ПЕРЕДМОВА

Випуск дайджесту присвячено досвіду установ світу щодо оброблення та зберігання електронних інформаційних ресурсів.

У публікації «Безопасное хранение данных» наведено основні риси, які характеризують електронні сховища даних**.**

У публікації «Соблюдение норм безопасности поможет сохранить информацию» розповідається, що Інтернет при бажанні можливо використовувати для тотального контролю. Для захисту інформації потрібно перенести ключові вузли управління Інтернет на територію країни.

У публікації «Тенденции развития угроз конфиденциальной информации в 2014 году» розповідається, що швидкість, з якою відбуваються зміни в сфері ІТ, не завжди дозволяють адаптувати системи забезпечення інформаційної безпеки (ИБ) до збільшення ризиків та нових загроз.

У публікації «Анализ концептуальной модели информационного хранилища» надані найбільш критичні, з точки зору процесу обробки даних та безпеки інформації, елементи інформаційного сховища.

У публікації «Модели нарушителей информационной безопасности» розглянуто можливі схеми дій зловмисників, для проникнення до інформаційної системи підприємства.

У публікації «Созданную у нас в стране инфраструктуру открытых ключей (PKI) невозможно применять в реальных бизнес-процессах» розповідається про необхідність внесення змін до діючої системи юридично значущої електронної взаємодії**.**

У публікації «США: 2015 год может стать годом хакерских атак на медицинские учреждения» розповідається, що хакери все частіше зламують відомчі комп'ютерні мережі з метою викрадення даних.

У публікації «Сбой облака Azure привел к отказу многих веб-сервисов» розповідається, що збій у облачній системі викликав відмову в роботі веб-сервісів в США, Європі, Японії, Бразилії та інших країнах.

У публікації «С гособлаками в США – понятно. С нашими гособлаками – тоже понятно, но иначе» розповідається про недоліки щодо регулювання хмарних послуг в держсекторі Росії.

У публікації «Проекты стандартов и технических отчётов, используемых в сфере управления документами, разрабатываемых ИСО» розповідається про розробку міжнародних стандартів ІСО серії 30300.

У публікації «Перелік міжнародних стандартів, проаналізованих НДІ мікрографії у ІІ півріччі 2014 року» надано Перелік міжнародних стандартів, проаналізованих НДІ мікрографії**.**

У публікації «Автоматический книжный сканер ЭЛАРобот Р-2» наведено технічні характеристики та комплектація сканера.

БЕЗОПАСНОЕ ХРАНЕНИЕ ДАННЫХ

Источник: http://www.itsec.ru/articles2/Oborandteh/bezopasnoe_hranenie_dannyh
Автор: Алексей Задонский, ведущий менеджер проектов в государственных структурах, компания Oracle

Развитие информационных технологий закономерно привело к модной сегодня архитектуре в построении информационных систем, к концепции электронных хранилищ данных. Эта закономерность продиктована появлением больших объемов информации, которую необходимо надежно хранить, своевременно обрабатывать и гибко анализировать.

Автор концепции хранилищ данных Билл Инмон определил их как «предметно ориентированные, интегрированные, неизменчивые, поддерживающие хронологию наборы данных, организованные с целью управления».

Характеристики хранилищ данных

Темой нашего рассмотрения будут вопросы обеспечения безопасности в построении таких систем, поэтому мы опустим многие интересные аспекты, связанные с программными и аппаратными средствами работы с хранилищами данных.

Укажем лишь на основные черты, характеризующие такие системы:

- весь основной объем информации накапливается в структурированных реляционных базах данных;
- все компьютерные ресурсы обычно находятся в выделенных, хорошо охраняемых серверных комнатах (так называемые центры обработки данных);
- хранилища - это не просто мертвый склад информации, но и наличие большого числа тесно связанных с ним прикладных и обслуживающих систем. Например, ПО для архивирования информации, управления, системы обработки типа ETL (extraction, transformation, loading), прикладные системы, которые, собственно, и порождают исходные данные, и т.д.;
- средний размер хранилища составляет 1 Тбайт и выше, что диктует серьезное отношение к сетевой инфраструктуре и системам хранения и обработки информации.

Как и везде, в вопросах построения систем информационной безопасности необходим комплексный взвешенный многоуровневый подход, поскольку недоработка в одном вопросе способна свести на нет все усилия в остальных направлениях.

Рассмотрим пример построения системы защиты типичного хранилища данных на основных уровнях.

Телекоммуникационная инфраструктура

Ясно, что территория хранилища должна быть максимально закрыта от попыток проникновения снаружи, поэтому при необходимости удаленного доступа обязательно шифрование трафика. И даже внутренняя сеть управления (которую желательно выделить отдельно с помощью VLAN или даже на физическом уровне, то есть управлять серверами по отдельным сетевым интерфейсам) должна шифроваться (SSH, IPSec, SSL и т.д.). Обязательно шифрование данных, выходящих наружу с использованием контроля целостности (MD5, SHA1). Обычно из-за больших объемов обрабатываемой информации не используют шифрование на уровне ядра сети из-за проблем с производительностью.

Разные сетевые протоколы и сетевые взаимодействия требуют наличия средств защиты на своем уровне.

Обычный транспортный уровень требует наличия следующих средств от подмены адресата и средств защиты:

- организация VLAN, Port Security и т.д.;
- proxy-серверы на периметре, анализирующие прикладной уровень взаимодействия;
- системы предотвращения вторжений (IDS/IPS) и др.;
- антивирусная защита и т.д.

Уровень Fibre Channel также требует своей защиты, например Fibre Channel Authentication Protocol, Switch Link Authentication Protocol и т.д.

На уровне Storage Area Networking применяется Virtual SAN, маркировка LUN и др.

Операционные и прикладные системы

Если речь идет об операционных и прикладных системах, то необходимо реализовать основную задачу: "Критичные данные должны быть доступны только уполномоченным лицам, только тем способом, который

разрешен политикой безопасности, и только с помощью средств, определенных политикой безопасности". В частности, это включает механизмы контроля запуска только авторизованных программ авторизованными пользователями.

Аутентификация и контроль доступа

Естественно, что при работе на всех уровнях необходима авторизация и многофакторная аутентификация. Причем желательно, чтобы эта аутентификация была поддержана не только на уровне операционных и прикладных систем, но и на уровне доступа к операциям баз данных как основных источников информации.

Необходимы прикладные средства и организационные меры по распределению прав администраторов (баз данных, прикладных и операционных систем) и специалистов по информационной безопасности.

Аудит событий

Принцип неотвратимости наказания в большинстве случаев является наиболее действенным методом обеспечения безопасности. Поэтому как минимум необходим многоуровневый аудит (независимый от администраторов) того, что происходит на всех уровнях. Здесь есть решения на разных уровнях. Для аудита того, что происходит в телекоммуникациях, прикладных и операционных системах можно использовать, например, решения ArcSight, NetForensics (чаще продающиеся под маркой корпорации Cisco Systems), CA Security Command Center. Но вдобавок к этому потребуется отдельный глубокий аудит того, что происходит на уровне баз данных, а это можно решить дополнительными средствами.

Защита баз данных

Важнейшим этапом обеспечения безопасности является защита от администраторов баз данных. Все мы знаем о наличии больших объемов конфиденциальной информации на черном рынке. Такую информацию очень трудно украсть через амбразуру прикладных систем (если, конечно, они грамотно написаны). Большинство взломов осуществляется путем непосредственного копирования информации из базы данных или использования незащищенных архивных копий.

Разграничение доступа к базам данных

Средствами СУБД должна обеспечиваться возможность реализации мандатного способа доступа, когда все пользователи делятся на уровни и группы в соответствии с уровнем доверия к ним, а также в соответствии с принадлежностью их к той или иной группе субъектов. Должна быть возможность в одной базе данных хранить информацию с разной степенью конфиденциальности и при этом ограничивать доступ к данным в соответствии с категориями допуска.

Необходимо реализовать лозунг: "Сделайте так, чтобы администратор баз данных не узнавал о финансовых результатах раньше генерального директора!" Для этого нужны развитые средства управления доступом к базам данных, поддерживающие строгую аутентификацию и позволяющие ограничивать права администраторов и приложений по разным параметрам.

Такое решение существует для баз данных Oracle. Здесь реализован механизм управления администратором базами данных без возможностей просмотра и работы с самим содержимым. При этом можно управлять тем, кто и какие команды может выполнять. Например, при работе аналитика, делающего выборку из базы, появляются критические данные (социальный номер и др.), и такие события следует заносить в протокол безопасности. В качестве другого примера можно предложить запрет на изменение конфигурации системы удаленно. В этом случае изменения конфигурации производятся из локальной консоли, когда авторизованный пользователь находится под прицелом видеокамеры, а суровый охранник на входе записывает время и фамилию вошедшего.

Организация хранилища данных – дорогостоящий и комплексный проект, в котором велика роль организационных процессов. Но компании идут на такие проекты, поскольку осознают, что информация является стратегической составляющей их бизнеса. А построение комплексной многоуровневой системы безопасности в этом проекте является одним из приоритетных направлений.

Физическая безопасность

Конечно, нужна и физическая безопасность, включающая в себя как ограничение физического доступа (охрана, видеокамеры, аутентификация доступа в помещения), так и защиту носителей данных. Если для жестких дисков в серверах шифрование часто является неоправданным, то для отторгаемых носителей (например, архивы на магнитных лентах) криптозащита является обязательным средством.

СОБЛЮДЕНИЕ НОРМ БЕЗОПАСНОСТИ ПОМОЖЕТ СОХРАНИТЬ ИНФОРМАЦИЮ

Источник: http://rostec.ru/news/4514765

Насколько опасна беспечность в Сети и почему информационная безопасность стала частью государственной политики – об этом в интервью «Независимой газете» рассказал доктор технических наук, заместитель генерального директора КРЭТ Игорь Жуков.

– В современном обиходе столько электронных приспособлений, призванных облегчить человеку жизнь, что уже трудно представить те высоты, которые способна достичь инженерная мысль в нашем желании управлять автоматизированными системами. Но все-таки можно что-то предвосхитить?

– На мой взгляд, даже не надо сильно предугадывать. Результаты таких исследований регулярно публикуются. Управление голосом и жестами –

реальность уже вчерашнего дня. Впереди – управление интеллектуальными системами мыслью. Поиски разнообразных способов информационно-технологического воздействия на автоматизированные системы не замирают ни на секунду. Причем со стороны желающих как облегчить жизнь человеку, так и усложнить.

