



ПЕРЕДМОВА

Випуск дайджесту присвячено досвіду установ світу щодо використання мікрофільмів для зберігання інформаційних ресурсів, наведено технічні характеристики сучасного обладнання.

У публікації «Использование легальных методов промышленного шпионажа в сетевой разведке» розповідається про легальні методи виявлення в сирих даних раніше невідомих нетривіальних практично корисних і доступних інтерпретації знань, необхідних для ухвалення рішень в різних сферах людської діяльності.

У публікації «Европейское агентство по кибербезопасности ENISA опубликовало анализ стандартов, касающихся поставщиков услуг доверия» розповідається

У публікації «США: Опубликована новая редакция авторитетного стандарта по защите документов NFPA 232» розповідається

У публікації «Италия: Новой проблемой в области электронной сохранности становятся «документы без формата»» розповідається

У публікації «Инструменты анализа форматов для архивистов» розповідається

У публікації «Великобритания: Архивы для будущего - новое видение» розповідається

У публікації «Перелік міжнародних стандартів, які опрацьовано та проаналізовано НДІ мікрографії за I півріччя 2016 року» розповідається

У публікації «Широкоформатные сканеры» наведено стислий опис найбільш популярних моделей широкоформатних сканерів, які запропоновано компанією АКТЕК XXI.

У публікації «Сканеры микроформ» наведено стислий опис найбільш популярних моделей сканерів мікроформ, які запропоновано компанією АКТЕК XXI.



ИСПОЛЬЗОВАНИЕ ЛЕГАЛЬНЫХ МЕТОДОВ ПРОМЫШЛЕННОГО ШПИОНАЖА В СЕТЕВОЙ РАЗВЕДКЕ

Источник: ust.team@gmail.com

"Data mining - это процесс обнаружения в сырых данных ранее неизвестных нетривиальных практически полезных и доступных интерпретации знаний, необходимых для принятия решений в различных сферах человеческой деятельности."

G. Piatetsky-Shapiro, GTE Labs

Едва начав читать данную статью, а именно прочитав только ее название, вы столкнулись уже как минимум с тремя терминами, определение которых необходимо для соответствующего понимания и применения способов и методов, изложенных ниже в вашей повседневной практике при возникновении подобных задач.

Определения терминов: "легальный метод", "промышленный шпионаж", "сетевая разведка".

Незнаю как вы, но многие материалы, в том числе и издание периодических СМИ, я привык читать с конца, с последней полосы. В данном случае и определения терминов я дам в противоположном порядке.

Что же я подразумеваю под термином "сетевая разведка"? Сетевая разведка - есть комплекс мероприятий по получению и обработке данных об информационной системе (далее ИС) клиента, ресурсов ИС, средств защиты, используемых устройств и программного обеспечения и их уязвимостях, а также о границе проникновения. Это определение впервые дано мной в статье "Сетевая разведка сервиса электронной почты", опубликованной как на нашем сайте, так и принявшая участие в конкурсе статей, посвященных информационной безопасности, организованным порталом SecurityLab.

Спросите у человека на улице, что он подразумевает под словами "промышленный шпионаж", что он знает или думает об этом. Наверняка, насмотревшись продукции Голливудской "фабрики грез" вам дадут ответ о многочисленных агентах, внедренных в персонал конкурентной компании, о службы экономической безопасности, которые охотятся за коммерческими секретами соперников, подкупая, запугивая и угрожая сотрудникам интересующей их компании, о покрытых завесой тайны хакерах, вторгающихся в информационные системы и ворующих секреты и планы Компаний. Да, несомненно все это имеет место быть в некоторых, исключительных случаях, но это не правило. Стоп, стоп, рассуждение и мой рассказ продолжатся чуть позже. Мероприятия, информация, планы конкурентных компаний, позволяющие компании-заказчику увеличить

прибыль, повысить уровень обслуживания клиентов (предвидеть запросы, лучше удовлетворять спрос), добиться конкурентного преимущества на рынке полученные различными способами - вот оно, определение термина "промышленный шпионаж" Это и есть причина, по которой миллионные вложения в этот вид деятельности приносят миллиардные прибыли. Но фильмы все-таки врут...

А правда в том, что в подавляющем большинстве современных, чаще всего транснациональных, компаниях, которым есть что оберегать, но у которых есть и конкуренты, которым соответственно есть, что скрывать, и которые, кроме всего прочего, вкладывают в защиту/разведку огромные суммы, огромную часть работы, которая по своим результатам, а главное эффективности, подпадает под определение "промышленный шпионаж", выполняют обычные клерки, секретарши, даже не понимая до конца истинный результат их совместной работы. И занимаются они ни чем иным, как внесением всей поступающей к ним информации в огромные, автоматизированные базы данных. Но все дело в том что информация, которая казалось бы не имеет никакого отношения к бизнесу, впоследствии оказывается на вес золота. Это информация о вечеринках, на которых присутствовали сотрудники компаний, информация о праздниках, днях рождениях, да похоронах в конце-концов, и лиц, на них присутствующих, это содержания вакансий компаний, содержание резюме лиц, работавших ранее в компаниях-конкурентах. А в результате мы имеем информацию о слиянии компаний конкурентов, о направлениях и разработках компании, даже выявлении сотрудников, "сливающих" информацию компании-конкуренту и любая другая информация, способная помочь в ведении бизнеса, получению и выигранию тендеров, устранении конкурента на рынке. Весь этот процесс называется Data-mining.

