совет министров Евросоюза, как ожидается, утвердит в июне 2014 года (тогда он вступит в силу в июле), сделает возможным трансграничное электронное взаимодействие между коммерческими организациями, гражданами и государственными органами.

По мнению Лога, одной из причин, по которым США смогли быстрее приспособиться к электронным подписям, была однотипность правовой системы. В США в 2000 году был принят Закон об использовании электронных подписей в глобальной и национальной коммерции (Electronic Signatures in Global and National Commerce Act, http://www.gpo.gov/fdsys/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf), придавший электронным подписям такую же правовую силу, как и собственноручным.

Мой комментарий: *С моей точки зрения, американцам сильно упрощают жизнь особенности английского права, способствующие применению в государственном управлении и в деловой деятельности любых разумных технологий, в том числе только что появившихся; а также широкое использование простых (по европейской терминологии) электронных подписей и, наоборот, очень ограниченное применение усиленных электронных подписей.*

В Европе различные точки зрения стран-членов Евросоюза стали причиной длительной тяжелой борьбы. Лог отмечает, что даже бумажные подписи все ещё не стандартизированы в масштабах Евросоюза: так, например, некоторые страны требуют нотариального заверения договоров, в то время, как другие допускают при тех же обстоятельствах устные контракты. Такого рода расхождения сделали процесс согласования и утверждения технического и правового стандарта неимоверно трудным.

Евросоюз опубликовал на своём сайте список доверенных поставщиков сертификационных услуг. Для обеспечения безопасности при совершении трансграничных транзакций электронные подписи в Европе должны использовать такие услуги в сфере обеспечения доверия (http://ec.europa.eu/digital-agenda/en/trust-services), как отметки (штампы) времени, электронные печати, аутентификацию веб-сайтов, правовую допустимость и электронную доставку. Под новое законодательство подпадают электронные цифровые подписи, средства создания которых выдаются удостоверяющими центрами, а также другие виды электронных подписей.

Как сообщает Лог, новое законодательство не отдает предпочтения какой-либо конкретной технологии, - подход, который лоббировали представители ряда поставщиков.

Как считает главный аналитик бостонской компании Blue Hill Research Дэвид Хулихан (David Houlihan), такие поставщики услуг, как фирма DocuSign из Сан-Франциско, Adobe System Inc. и стокгольмская TrustWeaver могут извлечь выгоду из нового законодательства.

Все эти компании конкурируют на поле «исполнения законодательно-нормативных требований ряда юрисдикций и смягчения рисков, связанных с использованием электронных подписей», отмечает Хулихан.

Мой комментарий: Почему эта новость для нас интересна? Просто потому, что закон, который будет вскоре принят Евросоюзом, спустя недолгое время может быть адаптирован и у нас – точно так же, как европейская Директива 1999/93/ЕС была нами почти дословно адаптирована в виде федерального закона «Об электронной подписи».

ОТКРЫТО ПУБЛИЧНОЕ ОБСУЖДЕНИЕ СТРАТЕГИЧЕСКОГО ПЛАНА МЕЖДУНАРОДНОЙ ОРГАНИЗАЦИИ ПО СТАНДАРТИЗАЦИИ НА 2016-2020 ГОДЫ

Источник: сайт Британского института стандартов http://drafts.bsigroup.com/Home/Details/52924

Автор: Наташа Храмцовская

С 6 мая 2014 года на сайте Британского института стандартов (BSI) выложен для публичного обсуждения проект стратегического плана Международной организации по стандартизации ИСО на 2016-2020 годы (ISO strategic plan 2016-2020), см. http://drafts.bsigroup.com/Home/Details/52924 . Обсуждение продлится до 25 июня 2014 года.

Новая стратегия ИСО разрабатывается в связи с тем. что в конце 2015 года заканчивается срок действия предыдущего плана. План разрабатывается для организации в целом, включая её членов, центральный секретариат и технические комитеты.

В опубликованном на сайте пояснении директор BSI по стандартам д-р Скотт Стидман (Dr Scott Steedman) пишет:

Международная организация по стандартизации (ИСО) начала публичное обсуждение своего стратегического плана на 2016-2020 годы. ИСО через своих членов и их экспертов является крупнейшим в мире разработчиком основанных на добровольном консенсусе международных стандартов, и Британский институт стандартов в качестве национального органа по стандартизации оказывает ИСО всестороннюю поддержку и является одним из основных её финансовых спонсоров. Мы рассматриваем стандарты ИСО как международные инструменты для ведения деловой деятельности, которые поддерживают и способствуют внедрению наилучшей практики в области разработки и поставки продуктов и услуг; а также хорошего делового поведения.