Это – бесконечная спираль развития. Даже привязка к биометрическим признакам – голосу, радужной оболочке глаза, отпечаткам пальцев – имеет уязвимости и механизмы обхода. Все они преобразуются в цифровой код, который можно сфальсифицировать и представить проверяющей системе вместо настоящих биометрических данных.

– Получается, чем совершеннее наша техника, тем меньше возможностей ее защитить?

– Не защитить, я бы сказал, а обезопасить. Появление новых болезней и вирусов ведь не означает, что мы совсем перестаем выходить на улицу, общаться или надеваем какие-то защитные костюмы. В такой ситуации нам помогают личная гигиена и определенные профилактические процедуры. Соблюдение даже элементарных норм безопасности при обращении с электронными системами поможет сохранить информацию и деньги. Например, если вы пытаетесь снять деньги в банкомате, установленном в подворотне, будьте готовы, что аппарат поставили там с целью получить данные карточки ее беспечного владельца.

Если расплачиваетесь кредитной картой, не выпускайте ее из вида. Иначе можете оказаться в зоне риска, данные легко копировать с помощью специального устройства. Мои хорошие знакомые во время отдыха в Европе остались без денег спустя полчаса после того, как расплатились в ресторане и позволили официанту унести карточку из зоны видимости.

Периодически менять пароль своего электронного почтового ящика – это так же естественно, как по утрам чистить зубы.

Знание современных угроз технологического свойства поможет обращать внимание на детали. Допустим, если ваш мобильник быстро разряжается, значит, определенно что-то с ним происходит. Случайностей не бывает. Возможно, проблема в аккумуляторе, а возможно, причиной служит вирус или другая вредоносная программа, которая отправляет вашу персональную информацию кому-то другому. Причем специальной разработки для этого не потребуется. На планшетах и смартфонах уже есть функция, обеспечивающая передачу данных. И элементарное изменение в программном обеспечении легко может сделать доступной для чужих глаз, например, вашу личную СМС-переписку.

– Например, у меня очень быстро разряжается телефон, особенно в каких-то определенных зонах. Что это может означать и как можно себя обезопасить?

– Универсальных решений нет, надо изучать ситуацию предметно. Действительно телефон быстро разряжается или вам так кажется? Но первое, что посоветую, перезагрузите телефон. Если во временных файлах есть вредоносная программа, по крайней мере, у вас будет шанс ее сбросить.

Здесь так же, как на обычный компьютер, имеет смысл загрузить программную защиту, которая отслеживает контроль целостности вашего программного обеспечения и данных.

– Значит, приобретая высокотехнологичную технику, надо тут же думать о ее информационной защите? И стопроцентной гарантии безопасности все равно нет?

– Абсолютной защиты не существует. И вряд ли она нужна. Потому что цена такой защиты становится чрезмерной. Дело не только в финансовой стороне вопроса. Забота о безопасности – это всегда определенное неудобство. При определенных условиях жизнь становится относительно безопасной, но абсолютно невыносимой.

А в целом вы правы: все уязвимо и несет потенциальные риски. На что-то можно не обращать внимания, а что-то несет угрозу национальной безопасности. И не обращать внимания на это уже нельзя. Мы еще задолго до Сноудена старались доходчиво объяснить уязвимость современных радиоэлектронных информационных систем.

– И все же откровения Сноудена открыли для вас что-то новое в техносфере?

– В техносфере – нет. Но Сноуден первым вслух и громко сказал то, о чем раньше говорили шепотом: Интернет при желании может использоваться для тотального контроля. Сегодня США, по сути, продолжают удерживать власть над важнейшими системами Интернета, многие ключевые узлы и серверы мировой Сети находятся на их территории, Штаты контролируют львиную долю наиболее популярных доменов. Это значит, что существенная часть интернет-трафика российских пользователей проходит через их объекты управления. Поэтому и становится актуальным создание альтернативных систем защищенного доверенного информационного общения.

– А почему именно сейчас мы вдруг этим озаботились?

– Согласен, инертность имела место. Да и западные партнеры не особенно проявляли себя. Но после того как США фактически признали, что они прослушивают первых лиц государств даже из числа своих союзников, не реагировать на это уже было невозможно. Мне кажется, общество и сегодня еще недостаточно понимает всю опасность информационной зависимости от другой страны.

– Стало быть, Эдвард Сноуден все-таки сыграл роль детонатора?

– Безусловно. Ну и Ассанж еще.

– И теперь пользователей Интернета периодически запугивают созданием национальной системы, которая будет отрезана от мировой Сети…

– С точки зрения безопасности независимый сегмент Интернета, конечно, в России создавать нужно. Равно как и национальную платежную систему. Серверы – хранилища информации должны находиться под контролем своего, а не иностранного государства. В Китае, например, уже

предпринимаются попытки защитить информацию и перенести ключевые узлы внутрь страны.

– Как быстро можно создать у нас такую систему? И сколько денег потребуется?

– Поверьте, это потребует не таких уж длительных сроков или сверхвысоких бюджетов. Но, с точки зрения специалистов по информационной безопасности, такая задача должна быть поставлена и решена. Некоторые защитные механизмы в нашей стране закладываются не только на законодательном, но и на технологическом уровне. События на Бушерской АЭС, когда программный вирус стал размножаться на ядерном объекте Ирана, наглядно продемонстрировали значимость информационной безопасности. Это разумно, что сейчас в нашей стране создаются процедуры защищенного ИТ-взаимодействия виртуальных и реальных информационных объектов. Изначально, при проектировании, в оборудование с программным управлением закладываются соответствующие механизмы защиты и контроля. В том числе для станков с программным управлением, подключаемых к Интернету. Методы безопасного использования импортного программного обеспечения и электроники также существуют.

– Но если говорить о защите персональных данных, можно их каким-то образом сохранить, если они уже оказались в виртуальном пространстве?

– Это отдельная тема для разговора, которая уже больше связана с соцсетями. Если ваш, мой и чей-то еще «информационный профиль» связан с местом жительства, с мобильным телефоном и т.д. – это информация, которая с большой долей вероятности уже записана в соответствующем центре обработки данных. Даже если вы меняете что-то, то все равно остаетесь объектом информационного мира, и вас легко идентифицировать. Когда вы приходите на работу в разной одежде, вас же все равно узнают. Просто еще раз повторю, что каждый человек должен давать отчет своим действиям. Когда люди выкладывают фотографии и информацию о себе в сетях, это все равно что личный альбом вынести на улицу и показывать всем подряд. И если пренебрежение обычными человеческими ценностями приводит к тому, что ты сам выложил и бросил на проезжей части свои личные данные, тогда на что ты рассчитываешь? На что обижаешься?

ТЕНДЕНЦИИ РАЗВИТИЯ УГРОЗ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В 2014 ГОДУ

Источник: http://www.top-personal.ru/officeworkissue.html?350
Автор: В.Я. Ищейнов В.Я. Ищейнов, к.т.н., доцент РГГУ

Появление новых информационных технологий (IT) и развитие мощных компьютерных систем хранения и обработки конфиденциальной (и не только) информации повысили уровни защиты и вызвали необходимость в том, чтобы защита росла вместе со сложностью архитектуры хранения данных. Быстрота, с которой происходят изменения в сфере IT, не всегда позволяет адаптировать системы обеспечения информационной безопасности (ИБ) к возрастающим рискам и новым угрозам. Таким образом, происходит разрыв между существующим и необходимым состоянием ИБ обусловленный многими факторами, к основным из которых относятся: виртуализация, облачные технологии, дистанционное банковское обслуживание (ДБО), политика консьюмеризации (BYOD) – использование личных планшетов, смартфонов, коммуникаторов, ноутбуков, домашних компьютеров в корпоративных сетях - и каждая из этих технических и технологических систем представляют собой потенциальную точку входа угроз и, соответственно, утечки конфиденциальной информации. [1] По данным исследований аналитического центра компании InfoWatch картина утечки конфиденциальной информации неоднородна по различным отраслям – банковское обслуживание, страховые компании, коммерческие структуры, государственный сектор. [2] Динамика утечек и, соответственно, угроз конфиденциальной информации имеет явную тенденцию к росту, что коррелируется с ростом разрыва в необходимости уровня защиты конфиденциальной информации.

За 2012 год в мире зафиксированы и опубликованы в средствах массовой информации (СМИ) 934 случая утечки конфиденциальных данных, что на 16% выше показателя 2011 года. Официально заявленные прямые убытки кредитно – финансовых компаний от утечек конфиденциальной информации в первом полугодии 2012 года составили более 37,8 млн долларов. Скомпрометировано более 1,8 млрд записей, в том числе финансовые и персональные данные (ПДн). В 2009 году 41% респондентов отмечали повышение количества внешних угроз. [3] К 2011 году количество таковых возросло уже до 72%. В 2012 году число респондентов, ощутивших рост внешних угроз, составило 77%. К тому же 46% респондентов констатировали увеличение и внутренних уязвимостей конфиденциальной информации. Экстраполируя динамику числа утечек и разрыв в уровне необходимой защиты конфиденциальной информации, можно сделать вывод об увеличении угроз в 2014 году на 5-8% по сравнению с 2013 годом. Это

связано в первую очередь с тем, что в современных центрах обработки конфиденциальной информации виртуальные машины динамически перемещаются между физическими устройствами, исходя из потребностей вычислительных операций, и общее управляющее программное обеспечение полностью автоматизирует все рабочие потоки, связанные с подключением и текущим управлением этих виртуальных машин. Когда виртуальные машины развернуты и динамически перемещаются, сложно гарантировать, что процедуры безопасности защиты от угроз будут успевать за ними. Системы будут по-прежнему иметь свой уникальный брандмауэр, свои требования по защите от несанкционированного проникновения и предотвращению угроз безопасности, которые должны работать независимо от того, когда машины с разным уровнем доверия разделяют общее пространство в одной физической машине. Это означает, что необходимо не только виртуализировать систему безопасности для каждой уникальной виртуальной машины, но и быть готовым к возможности горизонтального распространения угроз от виртуальных машин низкого уровня доверия в виртуальные машины более высокого уровня доверия через хост.