И вот суть этого процесса:

Планирование и целеуказание - составление "заданий разведке", подготовка плана сбора информации, отдача приказа исполнителям задания и контроль за ходом его выполнения; Сбор - добывание информации и передача ее в руки специалистов для обработки. Обнаружение знаний (knowledge discovery) — нахождение скрытых структур (patterns), которые преобразуют данные в информацию. Это поиск регулярностей среди групп записей.

Обработка - первичная обработка собранной информации, придание ей определенной формы (может включать, например, лингвистический перевод или переформатирование компьютерных данных).

Оценка - превращение собранной "сырой" информации в данные разведки (путем обобщения, анализа и синтеза, всесторонней оценки и интерпретации всех имеющихся данных) в соответствии с требованиями заказчика (потребителя).

Распространение - пересылка данных разведки потребителям.

Использование знаний (knowledge deployment) — применение найденных знаний для достижения преимуществ в бизнесе.

Более благозвучные названия этого метода - "конкурентная разведка", "бизнес-разведка".

Первые попытки по созданию подобной методики предпринимались сотрудниками различных подразделений ПГУ еще с начала шестидесятых годов. Поначалу эти мероприятия никем не координировались, хотя и давали некоторые результаты. В качестве рабочих материалов для пополнения информационного массива использовались биографические справочники Государственного департамента США. Суть метода заключалась в том, что в биографиях американских дипломатов был установлен ряд признаков, которые были присущи практически всем выявленным сотрудникам ЦРУ.

Аналогичными разработками занимались и по ту сторону «железного занавеса».

Так например, теплым июньским утром 1976 года одновременно по всей Западной Германии было арестовано свыше тридцати нелегалов внешней разведки ГДР. Причиной массового провала агентуры "Штази" было введение в эксплуатацию федеральной криминальной полицией ФРГ усовершенствованной системы выявления агентов противника по растровым признакам. "Растерфандунг" - метод выявления агентов иностранной разведки или террористов был основан на сопоставлении определенных "типовых профилей". То есть аналитики западногерманской контрразведки, проанализировав личные дела персоналий, изобличенных в шпионаже и терроризме, выявили ряд признаков, которые были присущи большинству из них. Так, например, одним из растровых признаков объединявшим всех арестованных было то, что они въехали на "новую родину" из Восточной Германии или третьей страны выдавая себя за беженцев. Каждому из выявленных факторов была присвоена стоимость в баллах и составлены профили всех лиц подозревавшихся в шпионаже. Те же, у кого сумма баллов превысила предельно допустимое значение, были взяты в более плотную разработку.

До появления компьютеров это кропотливое занятие требовало усилий сотен контрразведчиков, и больше всего напоминало составление мозаики из тысяч различных кусочков.

В апреле 1999 г. председатель совета директоров Procter & Gamble Джон Пеппер, выступая перед американским Обществом профессиональных корпоративных разведчиков (SCIP), во всеуслышание заявил, что едва ли может вспомнить, когда еще в корпоративной истории "компетентность, навыки, знания и умения сотрудников конкурентной разведки" были настолько востребованы бизнесом.

Два года спустя разгорелся конфликт между P&G и Unilever - ее главным конкурентом на рынке средств личной гигиены. Unilever пришла к заключению, что корпоративная разведка P&G вышла за рамки допустимого. Частные сыщики, нанятые P&G, прочесывали мусорные корзины неподалеку от офиса Unilever, выискивая неосторожно выброшенные документы, содержащие информацию о последних стратегических планах компании на рынке шампуней. Кроме того, по

утверждению представителей Unilever, агенты втирались в доверие к сотрудникам компании, представляясь аналитиками-маркетологами, и таким путем выводили нужную информацию. P&G отрицала этот факт, однако признавала, что действия, не вполне согласующиеся с ее собственными этическими принципами, в самом деле имели место. "Досадный инцидент" (по выражению Пеппера) завершился в сентябре 2001 г. мировым соглашением, детали которого компании не разглашали. Однако, по оценкам экспертов, его сумма могла достигать десятков миллионов долларов.

Эта история привлекла внимание деловой общественности к явлению, которое именуют "разгребанием мусора" или "мусорной археологией". Многие компании охотно пользуются таким способом сбора информации о конкурентах, хоть порой и не слишком афишируют это. Однако "разгребание мусора" далеко не всегда считается противозаконным действием. В разных штатах США, например, законы, касающиеся корпоративной разведки, различаются. В некоторых штатах мусорные корзины причисляются к "брошенному имуществу", и свободный доступ к их содержимому не возбраняется.

Строго говоря, не следует путать корпоративную разведку с корпоративным шпионажем. Корпоративная разведка (которой, в частности, занимаются и участники SCIP) - это вполне легальный сбор и анализ внешней информации, способной повлиять на планы и решения компании. По сути, услуги такого рода вписываются в понятие "нормального" консалтинга.