Среда разработки стандартов существенно изменились с 2011 года, когда была сформулирована действующая стратегия, и эти изменения продолжатся и в период до 2020 года. Очень важно, чтобы новая стратегия наметила устойчивую траекторию развития для ИСО в целом, включая членов организации, её центральный секретариат и технические комитеты, опираясь при этом на ранее достигнутые успехи и учитывая потенциальные будущие проблемы и возможности.

У Британского института стандартов, как у ведущего члена ИСО, есть все возможности для формирования направлений этой стратегии таким образом, чтобы они отражали потребности британского бизнеса, государства и потребителей. Выложенный для публичного обсуждения документ дает возможность почувствовать ход мысли, лежащий в основе новой стратегии, - в отношении которого Вы можете высказать свои замечания и предложения, дав нам знать, какими, по Вашему мнению, должны быть стратегические приоритеты ИСО в период до конца десятилетия.

Предлагаемый Вашему вниманию документ состоит из трех разделов. В первом разделе содержится базовая информация по текущей ситуации и по основным сильным сторонам системы ИСО. Во втором разделе даётся анализ будущей среды и ее потенциального воздействия на международной арене разработки стандартов.

Третий раздел, что наиболее важно, содержит ряд вопросов, ответ на которые мы хотели бы от Вас получить. Ваши замечания и предложения помогут подготовить официальный отзыв Британского института стандартов. Мы хотим быть уверенными в том, что наш отзыв отражает позиции и мнения британских заинтересованных сторон, и я буду очень благодарен, если Вы найдёте несколько минут на то, чтобы ответить на эти вопросы.

Вы можете оставить свои замечаний и предложения как на сайте BSI с помощью системы комментирования проектов (Draft Review System), так и заполнив соответствующую форму для подачи замечаний и отослав её по адресу standards.international@bsigroup.com до 25 июня 2014 года.

Структура второго раздела показывает, как авторы документа представляют себе успешно работающую Международную организацию по стандартизации в 2020 году:

- ИСО является ведущим органом по стандартизации;
- Управление деятельностью ИСО является заслуживающим доверие и динамичным;
- Состав членов ИСО является сильным и представительным, отличается глобальностью охвата;
- ИСО тщательно выбирает своих партнеров;
- ИСО является передовой организацией в плане налаживания взаимодействия с заинтересованными сторонами
- ИСО использует передовой, мирового класса процесс разработки стандартов;
- ИСО реагирует на потребности использующих стандарты потребителей;
- ИСО продолжает оказывать помощь и поддержку развивающимся странам;
- Центральный секретариат ИСО помогает организации реализовать её видение на 2020 год.

Мой комментарий: Ведущие страны – Великобритания, США, Франция и др. – стремятся изменить традиционную «кулуарную» модель процесса разработки стандартов и других документов за счет проведения публичных обсуждений, в которых могут принять участие все заинтересованные специалисты и организации. Одновременно появляется возможность заранее (и, что немаловажно, бесплатно) познакомиться с содержанием разрабатываемых стандартов ИСО – такой подход должен способствовать более активному использованию стандартов и, в конечном итоге, благотворно повлиять и на доходы от их продажи. Очень хотелось бы, чтобы Росстандарт тоже начал движение в этом же направлении.

ДОКУМЕНТ УМЕР, ДА ЗДРАВСТВУЕТ ДОКУМЕНТ!

Автор: Наташа Храмцовская

Статья известного американского специалиста, генерального директора и главного консультанта фирмы IRAD Strategic Consulting д-ра Кэрол Чокси была опубликована на сайте фирмы 16 мая 2014 года. Она посвящена «вечно зелёному» вопросу – «Что такое документ?», и отражает точку зрения, характерную для ряда коллег из США. Я предлагаю читателям перевод этой статьи как материал для размышлений; моя собственная точка зрения по ряду вопросов не совпадает с позицией Кэрол Чокси.

Заявления ученых мужей, что документы «умерли», свидетельствуют о невежестве в вопросах управление документами, управления рисками и

электронного раскрытия. Проблема в том, что большое число людей пытается заниматься управлением документами, не имея для этого соответствующей подготовки. Бухгалтеры, юристы, эксперты по раскрытию электронной информации в ходе судебных споров, консультанты по управлению контентом, консультанты по вопросам поиска и систем классификации - все они утверждают, что помогают организациям управляться с их «документами». Большинство готово давать советы о закупке технологий, даже не пытаясь определить, в какой мере используемая организацией корпоративная архитектура сковывает возможности даже хорошо подготовленных сотрудников по исполнению политик, касающимся управления информацией.