Таким образом, развитие облачных сервисов, заменяющих автономные цифровые устройства, должны обеспечить соответствующий уровень защиты от угроз, однако это требует преодоления проблем, связанных с объединением ресурсов мультиарендой и эластичностью облачных вычислений. Основными источниками угроз, имеющими тенденции к их росту являются:

- несанкционированный доступ (НСД);
- киберпреступность;
- IT-консьюмеризация;
- социальная инженерия;
- поддельное программное обеспечение (ПО);
- промышленный и государственный шпионаж.

НСД. Несанкционированный доступ в сочетании с кражей данных, как правило, называют взломом. Необходимо отслеживать каждый случай НСД к ресурсам организации или учреждения. Это осложняется тем, что происходит экспоненциальный рост доступности полосы пропускания, поэтому отследить нужные события в трафике проблематично. Крупные организации такие инциденты воспринимают серьезно, а компании малого и среднего бизнеса проявляют недостаточную осведомленность, что приводит к росту потенциальных угроз.

Киберпреступность. Киберпреступники используют широкий арсенал средств, начиная от взлома устройств и заканчивая атаками через социальные медиа. При этом увеличение угроз наблюдается у пользователей популярных мобильных платформ – Android и iOS. В период с 2007 по 2012 годы зафиксирован 35%-ный рост числа угроз, связанных с использованием Интернета. Это свидетельствует о том, что рост числа угроз – вирусных, фишинговых и т. п., из года в год только растет. Киберпреступники, как правило, сначала рассылают грамотно составленные фишинговые

электронные письма, предлагающие ничего не подозревающим пользователям открыть вредоносное вложение, или же применяют более сложную «стратегию водопоя», заранее заражая сайты, которые, по мнению злоумышленников, пользователи могут посетить. Заполучив учетные данные пользователя, киберпреступники проникают в сеть организации и внедряют вредоносное ПО. При этом определяются слабо защищенные привилегированные учетные записи, через которые происходит контроль над системой, что в дальнейшем позволяет осуществлять доступ к конфиденциальной информации и ее утечке. Уже сейчас сетевыми подключениями обзаводятся автомобили и даже импланты, которые передают удаленно информацию о состоянии больных. Все это приведет к тому, что кибератаки станут опасны и для здоровья людей.

IT-консьюмеризция. С распространением IT-консьюмеризации встал вопрос об управлении, поддержке и защите пользовательских устройств. Мобильность и широкий спектр устройств в корпоративных сетях вызовут новые угрозы в области конфиденциальной информации. Только в прошлом году со счетов фирм было украдено свыше 1 млрд долларов. К тому же угрозы создают проблемы не только для конечных пользователей, но и для поставщиков средств защиты конфиденциальной информации.

Социальная инженерия. Атаки с использованием методов социальной инженерии несут большие потери для конфиденциальной информации малого и среднего бизнеса. Это происходит в связи с недостаточностью средств, выделяемых на обеспечение безопасности данных. Базовых политик информационной безопасности становится недостаточно, в связи с чем необходимы более современные технологии защиты от угроз социальной инженерии, такие как мониторинг сети, предотвращение утечек данных и анализ лог-файлов.

Поддельное ПО. На сегодняшний день более 80% атак злоумышленников базируется на использовании уязвимостей в прикладном ПО. Для их снижения необходима установка обновлений ОС и ПО, а также необходимы процедуры управления изменениями. Аксиома – чем старше используемое ПО, тем больше уязвимостей для него будет найдено. К тому же наблюдается рост количества фальшивых антивирусных программ, что стало одной из наиболее распространенных и опасных интернет-угроз.

Промышленный и государственный шпионаж. Анализ источников показывает, что внешние угрозы конфиденциальной информации для крупных промышленных предприятий не так существенны, как угрозы внутренние. От внешних угроз уже существует достаточно эффективная защита, а вот угроза инсайдеров весьма актуальна и ее снижения ожидать не стоит. Причиной увеличения угроз в 2014 году является массовое использование мобильных устройств, к чему службы государственных и муниципальных организаций оказались не готовы.

Вывод. Угрозы конфиденциальной информации видоизменились за последние годы, а рост безопасности замедлился. Рассматривая тенденции развития угроз конфиденциальной информации, можно сделать вывод, что

они растут, выходя за рамки любой профилактики информационной безопасности. В 2014 году кибератаки на госструктуры и компании возрастут. Профессиональные киберпреступники станут более агрессивными, увеличится кража денег и конфиденциальной информации в социальных сетях, поскольку пользователи до сих пор доверяют этим ресурсам.

1 Колосков С., Абашев А., Мельник Р. Риски и тенденции в сфере обеспечения Информационной безопасности. - М.: «Информационная безопасность», №1, 2013, с.8.

2 Исследование аналитического центра компании Info Watch. Утечки корпоративной информации и конфиденциальных данных. – М.: «Информационная безопасность», №3, 2013, с.8.

3 Колосков С., Абашев А., Мельник Р. Риски и тенденции в сфере обеспечения Информационной безопасности. - М.: «Информационная безопасность», №1, 2013, с.8.

АНАЛИЗ КОНЦЕПТУАЛЬНОЙ МОДЕЛИ ИНФОРМАЦИОННОГО ХРАНИЛИЩА

Источник: http://inf-bez.ru/?p=1209

Одной из неотъемлемых составляющих частей практически любой системы организационного управления или корпоративной сети предприятия любого масштаба является система информационного хранилища, поэтому, прежде чем анализировать информационное хранилище как некоторый объект информатизации подлежащий защите, давайте проанализируем структуру информационного хранилища и выделим наиболее критичные с точки зрения процесса обработки данных и безопасности информации элементы. И так, давайте начнем наш анализ. В основе концепции хранилища данных лежат две основные идеи – интеграция разъединенных детализированных данных в едином хранилище и разделение наборов данных и приложений, используемых для оперативной обработки и применяемых для решения задач анализа. Концептуально модель хранилища данных можно представить в виде схемы представленной на рисунке 1.

Данные из различных источников помещаются в хранилище данных, а описания этих данных в репозиторий метаданных. Конечный пользователь, используя различные инструменты (средства визуализации, построения отчетов, статистической обработки и т.д.) и содержимое репозитория, анализирует данные в хранилище.

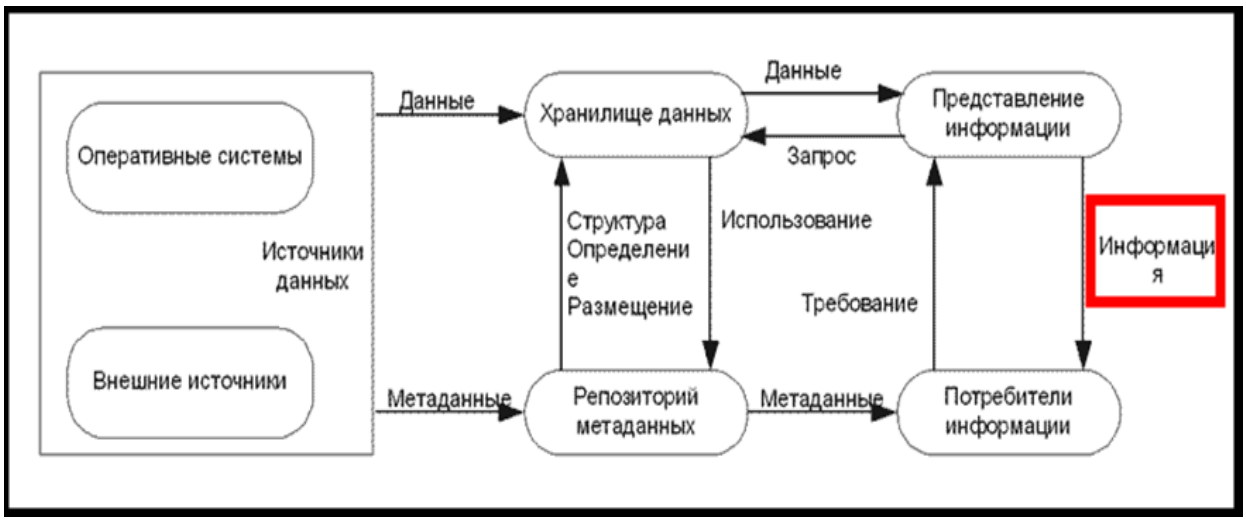


Рис. 1 Модель хранилища данных

Физическая реализация приведенной концептуальной схемы может быть самой разнообразной. Ниже приводятся наиболее часто встречающиеся подходы.

1. Виртуальное хранилище данных – это система, представляющая интерфейсы и методы доступа к регистрирующей системе, которые эмулируют работу с данными в этой системе, как с хранилищем данных. Виртуальное хранилище данных можно организовать, создав ряд представлений (view) в базе данных, либо применив специальные средства доступа.

Главными достоинствами такого подхода являются:

- Простота и малая стоимость реализации.
- Единая платформа с источником информации.
- Отсутствие сетевых соединений между источником информации и хранилища данных.

Однако недостатков у него гораздо больше, чем достоинств. Создавая виртуальное хранилище данных, создается не хранилище как таковое, а иллюзия его существования. Структура хранения данных и само хранение данных не претерпевает изменений, и остаются проблемы:

- Производительности.
- Трансформации данных.
- Интеграции данных с другими источниками.
- Отсутствия истории.
- Зависимость от структуры основной БД.
- Зависимость от доступности основной БД.
- Чистоты данных.

2. Витрина данных (Data Mart) представляет собой узкоспециализированную подсистему хранилища данных (Data Warehouse), его отдельный элемент.

Если же некоторая область деятельности компании практически не связана с другими, то можно построить независимую витрину данных, работающую автономно, без привязки к централизованному корпоративному хранилищу. Или начать автоматизацию компании не с создания корпоративного хранилища данных, а с независимой витрины данных по предметной области, наиболее востребуемой в компании. В этом случае под витриной данных понимается узко специализированное хранилище данных, обслуживающее одно из направлений деятельности компании.

Витрины данных по определению намного дешевле и проще в построении, чем хранилища данных, их внедрение не требует больших временных затрат и приносит быстрый и ощутимый эффект. В то же время необходимо понимать, что при таком подходе независимые витрины данных не будут создавать единой информационной системы компании, не будет единой системы извлечения информации, консолидации, управления и обслуживания.

Если компания небольшая, она может смело идти на создание автономных витрин данных. Если же компания крупная, то создание автономных витрин данных должно координироваться из единого центра с тем, чтобы в итоге придти к созданию единого хранилища данных компании.