Особенно тревожным среди всех недостатков, вытекающих из отсутствия подготовки по вопросам управления документами, является непонимание того, что такое «документ» (record). Эта проблема настолько общераспространенная, что она ставит под угрозу способность большинства компаний управлять рисками, и в особенности рисками, связанными с судебными спорами. Даже руководители юридических служб крупных американских корпораций не понимают, особенно в сфере электронного раскрытия, что такое документ и на что он способен, в результате подводя свои компании под самые уродливые и самые дорогостоящие формы представления информационного контента (*Согласно законодательству США и ряда других англосаксонских стран, в случае судебного спора или расследования стороны в принципе обязаны представить суду абсолютно всю относящуюся к делу информацию и документы, находящуюся под их контролем, вне зависимости от вида носителя и способа хранения. Те, кого ловят на неисполнении этого требования, обычно проигрывают спор и могут быть подвергнуты ряду болезненных дополнительных наказаний. Поэтому, вовремя не уничтожая документы и рабочие материалы по истечении установленных для них сроков хранения, организации создают для себя дополнительные риски. – Н.Х.*).

Что такое «документ»? Ответ: «Смотря по обстоятельствам». Государственные органы должны исполнять требования законов и нормативных актов, регламентирующих для них вопросы управления информацией. В определенный момент информация, относящаяся к деятельности по государственному управлению, меняет свой статус и становится «документом». Понятие «объявления документом» (declaring a record – *которое, следует отметить, в последние годы почти вышло из употребления как раз вследствие усиления открытости государственного управления и практики электронного раскрытия, в равной степени охватывающих документы и не-документы. – Н.Х.*) проистекает из используемой государственными органами практики выделения официально опубликованных для общественности материалов, в отличие от проектов, черновиков и другой информации, которая может никогда не публиковаться. Принципы прозрачности государственного управления требуют, чтобы

практически любая информация, созданная государственным органом или учреждением, могла быть раскрыта для общественности, однако такая информация может при этом так и не стать «документом». Именно поэтому соответствующий закон называется «Законом о свободе доступа к государственной информации» (Freedom of Information Act).

Причина, по которой государственные архивисты накануне и в период Второй мировой войны изобрели концепцию перечней с указанием сроков хранения (retention schedule), не была связана с управлением «документами»; это было сделано для того, чтобы массивы информации, которая никогда не станет «документами», не попадали на хранение в Национальные Архивы. Иными словами, перечни были изобретены для управления всей информацией, а не только «документами».

В путанице по вопросу о том, что такое «документы», во многом были виноваты сами архивисты. До 2001 года международная ассоциация специалистов по управлению документами и информацией ARMA International определяла «документы» как «зафиксированную информацию, вне зависимости от использованного носителя информации». По сути дела любая захваченная организацией информация, как созданная внутри организации, так и полученная ею извне, считалась «документом». (*С моей точки зрения, автор здесь не совсем точен. Примерно до 2005 года в США очень четко отделяли официальные документы организации от прочей информации, поскольку именно официальные документы организация обязана была представлять в суд. Всегда существовали четкие критерии, в соответствии с которыми документы отделялись от не-документов: а в законодательстве США имелось ясное определение понятия «государственный документ». Но вот после изменения законодательства границы, действительно, стали быстро размываться – Н.Х.*).

Именно этого определения придерживаются все американские и канадские специалисты по управлению документами, стремясь снизить риски и сделать информацию корпоративным активом. Поскольку любая имеющаяся в организации информация может быть истребована в ходе судебных разбирательств, то всей информацией следует управлять. Для информации не предусмотрено «безопасной гавани» только на том основании, что организация не считает её «документами». Документы и информация в равной степени должны раскрываться, и все они должны охватываться политиками, процедурами, программами обучения и подотчетностью – как корпоративной, так и персональной. Это касается, в том числе, текстовых сообщений, интернет-чата и сообщений электронной почты, в которых рассылаются свадебные фотографии.

С появлением стандарта ISO 15489, ставшего результатом консенсуса специалистов по управлению документами и архивистов многих стран мира, понятие «документ» определяется как «информация, созданная или полученная организацией или отдельным лицом, и сохраняемая в

дальнейшем в качестве доказательства и сведений, - для выполнения требований законодательства, или же в интересах деловой деятельности».

(*В российском ГОСТ Р ИСО 15489-1-2007, который, как в нем утверждается, «идентичен» международному стандарту ISO 15489-1:2001, это определение дано в несколько измененной редакции: «зафиксированная на материальном носителе идентифицируемая информация, созданная, полученная и сохраняемая организацией или физическим лицом в качестве доказательства при подтверждении правовых обязательств или деловой деятельности» - Н.Х.*)

Такое определение далеко отодвинуло понятие «документов» от моментов их создания (когда требуется управление контентом - document management) и распространения (где тоже требуется защита). Кроме того, оно потенциально не охватывает 90 процентов информации, создаваемой организацией для ведения деловой деятельности, включая большинство баз данных и электронную почту (*С моей точки зрения, это бездоказательное утверждение, не подтверждаемое американской же практикой – впрочем, перечитайте определение и судите сами. – Н.Х.*). И хотя стандарт ISO 15489 способствовал широкому распространению в мире идей и практики управления документами, понятие «документа» в нём сужено до такой степени, что следование стандарту для любой американской компании скорее приведет к увеличению риска, а не к его уменьшению.

Понятие «документа» является полезным, когда оно используется экспертами. Те, кто используют его, не имея надлежащей профессиональной подготовки в области управления документами, увеличивают риски своей организации и способствуют превращению её информационных активов в свалки токсичных отходов. Первое, с чего должна начинать всякая организация – это провести самооценку по «Модели зрелости для полномасштабного управления информацией» (Information Governance Maturity Model – *данная модель, информацию о которой можно найти здесь:* http://www.arma.org/r2/generally-accepted-br-recordkeeping-principles/metrics , *была разработана ассоциацией ARMA International в поддержку её «Общепринятых принципов делопроизводства» (Generally Accepted Recordkeeping Principles, GARP), см.* http://rusrim.blogspot.ru/search/label/GARP - *Н.Х.*), обратив первоочередное внимание на принцип подотчетности (Principle of Accountability).

ИТАЛИЯ: ЧТО ОБСУЖДАЮТ КОЛЛЕГИ? КОНФЕРЕНЦИЯ DIG.EAT 2014

Источник: сайт конференции http://www.digeat.it/digeat-2014-save-data-pr

Автор: Наташа Храмцовская

Тематика конференций иногда не менее интересна, чем сами доклады. Сопоставляя её с тематикой наших мероприятий, можно видеть, где мы идём впереди коллег из других стран и где отстаём.

22 мая 2014 года в Риме прошла бесплатная ежегодная конференция по вопросам оцифровки и перехода на использование электронных документов DIG.Eat 2014 под девизом «Спасти данные» (Save the Data).

Конференция была организована Национальной ассоциацией руководителей и специалистов по вопросам электронной сохранности (Associazione Nazionale per Operatori e Responsabili della Conservazione Digitale, ANORC, http://www.anorc.it/).

Программа (см. http://www.digeat.it/digeat-2014-save-data-pr), помимо открывающего и закрывающего пленарных заседаний, включала четыре межотраслевых «круглых стола»:

- Электронная идентификация. электронная подпись и биометрия (Identità digitale, firme elettroniche e biometria), организатор – Итальянская ассоциация биометрической и графометрической усиленной электронной подписи (Associazione Italiana Firma elettronica Avanzata Biometrica e Grafometrica, AIFAG, http://aifag.org/it);
- Сертификация систем, обеспечивающих долговременную сохранность электронных материалов (Certificazione del sistema di conservazione digitale), организатор – ANORC;
- Новые профессии в электронную эпоху (Le nuove professioni dell'era digitale), организатор – ANORC;
- Большие данные и облака (Big Data e Cloud), организатор – Генеральные Штаты электронной памяти (Stati Generali della Memoria Digitale, http://www.memoriadigitale.eu/);

и четыре «круглых стола» по отраслевой тематике:

- Электронные документы в медицине (Il documento elettronico in sanità);
- Будущее электронного правительства (Il futuro della PA digitale);
- Перевод в электронный вид налоговых документов (Dematerializzazione dei documenti fiscali);
- Электронные документы в банковском и страховом деле (Il documento informatico per banche e assicurazioni).

Как мне кажется, некоторые из этих тем вполне могли бы «освежить» программы наших отечественных конференций, как-то не отличающиеся в последнее время разнообразием.

ПРОЕКТ ОСНОВ ГОСУДАРСТВЕННОЙ КУЛЬТУРНОЙ ПОЛИТИКИ: ЧТО ГОВОРИТСЯ ОБ АРХИВАХ?