Создание витрины данных это создание соответствующей базы данных и системы ее загрузки. Если создание базы данных вопрос чисто технический, создание системы загрузки представляет основную сложность. Эта система содержит три этапа:

- извлечение данных из исходных систем;
- преобразование их в требуемую форму;
- загрузка подготовленных данных в витрину.

Извлечение данных требует точного знания структуры исходных систем. Структуры и взаимосвязи таблиц, структуры информации в исходной системе. Необходимо четко знать из каких таблиц и полей необходимо извлекать данные и какова структура этих данных.

Исходная система изначально никак не ориентирована на работу с витриной данных и данные, извлекаемые из нее, не предназначены для непосредственного использования и должны пройти ряд преобразований. Процесс этих преобразований зависит и от структуры исходных систем, и от требований к самой витрине данных, он может заключать в себе множество функций:

- Создание агрегатных данных
- Изменение форматов данных.
- Проверку достоверности и целостности данных.
- Удаление избыточных данных

Все эти преобразования осуществляются только на этапе ввода данных в витрину, что обеспечивает высокую скорость извлечения данных из витрины и наилучшее представление этих данных с точки зрения пользователя. В конечном итоге это приводит к лучшему информационному

обеспечению пользователя, и способствуют быстрому принятию им правильных управленческих решений.

Данные в витрине должны соответствовать данным исходных систем, которые, естественно, изменяются со временем. Поэтому инструменты, осуществляющие преобразования и загрузку данных в витрину должны запускаться периодически при определенных изменениях данных исходных систем и/или автоматически по определенному расписанию.

Из изложенного вытекает довольно важный вывод. Нельзя купить готовую витрину данных для своей компании. Витрина данных это эксклюзивный заказной продукт, который должен создаваться непосредственно под конкретную компанию, под всю ее специфику.

Плюсами витрин данных являются:

- Простота и малая стоимость реализации.
- Высокая производительность за счет физического разделения регистрирующих и аналитических систем, выделения загрузки и трансформации данных в отдельный процесс, оптимизированной под анализ структурой хранения данных.
- Поддержка истории.
- Возможность добавления метаданных.

3. В последнее время все более популярной становится идея совместить концепции хранилища и витрины данных в одной реализации и использовать хранилище данных в качестве единственного источника интегрированных данных для всех витрин данных — глобального хранилища данных. На первом уровне расположены разнообразные источники данных – внутренние регистрирующие системы, справочные системы, внешние источники (данные информационных агентств, макроэкономические показатели). Второй уровень содержит центральное хранилище данных, куда стекается информация от всех источников с первого уровня, и, оперативный склад данных (ОСД). Оперативный склад не содержит исторических данных и выполняет две основные функции. Во-первых, он является источником аналитической информации для оперативного управления и, во-вторых, здесь подготавливаются данные для последующей загрузки в центральное хранилище. Под подготовкой данных понимают их преобразование и осуществление определенных проверок. Наличие ОСД просто необходимо при различном регламенте поступления информации из источников. Третий уровень в описываемой архитектуре представляет собой набор предметно-ориентированных витрин данных, источником информации для которых является центральное хранилище данных. Именно с витринами данных и работает большинство конечных пользователей.

На основе анализа основных видов информационных хранилищ, можно сделать вывод о том, что в настоящее время наиболее распространена реализация глобального хранилища данных, характеризующегося как единственный источник интегрированных данных для всех витрин данных.

МОДЕЛИ НАРУШИТЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Источник: http://inf-bez.ru/?tag=%D0%B8%D0%BD%D1%84%D0%BE%

Рассмотрим более подробно возможные схемы действий злоумышленника, использующего удаленное проникновение в информационную систему предприятия. Начнем с самого простого варианта. Это хакер-одиночка, обладающий стандартным персональным компьютером, с модемным (реже выделенным) выходом в Интернет. Данный тип злоумышленников очень сильно ограничен в финансовом плане и необязательно обладает глубокими знаниями в области компьютерных технологий.

Закон и информационные системы предприятий

Федеральным законом № 152 «О персональных данных», главой 14 Трудового кодекса Российской Федерации и Постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781 установлены правила в отношении порядка обработки и обеспечения конфиденциальности персональных данных собственных работников и сторонних физических лиц, персональные данные которых обрабатываются в организации.

Причины утечек в корпоративных сетях

В настоящее время известен достаточно обширный перечень угроз безопасности информационных систем, содержащий сотни позиций. Перечень угроз, оценки вероятностей их реализации, а также модель нарушителя служат основой для анализа риска реализации угроз и формулирования требований к системе защиты информационной системы. Кроме выявления возможных угроз, целесообразно проведение анализа этих угроз па основе их классификации по ряду признаков.

Персонал как неотъемлемая часть корпоративных информационных систем

Сегодня деятельность любой организации тесно связано с использованием информации в различных ее видах, и, как правило, основная ее часть представляет собой электронную информацию, которая обрабатывается посредством информационных систем. С развитием информационных технологий стала возможна организация корпоративных сетей организаций, включающая в себя локальные сети и автономные компьютеры. Помимо явных преимуществ такой переход несет и ряд проблем.

Злоумышленники в информационно-телекоммуникационных системах

В качестве потенциального злоумышленника информационной безопасности рассматривается лицо или группа лиц, состоящих или не

состоящих в сговоре, которые в результате умышленных или неумышленных действий могут реализовать разнообразные угрозы информационной безопасности, направленные на информационные ресурсы и нанести моральный и/или материальный ущерб интересам ИТКС. По характеру воздействия, угрозы разделяются на: случайные и преднамеренные; активные и пассивные.

Обзор уязвимостей типовых корпоративных сетей организаций

Уязвимостью – называют любую характеристику информационной системы, использование которой нарушителем может привести к реализации угрозы. При этом неважно, целенаправленно используется уязвимость или это происходит ненамеренно. В качестве злоумышленника может выступать любой субъект корпоративной сети, который попытался осуществить попытку несанкционированного доступа к ресурсам сети по ошибке, незнанию или со злым умыслом.

Типы моделей управления доступом

Модель конечного автомата описывает систему как абстрактную математическую машину. В этой модели переменные состояния представляют состояния машины, а функции перехода описывают способ изменения переменных. Напомним, что модель управления доступом имеет дело только с наиболее существенными переменными состояния, влияющими на безопасность, и потому намного проще, чем полная модель конечного автомата для данной системы.

Сущность моделей управления доступом

в достижении высокой степени безопасности АС зависит от тщательности разработки и реализации управления имеющимися в системе механизмами безопасности. Как показывает практика, наилучшие результаты в создании безопасных систем достигаются в том случае, когда разработчики системы учитывают требования безопасности уже на этапе формулирования целей разработки и самых общих принципов построения системы.

Мандатное разграничение доступа как элемент защиты информации в информационных системах

Защита информационных систем – непростая задача, и в особенности это относится к защите данных. Технологии безопасности всегда отставали от других областей, таких как сетевые и коммуникационные средства. Многие модели, предложенные еще в середине – конце 80-х годов, только сейчас начинают активно внедряться в коммерческие продукты. В среде защиты информационных систем в нынешнее время мандатные модели.

Организационные меры по защите информации

Да конечно, использование всевозможных технических новинок и программно-аппаратных средств по защите информации в любой организации необходимо (не забывайте только что они все по возможности должны иметь сертификат ФСТЭК и т.д.). Однако не стоит забывать о таком необходимом просто способе защиты информации - как различного рода организационные мероприятия, своевременное обучение сотрудника и постоянный контроль за качеством.

Обзор и характеристики программных средств по защите информации

На современных предприятиях с информационными системами различного типа первой группы защищенности наиболее часто используемыми программными средствами защиты являются следующие: антивирусы; средства от НСД. Антивирусы. В современных компаниях используются антивирусные программы таких производителей, как Dr.Web, Антивирус Касперского, SymantecEndpointProtection и т.д. Средства от НСД. Среди программных средств защиты от НСД можно выделить следующие:

–«SecretNet»;

–«DallasLock».

Обзор программно-аппаратных средств по защите информации

На современных предприятиях с РИС первой группы защищенности наиболее часто используемыми программно-аппаратными средствами защиты являются следующие: межсетевые экраны; средства от НСД; маршрутизаторы. Межсетевые экраны. Межсетевой экран — программный или программно-аппаратный комплекс, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами. Среди межсетевых экранов, сертифицированных ФСТЭК, можно выделить Cisco, ALTELL NEO.

СОЗДАННУЮ У НАС В СТРАНЕ ИНФРАСТРУКТУРУ ОТКРЫТЫХ КЛЮЧЕЙ (PKI) НЕВОЗМОЖНО ПРИМЕНЯТЬ В РЕАЛЬНЫХ БИЗНЕС-ПРОЦЕССАХ

Источник: http://www.pcweek.ru/its/blog/its/6954.php Автор: Андрей Колесов

Как обстоят дела с юридически значимым электронным взаимодействием? Сразу скажу: для меня в этом тезисе нет никаких особых откровений. Я именно так себе и представлял положение дел в сфере, которая у нас называется "юридически значимое электронное взаимодействие". Представление о неблагополучности дел в этой сфере базируется на двух моментах:

1. Даже самый простой анализ организации этого самого ЮЗЭВ показывает насколько созданная система сложная и неудобная.

2. Теоретический анализ (п.1) подтверждается как отзывами конкретных бизнес-пользователей, так и долгим отсутствием хоть какой-то официальной статистики по состоянию дел в этой сфере.

Но при этом – что характерно – все участники данного рынка со стороны поставщиков (ФНС, операторы ЭДО, удостоверяющие центры,

Минкомсвязи) по этой теме молчат. Но это явно затянувшееся молчание достаточно красноречиво говорит само за себя.

Почему об этом молчат поставщики, в целом, понятно: система PKI построена именно в интересах "поставщиков", а не "пользователей". Упрощенно говоря, она позволяет собирать с пользователей дополнительные деньги. Но сейчас для них видна другая проблема: пользователи не хотят работать с неудобной, неэффективной системой. И не хотят платить деньги за подобные услуги.

Собственно говоря, все это я и увидел сразу в выступлении замминкомсвязи Олега Пака, который рассказывал о перспективах развития ЮЗЭВ и о необходимости коррекции законодательства. Не сказав ни слова о реальном состоянии дел, причем было сразу понятно – почему не сказал.