Источники: сайт Министерства культуры РФ / SecurityLab http://mkrf.ru/open-ministry/public-discussions/proekt-osnov-gosudarstvennoj-kulturnoj-politiki, http://www.securitylab.ru/news/452978.php

Министерство культуры на своем официальном сайте опубликовало для общественного обсуждения проект «Основ государственной культурной политики».

К культурному наследию народов Российской Федерации, среди прочего, отнесен Архивный фонд Российской Федерации, а в число задач государственной культурной политики входит и «систематизация, расширение и развитие существующего опыта использования» Архивного фонда.

Документ определяет информационную среду как всю «совокупность средств массовой информации, радио- и телевещание, сеть Интернет, распространяемые с их помощью текстовые и визуальные материалы, информация, а также созданные и создаваемые цифровые архивы, библиотеки, оцифрованные музейные фонды».

Вместе с тем, понятие «информационной среды» не должно сводиться исключительно к электронной среде.

Единое общее национальное электронное пространство знаний будет сформировано на основе:

- Оцифровки книжных, архивных, музейных фондов
- Создания национальной электронной библиотеки и национальных электронных архивов (по музыке, живописи и т.д.).

По вопросам, затрагивающим деятельность архивов, самым революционным стало предложение об обеспечении долговременной сохранности электронного контента:

Проект Основ государственной культурной политики, май 2014 года

Необходим также поиск решения проблемы сохранения электронной информации, особенно ресурсов Интернета. Аудиовизуальные документы, электронные ресурсы, электронные книги, сайты, социальные медиа и т.д. полностью меняют концептуальный подход к сохранению информации. К настоящему времени огромное количество ценнейших электронных информационных ресурсов уже потеряно. Огромные массивы информации русскоязычного сегмента Интернета, сформированные на таких ресурсах, как Instagram, YouTube, Facebook, Twitter, Google, передаются на хранение в хранилища США, в том числе в Библиотеку конгресса, в то время как в России они никак не сохраняются.

Работа «по созданию государственной программы сохранения электронной информации» отнесена к числу задач государственной культурной политики. В прессе (см.: http://www.securitylab.ru/news/452978.php) по этому поводу уточняется:

Россия обдумывает создание национальной базы хранения файлов русскоязычного сегмента Интернета

Руководитель администрации президента Сергей Иванов считает, что в России необходимо разрабатывать национальную систему хранения информации из Рунета. Он является главой рабочей группы по решению этого вопроса. Русскоязычный сегмент Интернета владеет огромным количеством информации, некоторая часть ее размещена на таких сервисах как Instagram, Facebook, Twitter, Google, YouTube, хранясь таким образом в США.

В документе архивы отнесены к числу «исторически сформировавшихся институтов, обеспечивающих различные виды культурной деятельности», чья история «ведется с античной эпохи» - (п.70.).

Задачей государственной культурной политики, согласно проекту, является «создание таких условий деятельности для этих институтов, когда органы управления, в том числе в финансовой и экономической сферах, при принятии соответствующих решений исходят из того, что музей, библиотека, **архив,** театр, филармония, концертный зал, дом культуры **выполняют важнейшую государственную и общественную функцию исторического и культурного просвещения и воспитания общества**».

Не умаляя значения функции архивов по историческому и культурному просвещению и воспитанию общества, следует отметить, что ограничиваясь одной лишь этой задачей, мы рискуем потерять возможности для возрождения архивного дела и архивов на новом уровне как одного из основополагающих элементов системы современного государственного управления страны.

Вопрос о том, какую роль играют архивы в современном обществе, для чего они создавались и создаются, в данном случае является ключевым. Принимая как данность утверждение, что архивы – это только просвещение и воспитание, мы тем самым принижаем значение архивов для государственного управление и деловой деятельности.

Ненадлежащее обеспечение сохранности архивных документов (любых, а не только документов Архивного фонда страны) наносит ущерб в первую очередь не историкам и исследователям, а рядовым гражданам и организациях, государству в целом. К сожалению, этот существенный момент в документе совершенно не отражен.

РИСКИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ: СБОЙ СЕРВИСА ХРАНЕНИЯ ДАННЫХ ОТБРОСИЛ НАЗАД ИССЛЕДОВАТЕЛЬСКИЕ ПРОЕКТЫ

Источник: сайт «Хроника высшего образования» (The chronicle of higher education) http://chronicle.com/blogs/wiredcampus/hazards-of-the-cloud-data-storage-services-crash-sets-back-researchers/52571

Статья Стива Коловича (Steve Kolowich) была опубликована 12 мая 2014 года на сайте «Хроника высшего образования» (The chronicle of higher education, http://chronicle.com) *в блоге WiredCampus*

На прошлой неделе облачное приложение для управления научными данными Dedoose (http://www.dedoose.com/) стало жертвой «разрушительного» технического сбоя, вследствие чего многие исследователи из различных уголков страны потеряли плоды больших усилий, вложенных в научные исследования, а часть данных, возможно, уже не удастся восстановить.

Компания SocioCultural Research Consultants, продающая услуги сервиса Dedoose, всё ещё продолжает попытки восстановить как можно больше материалов своих клиентов, и в своем блоге сообщила, что «подавляющее большинство» хранящихся на их платформе научных данных не пострадало. Тем не менее, последствия сбоя стали обескураживающими для ряда исследователей, отбросив назад проводимые ими исследования, - тем самым ещё раз высветив риски, которые появляются, когда управление данными доверяется третьей стороне.

В числе пострадавших – исследователь-социолог из Гарвардского университета Маргарет Фрай (Margaret Frye). Г-жа Фрай использовала Dedoose для сортировки и аннотирования журнальных статей о СПИДе и сексуальном влечении в южной части Африки. Но когда она вошла в систему вечером 6 мая, её «приветствовало» сообщение о том, что та не работает. Сначала г-жа Фрай не паниковали. «Ничто не намекало на утрату данных», - сказала она. Но когда Dedoose наконец снова заработал, у неё исчезли около 60 аннотированных текстов.

Г-жа Фрай и её коллега-исследователь все еще хранят исходные материалы на своих компьютерах, но свыше 100 часов труда, затраченного на «кодирование» - разметку журнальных статей с использованием метатегов и примечаний - были потеряны. Г-жа Фрай не питает больших надежд на то, что эти данные будут восстановлены поставщиком.

В аналогичную ситуацию попал доцент Университете Кентукки Джейсон Ричардсон (Jayson Richardson). Он и двое его студентов использовали Dedoose для «кодирования» объявлений о вакансиях на должности директоров начальных и средних школ, с тем, чтобы оценить, насколько хорошо в штате Кентукки стремящихся к карьерному росту руководителей в сфере образования готовят к тому, чтобы соответствовать критериям потенциальных работодателей. По его словам, «Последние две-

три недели мы занимались этой работой довольно плотно». Когда Dedoose рухнул, г-н Ричардсон и его коллеги потеряли результаты порядка 100 человеко-часов работы.

В социальных сетях стали накапливаться сообщения, поступающие от разъяренных исследователей. Многие критиковали компанию за поведение, которое они расценивают как нарушение доверия. «Похоже, вам удалось уничтожить исследовательский проект моей жены с бюджетом в 10 тысяч долларов», - написал на странице продукта в Facebook один из комментаторов.

Президент компании SocioCultural Research Consultants Эли Либер (Eli Lieber) в воскресенье 11 мая отказался дать интервью, сказав, что он и его коллеги в данный момент заняты решением проблемы. На прошлой неделе он написал сообщение в блоге, кратко подытожив случившееся.

«Эта разрушительная системная «коллизия» вечером во вторник 6 мая возникла в результате неожиданного сбоя одного из наших критически-важных системных сервисов Microsoft Azure, что повлекло за собой падение Dedoose», пишет г-н Либер. «Момент оказался особенно неудачным, поскольку как раз шёл процесс полного шифрования базы данных и её резервного копирования. В свою очередь процесс резервного копирования повредил всю нашу систему хранения».

Для многих ученых переход на хранение данных и управление ими с помощью облачных услуг представляется неизбежным. Университеты все больше доверяют хранение своих данных сторонним организациям, а в результате развития доступных широкому кругу пользователей услуг, таких как Google Docs, облако стало восприниматься как факт жизни.

«Своим студентам я говорю, что просто такова природа зверя», отмечает Ричардсон. «Любая системы хранения может отказать, а отдача от использования облачных услуг перевешивает риски, связанные с хранением результатов работы на далеких серверах».

Тем не менее, подобные инциденты служат суровым напоминанием о том, что риски существуют. «В своё время сохранение данных в облаке казалось мне способом сделать мои данные более защищёнными», сказала г-жа Фрай из Гарвардского университета. «Но теперь, после подобного опыта, я уже не так в этом уверена».

ЗМІСТ