Так вот Сергей Муругов считает, что нужно не латать созданную PKI-систему, а переделывать ее самым коренным образом.

Вот его комментарии:

Всё много печальней и бесперспективней, чем написано. "Надо в консерватории править" а не латанием заниматься.

Ну, например, самый очевидный тезис: На мой взгляд, рынка для УЦ в РФ вообще нет, поскольку физиков заберёт под себя ФМС с е-паспортами, а оставшиеся юридические лица (которых порядка 3 миллионов) запросто потянет технически всего один УЦ. Это если конечно не заняться интеллектуальным рэкетом в виде искусственного создания условий, что юридическому лицу для каждой отдельной операции нужен отдельный сертификат. Если говорить серьёзно, то сертификаты юридического лица надо преобразовать в е-печати (как в Европе), которые бы выдавались в ФНС при регистрации фирмы - это своего рода фирменный защищённый электронный бланк государственного образца. Соответственно ФНС и отслеживает актуальность - когда фирма умирает.

Вдогонку, цитата из слов Пака: "Итогом нашей работы станет создание условий для дальнейшего расширения электронной коммерции". Сие вряд ли произойдет. Я не так давно разговаривал с людьми из ФНС на тему ЭЦП в бизнес-процессах. Ответ свелся приблизительно к следующему тезису: фининспектор получает 20 000 руб но именно он принимает решение по законности и объему налогов и ему по-фигу любые ЭЦП и иностранные в том числе, он в праве запросить оригинал документов в бумажном виде. А отсюда вывод, на кой мне связываться с использованием рисковых электронных технологий, особенно если бизнес связан с возвратом НДС. На кой весь этот геморрой?

Еще раз повторю: для меня нет ничего нового в такой оценке. Точно такая же ситуация, на мой взгляд, наблюдается в теме электронного документооборота в целом, где идет латание "тришкиного кафтана" – модели традиционного бумажного документооборота, которую пытаются заштопать электронными нитками.

Но это мнения двух людей. А что по этому думает более широкое экспертное сообщество? Создается впечатление, что всех все устраивает в

сегодняшнем положении KPI-дел. Или более верной является – "Все хорошо, прекрасная маркиза, за исключением пустяков…"?

США: 2015 ГОД МОЖЕТ СТАТЬ ГОДОМ ХАКЕРСКИХ АТАК НА МЕДИЦИНСКИЕ УЧРЕЖДЕНИЯ

Источник: http://rusrim.blogspot.com/2015/01/2015_13.html

Статья Майка Оркута была опубликована 23 декабря 2014 года на сайте издаваемого Массачусетским технологическим институтом журнала «MIT Technology Review» (Обзор технологий).

Учреждения здравоохранения часто хранят медицинские документы и другую информацию без надлежащей защиты. Почему это важно? Медицинская информация особенно полезна для преступников, которые планируют «кражу личности» или финансовые мошенничества.

Наряду с большими объёмами сведений о кредитных картах и пикантными фотографиями знаменитостей, хакеры в 2014 году украли рекордное количество медицинских документов из американских учреждений здравоохранения. По мнению специалистов в области безопасности, в 2015 году атаки на медицинские данные станут еще более распространенными.

Карл Леонард, главный аналитик фирмы Websense по вопросам безопасности, говорит, что хакеры всё чаще взламывают компьютерные сети медицинских учреждений и скачивают из них ценные персональные данные, которые часто как следует не защищены. В августе исследователи Websense сообщили о том, что в течение предыдущих 10 месяцев они наблюдали увеличение числа нападений на больницы на 600 процентов (см. статью «Хакеры нацеливаются на больницы» (Hackers Are Homing In on Hospitals), http://www.technologyreview.com/news/530411/hackers-are-homing-in-on-hospitals/). Группа Леонарда прогнозирует, что в 2015 году медицинская отрасль увидит «значительное увеличение» числа и объёмов краж данных.

Причину этого всплеска диагностировать несложно. Во всём мире медицинские учреждения переходят на использование электронных медицинских документов, при этом обеспечение компьютерной безопасности далеко не всегда имеет достаточно высокий в ходе этого процесса, отмечает Леонард. Кроме того, по его словам, удобный и быстрый доступ к медицинской информации зачастую гораздо важнее для медиков, чем безопасность.

Различные исследования показывают, что кибер-воры считают медицинские данные легкодоступной целью. Институт Понемон (Ponemon Institute), являющийся идейным центром США по проблемам обеспечения неприкосновенности частной жизни, установил, что 40% опрошенных в 2014 году учреждений здравоохранения подвергались атакам с использованием вредоносных программ, разработанных с целью кражи данных – по сравнению 20% в 2010 году. Организация Privacy Rights Clearinghouse («Информационная служба по правам обеспечения неприкосновенности частной жизни»), которая отслеживает серьёзные инциденты компьютерной безопасности, сообщает, что в 2014 году было украдено на четыре миллиона документов больше, чем в любой из предыдущих годов.

Сейчас на чёрном рынке сведения о кредитных картах ценятся ниже, чем несколько лет тому назад, говорит Дон Джексон, директор по информированию об угрозах в фирме PhishLabs, оказывающей услуги в сфере безопасности. По его словам, этот рынок переполнен, и сведения о кредитных картах становится менее полезными без поддерживающей идентификационной информации.

Медицинские документы, однако, часто содержат как идентификационную информацию (например, номера социального страхования), так и финансовую информацию. Этого может быть достаточно для построения практически полной картины личности. И такая информация может принести сотни долларов от клиентов черного рынка, желающих выдать себя за кого-то иного с целью доступа к банковским счетам или к рецептам на наркотические препараты.

У хакеров, говорит Джексон, сейчас имеется «практически менталитет больших данных», в том плане, что они регулярно имеют дело с огромными объемами информации и могут устанавливать взаимосвязи между разнородными наборами украденных данных с тем, чтобы «собрать» воедино полные сведения о личности.

Сейчас с возрастающей скоростью к сетям медицинских учреждений подключаются новые устройства, в том числе смартфоны, планшеты и различных медицинские устройства и датчики. Это может, по мнению Леонарда, привести к появлению новых уязвимостей.

СБОЙ ОБЛАКА AZURE ПРИВЕЛ К ОТКАЗУ МНОГИХ ВЕБ-СЕРВИСОВ

Источник: http://www.pcweek.ru/its/article/detail.php?ID=168909
Автор: Елена Гореткина

В облачной системе Azure компании Microsoft произошел серьезный сбой, который вызвал отказы в работе веб-сервисов в США, Европе, Японии, Бразилии, Азиатско-Тихоокеанском регионе и даже привел к остановке собственных информационных ресурсов Microsoft, таких как MSN.com, Office 365 и Xbox Live.

На устранение проблем потребовалось почти 11 часов. Как сообщает Microsoft, причиной стало обновление, направленное на повышение производительности работы сервиса хранения данных Azure Storage. Несмотря на длительное предварительное тестирование, при развертывании этого обновления проявилась ошибка, которая вызвала отказ Azure Storage и других связанных с ним сервисов. В частности, это привело к тому, что эти сервисы стали неправильно отображать состояние Azure Storage. Многие пользователи отмечали, что на странице состояния Azure было указано, что все работает нормально, хотя на самом деле это было не так.

Хотя причина сбоя была быстро обнаружена, на устранение его последствий потребовалось немало времени из-за нарушения регламента работы. Вместо того, чтобы развертывать обновление постепенно, как требовал регламент, это было сделано почти сразу по многим регионам.

Microsoft обещала извлечь урок из этого события за счет ужесточения правил развертывания изменений, улучшения методов восстановления после сбоя, устранения причины данной ошибки и усовершенствования инфраструктурных инструментов и протоколов.

Однако такой серьезный сбой, уже второй за последние три месяца, может стать серьезным препятствием для облачного бизнеса компании Microsoft, которая конкурирует в этой области с Amazon, IBM, Google и другими игроками.

В число пользователей Azure входят такие крупнейшие компании, как Easyjet, Toyota, Tesco, eBay, Boeing и Apple. Однако в основном облачными услугами пользуются небольшие предприятия, которые стараются сэкономить затраты за счет аутсорсинга ИТ-услуг. Они пострадали из-за сбоя в наибольшей степени. У одних отключился веб-сайт, другие почти целый день не могли воспользоваться офисными приложениями и электронной почтой.

В результате среди пользователей распространяется мнение, что облачные технологии еще недостаточно зрелые для того, чтобы переводить на них всю ИТ-инфраструктуру организации.

Некоторые аналитики с эти согласны, указывая на то, что и в других облачных системах, включая облако Amazon, происходят отказы, которые

приводят к перебоям в работе публичных облачных сервисов и ИТ-операций предприятий. Это связано с тем, что облачные технологии находятся еще на раннем этапе развития, когда вероятность сбоев еще велика.

Чтобы сократить время простоя, специалисты советуют пользователям развертывать свое ПО в облачных структурах, находящихся в разных регионах или даже в облаках разных компаний. Однако это не всегда возможно. Например, в Европе действуют строгие правила, по которым многие компании должны хранить данные в ЦОДах, находящихся на территории ЕС.

С ГОСОБЛАКАМИ В США – ПОНЯТНО. С НАШИМИ ГОСОБЛАКАМИ – ТОЖЕ ПОНЯТНО, НО ИНАЧЕ

Источник: http://www.pcweek.ru/its/blog/its/7082.php Автор: Андрей Колесов

В одном американском Интернет-издании увидел статью: Federal IT Leaders Look for Trust, Transparency in Cloud Vendors (федеральные ИТ-директора хотят от облачных провайдеров надежности (в данном контексте – "доверия, честности и прозрачности").

Сразу замечу, что этого хотят не только федеральные менеджеры и не только по отношению к облакам. Надежности и прозрачности хотят абсолютно все в любых партнерских отношениях.

Система управления страной (то, что у нас обычно называется "государством") – это некоторая большая корпорация. Понятно, что в любой корпорации должны быть правила, стандарты.

Причем важность нормативной базы работы госсектора (перейдем на наш язык) заключается еще и в том, что на нее во многом ориентируется и рынок в целом, в первую очередь корпоративный сегмент. Зачем придумывать самим то, что уже придумали знающие люди.

Из приведенной выше статься видно, что в США для федеральных органов власти есть специальная программа Federal Risk and Authorization Management Program (FedRAMP), которая, в том числе описывает требования к облачным поставщика. И есть некая система сертификации вендоров на соответствие этих требований. Обязательность наличия такого сертификата (обязателен или только желателен) – это вопрос уже второй. Главное – есть описанные и зафиксированные процедуры.

То есть в плане выбора федералом облачного поставщика (опять же сейчас не очень важно – вендора или провайдера), все понятно: есть сертификат – годится, нет – "отвали от военного эшелона".

Насколько мне известно, никаких планов по созданию "гособлаков", как некой специальной выделенной ИТ-инфраструктуры, управляемой "госоператором" (к тому же "единственным") в США и Европе нет. Есть единые требования к операторам, а дальше – рынок, конкуренция.

При это понятно, что есть специальные ведомственные ИТ-инфраструктуры для специальных ведомств (оборона, национальная безопасть и пр.). Но хорошо известно, что даже "специальные ведомства" широко используют обычные рыночные предложения, в том числе облачные.

У нас все как-то не так. Разговоры о гособлаках идут давно, но все в основном на уровне общих идей-пожеланий, слухов, утечек, недомолвок.

То ли будет создаваться какая-то особая государственная ИТ-инфраструктура с особым госоператором (хотя, на самом деле, грандиозный проект с созданием "Национальной облачной платформы" в исполнении Минкомсвязи+Ростелеком уже был), то ли будет вводиться какая-то сертификация.

По моим наблюдениям, последний всплеск разговоров наблюдался летом, в том числе на одной из конференций, на которых мне пришлось побывать и послушать выступление представителя МКС (набор общих слов ни о чем). У меня была написана серия постов, вот последний из них от 02.09.14 - Публичное обсуждение неопубликованного облачного закона Минкомсвязи.

В целом ситуация выглядела так. Минкомсвязь в мае объявило о подготовке законопроекта по регулированию облачных услуг в госсекторе (даже был опубликован проект), а в конце июня – о создании облачного экспертного совета, который займется, в том числе, некой доработкой законопроекта. В конце августа я пытался найти концы этого законопроекта и следы деятельности экспертного совета. Поиски в Интернете и опросы спецов, которые "в теме" не помогли найти ни то, ни другое.

Я на днях предпринял еще одной попытку найти концы и следы.

Вот ответ знающего человека:

Работа совета идет никак, ни одного собрания не было, как нет и дальнейшего развития облачного закона МКС. Полагаю, что закон завис на стадии разработки, поэтому и обсуждения совета не проводилось. Вот такое российское гособлако.

ПРОЕКТЫ СТАНДАРТОВ И ТЕХНИЧЕСКИХ ОТЧЁТОВ, ИСПОЛЬЗУЕМЫХ В СФЕРЕ УПРАВЛЕНИЯ ДОКУМЕНТАМИ, РАЗРАБАТЫВАЕМЫХ ИСО

Источник: http://www.top-personal.ru/officeworkissue.html?333

Международная организация по стандартизации ИСО является ведущей в сфере разработки стандартов и технических отчётов по управлению документами. Эту деятельность в рамках ИСО осуществляет ПК 11 «Управление документами / архивами» / ТК 46 «Информация и документация». Разработка первых стандартов ИСО серии 30300, начатая в 2009 году, принципиальным образом изменила мировоззрение ИСО на управление документами. Существовавший до этого единый и единственный базовый международный стандарт этой сферы ИСО 15489-1-2001 вдруг стал составной частью целого комплекса стандартов по управлению документами, развивающих его положения. Объём и трудоёмкость этой работы оказались столь велики, что планы ИСО / ТК 46 / ПК 11 были серьёзно скорректированы, а сроки разработки проектов стандартов увеличены. Таким образом, 2011 год стал «годом доработок» основных проектов 2010 года и «годом идей» развивающих концепцию системы управления документами, заложенную ИСО в проектах стандартов серии 30300. Говоря о проектах стандартов ИСО по управлению документами, разрабатываемых в ИСО / ТК46 / ПК 11 следует отметить их преемственность и взаимосвязанность, несмотря на то, что их разработка ведётся разными рабочими группами. Рассмотрим каждый из проектов в отдельности.

Проекты международных стандартов ИСО, распространяющиеся на системы управления документацией в целом. Говоря о проектах международных стандартов ИСО, непосредственно связанных с регламентацией процессов и систем управления документами, в первую очередь следует иметь в виду стандарты ИСО серии 30300. Стандарты этой серии разрабатываются ИСО с целью оказания помощи организациям всех форм собственности и всех организационно-правовых форм по созданию, использованию и модернизации (повышению эффективности деятельности) систем управления документами. Стандарты ИСО серии 30300 разрабатываются в рамках стандартов на системы управления документами с целью совместимости и применения общих элементов и методологии с другими международными стандартами ИСО, распространяющимися на иные системы управления документами, включая СМК, а также с международными стандартами и техническими отчётами ИСО, разработанными ранее и / или находящимся в разработке.

Настоящие стандарты применяются как основа и как руководство по:

– установлению системного управления политикой, процедурами и ответственностью в отношении документов, вне зависимости от целей их создания, содержания или носителя информации, на котором они созданы;

– определению ответственности, полномочий и отчётности организаций в отношении этих документов, а также в отношении документированной информации, политики, процедур, процессов и систем;

– проектированию и внедрению систем управления документами;

– достижению качественных результатов от применения систем управления благодаря аудиту и оценке её деятельности, а также постоянному совершенствованию.

Настоящие стандарты предназначены для высшего руководства организации, принимающего решения в отношении выбора и внедрения систем управления документов в организации; людей, ответственных за внедрение этих систем, включая специалистов по управлению документами, риском, аудита, информационным технологиям и защите информации.

В рамках международных стандартов ИСО серии 30300 планируется разработать следующие стандарты:

– ИСО 30300 «Информация и документация. Системы управления документами. Основные положения и словарь», закладывающий основные положения, которым должны соответствовать системы управления документами, и терминологию этой серии стандартов.

– ИСО 30301 «Информация и документация. Системы управления документами. Требования», закладывающий основные требования к системам управления документами.

– ИСО 30302 «Информация и документация. Системы управления документами. Руководство по внедрению», содержащий практическое руководство по внедрению и использованию систем управления документами, созданных на базе ИСО 30301.

– ИСО 30303 «Информация и документация. Системы управления документами. Требования к органам, проводящим аудит и сертификацию», содержащий требования, предъявляемые к органам, проводящим аудит и сертификацию систем управления документами, созданным на базе ИСО 30301.

– ИСО 30304 Информация и документация. Системы управления документами. Руководство по оценке», содержащий руководящие указания по оценке и самооценке систем управления документами, созданными на базе ИСО 30301. Стандарт находится в стадии разработки.

Проекты международных стандартов ISO 30300 «Information and documentation. Management system for records. Fundamentals and vocabulary» («Информация и документация. Системы управления для документов. Основные положения и словарь») и ISO 30301(«Information and documentation. Management system for records. Requirements») («Информация и документация. Системы управления для документов. Требования» в 2011 году проекты вошли на стадии FDIS и были утвержден ИСО без существенных доработок и изменений.

Проект международного стандарта ISO 30302 «Information and documentation — Management systems for records — Guidelines for implementation» («Информация и документация. Системы управления документами. Руководство по внедрению») в 2011 году был разработан на уровне WI, т. е. на уровне авторской разработки общей концепции и обоснования необходимости стандарта. Проект стандарта содержит в себе основные положения по внедрению системы управления документами, соответствующую требованиям ИСО 30301. Стандарт будет содержать в себе определённые организационные положения и инструкции, которые следует использовать для:

– установления (создания), использования, поддержания и улучшения (развития) системы управления документами, используемой в бизнес-процессе организации;

– подтверждения её соответствия установленной политике;

– демонстрации соответствия с ИСО 30301 через обязательства по самооценке, подтверждение самооценки организации через соответствующие структуры самой организации или сертификацию MSR третьей стороной.

Руководства по внедрению систем управления документами будут дифференцированы в зависимости от потребностей организации, переменчивых в контексте её деятельности. Разработка проекта стандарта ISO/WI 30302 «Information and documentation — Management systems for records — Guidelines for implementation» была запланирована на май 2012 г. Проект международного стандарта ISO 30303 «Information and documentation — Requirements for bodies providing audit and certification» («Информация и документация. Система управления документами. Требования к органам, проводящим сертификацию») был инициирован в 2011 году, но так и не получил развития. Следует отметить, что данный проект невольно столкнул интересы ИСО / ТК 46 «Information and documentation» («Информация и документация») и ИСО / ТК 176 «Quality management and quality assurance» («Управление качеством и гарантии качества»). Последним в 2002 году разработан международный стандарт ISO 19011: 2002 «Management system — Guidelines for auditing management systems» («Системы управления. Руководство для аудита систем управления»), который успешно применяется организациями, хотя и требует пересмотра. Проект ИСО 30303 частично подменяет собой положения ИСО 19011, что недопустимо. Поэтому разработка проекта была приостановлена до решения вопроса с ИСО / ТК 176, анализа совместимости всех стандартов ИСО затрагивающих этот вопрос (например, ИСО / МЭК 17021) и устранения конфликта. Разработка проекта стандарта ISO / WI 30303 «Information and documentation — Management systems for records – Guidelines for auditing management systems» была перенесена на 2012 г. Проект стандарта ISO 30304 «Information and documentation – Management systems for records – Guidance for auditing and performance measurement» («Информация и документация. Системы управления документами. Руководство для аудита и измерения работ») был инициирован в конце 2011 года. Согласно представленной ИСО концепции,

стандарт будет содержать руководящие положения, достаточные для оценки системы управления документами. Следует отметить, что в отношении этого проекта определённости никакой нет, о чём говорит даже постоянно меняющееся название, правда, отражающее одну и ту же суть проекта – оценка систем управления документами. Среди них: «Guidance for auditing and performance measurement» («Руководство для аудита и измерения работ»); «Assessment guide». («Гид оценки»); «Self-assessment guide» («Гид по самооценке»). В стандартах ИСО 30300 и 30301 зафиксировано название «Guidance for assessment» («Руководство по оценке»). Работа над проектом международного стандарта ISO/WI 30303 «Information and documentation – Management systems for records – Guidelines for auditing management systems» была запланирована на 2012 год. Проект международного стандарта ISO 15489-1 «Information and documentation – Records management – Part 1: General» и технического отчета ISO / TR 15489-2 «Information and documentation – Records management – Part 2: Guidelines». На этапе подготовки проектов стандартов ИСО серии 30300 (первых двух частей) стало очевидно, что сама концепция этих стандартов, да и текст, заимствованы у ИСО 15489-2001. Именно это и стало причиной столь затяжного обсуждения этих стандартов экспертами ИСО. В 2011 году с принятием этих стандартов встал вопрос о дальнейшей судьбе ISO 15489 1:2001 «Information and documentation – Records management – Part 1: General». Предлагалось несколько вариантов, из которых наиболее жизнеспособными были два: – отменить стандарт, а его положения отразить в стандартах серии 30300; – сохранить и переработать стандарт с учётом положений ИСО 30300 и ИСО 30301 и исключения дублирования. Победила вторая точка зрения, и стандарт ISO 15489-1 «Information and documentation – Records management – Part 1: General», равно как и технический отчёт ISO / TR 15489-2 «Information and documentation – Records management – Part 2: Guidelines», решено было переработать. ИСО / ТК 46 / ПК 11 официально уведомил членов об этом решении. Проекты международных стандартов и технических отчётов ИСО, распространяющиеся на автоматизированные системы управления документами. Говоря о проектах стандартов ИСО, регламентирующих отдельные вопросы автоматизированных систем управления документами, следует отметить их технологическую составляющую. Как правило, эти документы относятся к техническим отчётам и в традиционном понимании не являются стандартами. По крайней мере, в ИСО. В этой связи достаточно проблематично их анализировать. Поэтому они будут освещены в общих чертах. Проект технического отчета ISO/TR 23081-3 «Information and documentation – Managing metadata for records – Part 3: Self-assessment method» («Информация и документация. Руководящие метаданные для документов. Часть 3: Метод самооценки») является продолжением (составной частью) международного стандарта ISO 23081-1:2006, Information and documentation – Records management processes – Metadata for records – Part 1: Principles (ИСО 23081-1-2006. Информация и документация. Процессы управления документами. Метаданные для

документов. Часть 1. Принципы), подробно описанного в предыдущих аналитических обзорах, и развивает его положения на уровне технического отчёта. Данный проект в конце 2011 года был утверждён ИСО как ISO / TR 23081-3 «Information and documentation – Metadata for records – Part 3: – Assessment of Records management metadata set», т. е. технический отчёт. Проект стандарта посвящён вопросам создания и использования метаданных по самооценке (самоконтролю) системы управления документами, в том числе делопроизводственных метаданных. Рабочая группа инициировала разработку 4-ой части этого стандарта ISO 23081-4 «Information and documentation – Records management processes – Managing metadata for records – Part 4: How to implement metadata». Вопрос о сроках его разработки пока открыт, но не ранее 2012 года. Проект технического отчёта ISO / TR 17068 «Information and documentation. Record Management. The trusted third party repository for electronic records» («Информация и документация. Хранилище цифровых документов доверенной третьей стороной») начат ИСО ещё в 2010 году. В 2011 году работа по проекту велась вяло: свелась к разработке концепции документа, описывающей современное положение дел с цифровыми документами, их распространение и широкое использование, как в бизнесе, так и в государственных структурах. В связи с этим проблема доверенного хранения цифровых документов третьими лицами с каждым годом встает всё острее, но здесь возникает ряд вопросов. Например, аутентификация как самих документов, так и хранилищ. Этот технический отчёт является попыткой описать набор ресурсов, услуг и процессов, которые гарантировали бы, что цифровые документы, переданные клиентом на доверительное хранение, останутся аутентичными и надёжными. Документ также рассматривает вопросы сертификации и нотариального обслуживания документов. Технический отчёт описывает принципы социального доверия, необходимого для управления надёжными цифровыми документами, и определяет требования к TTPR сервисам и системам управления, основанным на TTPR сервисной модели. Положения технического отчёта могут быть использованы как эффективный метод для предотвращения широко распространённой путаницы, обусловленной перемещением документов (например, на хранение). Проект разрабатывается рабочей группой № 7 «Digital records preservation» («Сохранность цифровых документов»). Доработка проекта технического отчета ISO / CD / TR 17068 «Information and documentation. Record Management. The trusted third party repository for electronic records» («Информация и документация. Хранилище цифровых документов доверенной третьей стороной») перенесена на 2012 год. Проект международного стандарта ISO (без номера) «Information and documentation. – Risk identification for records» («Информация и документация. Выявление (идентификация) рисков для документов») внесён как предложение рабочей группой № 11 «Risk assessment for records systems» («Оценка рисков для документных систем»). Предложение рассмотрено и принято, тем более что назрел вопрос необходимости переработки ISO / IEC 27005: 2008 «Information technology – Security techniques – Information security

risk management». Проект международного стандарта ISO / WI «Information and documentation. – Risk identification for records» («Информация и документация. Выявление (идентификация) рисков для документов») заложен в план работы ИСО / ТК 46 / ПК 11 без определения срока разработки, но не ранее 2012 года. Проект международного стандарта ISO 13008 «Information and documentation — Digital records conversion and migration process» («Информация и документация. Процессы преобразование и миграции цифровых документов») внесён и разрабатывается одноимённой рабочей группой № 12 «Digital records conversion and migration process». Проект разрабатывается на базе стандарта ANSI / ARMA 16-2007 «The digital records conversion process». Проект посвящён вопросам преобразования цифровых документов, включая вопросы их конвертирования и миграции. Доработка проекта ISO /DIS 13008 «Information and documentation — Digital records conversion and migration process» («Информация и документация. Процессы преобразование и миграции цифровых документов») запланирована на 2012 год. Проект международного стандарта ISO / FDIS 16175-2 «Information and documentation – Principles and functional requirements for records in electronic office environments – Part 2: Guidelines and functional requirements for records in electronic office environments» («Информация и документация. Принципы и функциональные требования к документам в электронной офисной среде. Часть 2. Руководство и функциональные требования к документам в электронной офисной среде») является составной (второй) частью международного стандарта ISO 16175 под общим название «Information and documentation – Principles and functional requirements for records in electronic office environments» («Информация и документация. Принципы и функциональные требования к документам в электронной офисной среде) и перешёл в 2011 год для доработки. Эта часть вышеназванного стандарта вызвала наибольшие споры по целому ряду вопросов, среди которых терминологическая совместимость со ссылочными нормативными стандартами стоит на одном из первых мест. Проект стандарта стремится дать ответ на вопрос: что такое электронные документы и насколько они важны. В этом доработанном проекте предпринята попытка охарактеризовать цифровой (электронный) документ и систему управления ими. Надо сказать, что проект был доработан, но не до конца. Тем не менее, он принят и утверждён ИСО в 2011 году. Таким образом, ИСО / ТК 46 / ПК 11 «Управление документами / архивами» в 2011 году: – разработал (доработал) четыре проекта стандартов и технических отчётов; – приступил к переработке четырёх стандартов и технических отчётов, разработанных ТК ранее; – обосновал необходимость разработки трёх новых стандартов и запланировал их разработку в 2012 году. Даже исходя из статистических данных, приведённых выше, можно понять, насколько активно ведётся работа по стандартизации сферы управления документами в Международной организации по стандартизации (ИСО) и какую роль играет в этом технический подкомитет ИСО / ТК 46 / ПК 11 «Управление документацией / архивами». Обращает на себя внимание не только активность ИСО / ТК 46 /

ПК 11 в разработке стандартов и технических отчётов по вопросам применения информационных технологий в управлении документами, но и взаимосвязанность и взаимозависимость работы всех технических комитетов ИСО. При этом каждый из ТК занимается своим направлением деятельности, а в случае появления смежных тем (тем, связанных с тематикой работ нескольких комитетов), проект готовится либо совместно, либо проходит экспертную оценку во всех заинтересованных ТК. Именно это приводит к продуманности и взаимосвязанности стандартов ИСО всех сфер и создаёт ИСО репутацию крупнейшей международной организации по стандартизации, результаты работы которой признаны во всем мире.

В России, к сожалению, технические отчёты ИСО внедряются как национальные стандарты под давлением заинтересованных фирм-разработчиков программных продуктов для ДОУ, т. е. автоматизированных систем ДОУ. Это приводит к нивелированию уровня стандарта ИСО как важного международного ориентированного документа и сведению его к уровню технического отчёта ИСО, используемого в качестве примера той или иной технологии, и, как правило, серьёзно адаптирующейся к национальным особенностям стран в том случае, если принимается решение этот пример использовать. В России и те, и другие разные по своей сути и уровню международные документы принимаются методом обложки, что принято для стандартов ИСО и недопустимо для технических отчётов ИСО.

Следует отметить, что проблема совместимости терминологии с терминологией международных стандартов ИСО 15894: 2001 и другими стандартами ИСО по управлению документацией характерна для всех частей проекта международного стандарта ИСО 16175.

ПЕРЕЛІК МІЖНАРОДНИХ СТАНДАРТІВ, ПРОАНАЛІЗОВАНИХ НДІ МІКРОГРАФІЇ У ІІ ПІВРІЧЧІ 2014 РОКУ

Автор: Шевченко І. І.

Прагнення України стати рівноправним членом Європейського союзу потребує вдосконалення національної системи технічного регулювання. Участь у Світовій організації торгівлі неможлива без використання міжнародних стандартів. Застосування міжнародних стандартів та гармонізація національних нормативних документів зі світовими аналогами сприяє розвитку ефективних інноваційних технологій.

На виконання цих вимог часу у ІІ півріччі 2014 року Науково-дослідний, проектно-конструкторський та технологічний інститут мікрографії продовжував роботу щодо дослідження матеріалів міжнародних стандартів ISO для адаптації нормативної бази державної системи страхового фонду документації до вимог європейської системи технічного регулювання та розроблення рекомендацій щодо гармонізації науково-технічної продукції сфери страхового фонду документації з міжнародною.

За ІІІ та ІV квартали проведено аналіз 14 міжнародних стандартів, що розробляють або переглядають міжнародні технічні комітети зі стандартизації:

– ISO/TC 42 “Фотографія;

– ISO/TC 46 “Інформація та документація”;

– ISO/TC 171 “Управління документообігом”;

– ISO/TC 223 “Цивільний захист”, з якими НДІ мікрографії веде співробітництво та є їх членом.

Перелік міжнародних стандартів, які досліджено та проаналізовано за поточний період:

1. ISO/SR 20462-1 Фотографія – Психофізичні експериментальні методи для оцінки якості зображення – Частина 1: Огляд психофізичних елементів (Photography – Psychophysical experimental methods for estimating image quality – Part 1: Overview of psychophysical elements).

2. ISO/WD 20087 Фотографія − Цифрова фотокамера − Вимір терміну служби акумулятора (Photography − Digital still camera − Battery life measurement).

3. ISO/SR 18907 Зображувальні матеріали − Фотоплівки та папери – Клин-тест на ламкість (Imaging materials – Photographic films and papers – Wedge test for brittleness).

4. ISO/SR 18914 Зображувальні матеріали – Фотографічна плівка та папір – Метод визначення стійкості фотографічних емульсій у вологому стані до стирання (Imaging materials – Photographic film and papers – Method for determining the resistance of photographic emulsions to wet abrasion).

5. ISO/CD 15489-1 Інформація та документація − Управління записами − Частина 1: Загальні положення (Information and documentation − Records management − Part 1: General).

6. ISO/FDIS 13800 Інформація та документація − Процеси конверсії та міграції електронних документів (Information and documentation − Digital records conversion and migration process).

7. ISO/SR 8459:2009 Інформація та документація − Бібліографічний покажчик елементів даних для використання під час обміну даними та запиту (Information and documentation − Bibliographic data element directory for use in data exchange and enquiry).

8. ISO/CD 22316 Цивільний захист – Організаційна стійкість – Принципи та настанови (Societal security – Organizational resilience – Principles and guidelines).

9. ISO/CD 25222 Цивільний захист – Управління безперервністю діяльності – Настанова для безперервності системи постачання (Societal Security – Business continuity management – Guidance for supply chain continuity).

10. ISO/CD 19444-1 Управління документообігом − Дані форми в форматі XML − Частина 1: XFDF 3.0 (Document management − XML forms data format − Part 1: XFDF 3.0).

11. ISO/WD 19475-2 Управління документообігом − Мінімальні вимоги для зберігання документів − Частина 2: Збереження (Document management − Minimum requirements for the storage of documents − Part 2: Storing).

12. ISO/SR 18935 Зображувальні матеріали – Кольорові зображення на паперових відбитках – Визначення водостійкості друкованих кольорових зображень в приміщенні (Imaging materials – Colour images on paper prints – Determination of indoor water resistance of printed colour images).

13. ISO/SR 24537 Мікрографія – Розміри котушок, використовувані для 16 мм і 35 мм мікрофільмів (Micrographics – Dimensions for reels used for 16 mm and 35 mm microfilm).

14. ISO/SR 19005-1 Управління документообігом − Формат файлів електронних документів для довгострокового збереження. Частина 1: Використання формату PDF 1.4 (PDF/A-1) (Document management – Electronic document file format for long-term preservation – Part 1: Use of PDF 1.4 (PDF/A-1).

За зазначений вище період рекомендовано 12 міжнародних стандартів для використання в наукових роботах (далі − НДР) НДІ мікрографії.

Матеріали трьох міжнародних стандартів рекомендовано використати під час проведення НДР у 2014 році за темами:

– 1.3 «Розроблення методу створення комплексного електронного образу документації, наданої на мікрофільмування, з використанням специфічних схем освітлення» матеріали міжнародного стандарту щодо експериментального методу оцінки якості зображення;

– 2.1 «Дослідження питання створення сховища електронних копій документів страхового фонду документації у Державному реєстрі документів страхового фонду документації України» матеріали міжнародних стандартів щодо переліку заходів з періодичного контролю електронних мікрофільмів та формату файлів PDF 1.4 (PDF/A-1), на підставі якого формувались комплектувальні документи СФД.

На перспективу рекомендовано матеріали восьми міжнародних стандартів під час:

а) патентного пошуку інформації;

б) класифікації стандартів залежно від специфіки об’єктів стандартизації;

в) гармонізації стандартів для визначення сфери взаємодії з іншими стандартами;

г) переглядання або внесення змін до:

– ТТП 321.02200.00056 «Комплект документів на типовий технологічний процес виготовлення мікрофільмів страхового фонду документації з використанням цифрових технологій»;

– МВ 75.2-00010103-007:2009 «Застосування поляризаційних світлофільтрів під час зйомки об'єктів культурної спадщини та історико-культурних пам'яток в місцях їх розташування»;

– ТІ 321.02200.00049 «Цифрова зйомка документації в місцях її зберігання для створення СФД»;

д) робіт з автоматизації операцій технологічного процесу виготовлення та зберігання мікрофільмів СФД, які передбачається виконувати у 2015 − 2017 роках.

є) мікрофільмування, зберігання та контролю документів СФД для визначення:

– очищувачів поверхні мікрофільмів;

– розчинів, які використовуються в якості фунгіцидів для антибактеріального оброблення мікрофільмів;

– стійкості плівок у використанні на наявних проявних машинах та під час проведення вхідного контролю фотоплівки.

Решту стандартів занесено до узагальненої бази даних міжнародних стандартів та проектів міжнародних стандартів ISO за напрямами діяльності системи СФД для використання в перспективі фахівцями НДІ мікрографії.

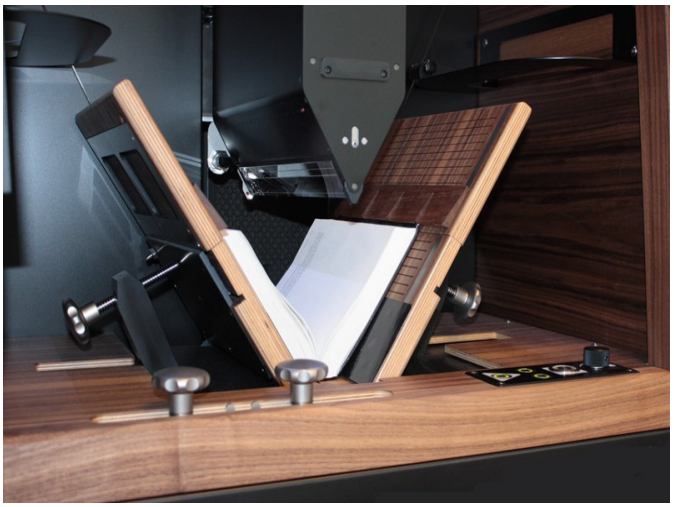
АВТОМАТИЧЕСКИЙ КНИЖНЫЙ СКАНЕР ЭЛАРОБОТ Р-2

Источник: http://www.elarobot.ru

Невероятная производительность

Автоматический книжный сканер ЭЛАРобот Р-2 – устройство, разработанное для оцифровки больших и малых книжных собраний. Главная особенность: сканирование двух страниц одновременно, а также автоматическое перелистывание страниц.

Данное оборудование может автоматически отсканировать до 3000 страниц в час, в зависимости от формата книги.



Изобретение «сканирующего листания»

Отсутствуют сложные манипуляторы и сенсоры, нет настраиваемых осветителей, не надо регулировать под каждую книгу, не нужна какая-либо предобработка, всего 2-3 минуты на то, чтобы положить новую книгу на колыбель и сделать пробный скан. Невероятно простая на вид система надежно и с высокой скоростью сама листает и сканирует страницу за страницей, книгу за книгой.

Самое деликатное обращение

При сканировании книга приоткрывается всего на 60°, исключая риск деформации или повреждения корешка. Нежное скольжение страницы по полированному стеклу призмы (вместо ручного или механического листания)

признано экспертами наиболее деликатным способом: сканеру доверяют поточное сканирование книжных раритетов XVI века.

Искажения не надо исправлять

Обычная для книжного сканирования деформация в области сгиба — исключена, что делает ненужным применение программного выравнивания страниц. Полная плоскостность страницы во время сканирования обеспечивает высококачественные, идеально пригодные для архивации, репринта и безошибочного авторазпознавания электронные образы.

Безопасное минимальное освещение

Светодиодное освещение исключает инфракрасное и ультрафиолетовое излучение и, в отличие от традиционных технологий, воздействует на оригинал в течение лишь нескольких миллисекунд.

Экономичность и надёжность

Лаконичная патентованная конструкция, абсолютный минимум движущихся деталей и регулировок, исполнительных сервоприводов, управляющих сенсоров, механических элементов и компьютеров в сочетании с полным отсутствием юстируемых и настраиваемых оператором узлов (осветителей, фотоаппаратов, линз, манипуляторов и пр.) обеспечивают простую, удобную и надёжную систему с минимумом затрат на поддержание в рабочем состоянии. Применение промышленных высококачественных компонентов обеспечивают реальную работоспособность системы 24 часа в сутки.

Программное обеспечение

ЭЛАРобот поставляется в комплекте с программным обеспечением ScanGate и обладает всеми необходимыми функциями для высококачественного сканирования и обработки изображения.

КОМЛЕКТАЦИЯ И ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ СКАНЕРА

Комплектация:

Высокопроизводительная рабочая станция на базе PC

Рабочая станция обработки (опция)

Профессиональный широкоформатный монитор 22“

Интегрированный сканер А3 для сканирования обложек книг
Эргономичный держатель монитора и рабочей станции
Управляющее программное обеспечение
Программное обеспечение обработки и распознования (опция)

Характеристики	
Тип сканера	Автоматический комплекс сканирования
Тип сканирующей системы	Два сканирующих элемента и зеркальная призма
Система освещения	Светодиодная система освещения, работающая в дискретном режиме
Система переворота листа	Вакуумная система переворота страницы
Интерфейс оператора	Панель сканера позволяет осуществлять настройки книжной колыбели и запуска процесса сканирования. Процесс сканирования управляется ПО на станции сканирования.
Скорость сканирования	До 3000 стр/час (в зависимости от формата книги)
Режимы цветности	Цветное, Серое, Черно-белое
Глубина цвета	30 бит
Разрешение	300-600dpi (вне зависимости от формата оригинала)
Максимальный размер книги	Ширина: до 355мм Длина: до 355мм Толщина: до 150мм
Размер страницы	Ширина: от 50 до 290мм Длина: от 80 До 320мм Толщина: от 40 до 300г/m2
Режимы сканирования	Автоматический, полуавтоматический, ручной
Контроль двойного листа	есть
Выходные форматы	tiff, jpg, png, gif, bmp, pdf
Габариты (ШхДхВ) без монитора	780 х 780 х 1900 мм
Вес	260кг

ЗМІСТ