Вся информация берется из открытых информационных источников: изданий периодической прессы, отраслевой прессы, отраслевых баз данных и многих других. Но зачастую все источники можно найти в одном месте - в глобальной сети Интернет! А значит они общедоступны, получение информации из них не нарушает государственных и федеральных законов (я не беру в расчет различные "закрытые" государства с государственным ограничением доступной для пользователей сети Интернет информации).

Теперь вернемся к теме статьи и определению сетевой разведки. Комплекс мероприятий по получению и обработке данных об информационной системе (далее ИС) клиента, ресурсов ИС, средств защиты, используемых устройств и программного обеспечения и их уязвимостях, а также о границе проникновения, что мы уже назвали, не должен нарушать законодательства, не должен привлекать внимание служб экономической и информационной безопасности. Ведь активная разведка топологии интересующей сети заказчика, сканирование портов серверов, установленных в ней, законодательство не нарушает, но внимание привлечет обязательно, ведь компании есть что охранять...

А для этого мы и будем использовать, применять технологию, получившее название Data Mining, основу промышленного шпионажа.

Что не привлечет внимания служб безопасности, при наличии у компании собственного представительства в сети Интернет, собственного

интернет-сайта? Правильно, получение только той информации, которая доступна всем пользователем сети, без всякого взлома, составления некорректных запросов, и всего прочего арсенала, который есть в нашем распоряжении, но на который в рамках этой статьи наложено табу.

Одним из спутников крупных компаний является постоянная ротация кадров, текучка кадров, одни увольняются, другие нанимаются или ищутся для найма, особенно если компания развивающаяся, открывающая филиалы в различных городах своей страны, города и зарубежом (опять же не берем в расчет японские компании, где в одной компании работают деды, отцы, дети и внуки, являющиеся прямо таки семейными кланами). Именно поэтому на сайте компании присутствует раздел "Вакансии" и он мало того еще и не пустует. А большой компании нужно много специалистов, администраторов и программистов, специалистов по безопасности и системных инженеров, и в теле вакансии наверняка указан тип оборудования, программного обеспечения, с которыми кандидаты должны уметь работать. А это именно то, что мы ищем.

<http://www.amtkom.ru/index.html?page=about.vacancy> Служба сервиса и технической поддержки

Инженеры

Основные качества:

Знание на уровне системного инженера:* оборудования АТС NEC, Ericsson, Lucent, программного обеспечения к ним;* телекоммуникационного оборудования CISCO (certificate) и SUN Microsystem.

Что применяется в компании и чем она торгует - сразу понятно.

Продолжаем, нравится мне на сайтах публикация адресов корпоративной электронной почты сотрудников, особенно IT-работников. Поискав эти адреса в поисковых системах Интернета можно без особого труда наткнуться на их сообщения в тематический форумах, в которых они задают вопрос или дают ответы на заданные вопросы по работе какого-то компьютерного, серверного оборудования, специфического программного обеспечения.

<http://portal.sysadmins.ru/board/viewtopic.php?t=67782&sid=f2ae361eea7df4ab96b707a778724d3c> при попытке отправить почту на домино практически с любого адреса, приходит ответ: Failed to deliver to 'admin@lotus.tatneft.ru' SMTP module(domain @195.2.83.145:lotus.tatneft.ru) reports: host lotus.tatneft.ru says: 571 - MAIL REFUSED - IP (195.2.83.145) is in RBL black list spam.dnsbl.sorbs.net в настройках всем разшено посылать и получать почту, DNS Blacklist filters - disabled --- и адрес сервера, и программное обеспечение....

Вот на чем я бы хотел остановиться, так это на информации, получаемой из документов, опубликованных на сайте (тех же самых пресс-релизов), или в документации к оборудованию или программному обеспечению, если компания занимается его поставкой. Особенно меня интересуют документы, подготовленные в формате приложений, входящих в Microsoft Office: это MS Word, MS Excel, MS PowerPoint. По странному стечению обстоятельств,

деятельности программистов компании Microsoft, документы подготовленные в этих приложениях представляют из себя СОМ-объект, который может нести все что угодно. Они могут, они и несут... И те данные, которые они несут, принято называть метаданными (metadata). Изначально они созданы для облегчения поиска, редактирования и управления документами.

Читаем, смотрим... <http://support.microsoft.com/default.aspx?scid=kb;EN-US;223396> How to Minimize Metadata in Microsoft Office Documents. Из статьи мы узнаем что в документах MS Office может быть следующая информация:

- Автор документа
- Название компании на которую зарегистрирован Office
- Имя вашего компьютера (рабочей станции, где происходило редактирование документа)
- Имя сервера и домена (в которых происходило редактирование документа)
- Авторы предыдущих версий документа
- Записи о всех попытках редактирования документа
- Скрытые комментарии
- Прочая информация.

Для получения этой информации не требуется особого труда. В интернете доступны для свободного скачивания десятки подобных продуктов.

А теперь посмеемся:

Документы, свободно выложенные на сервере Центральной Избирательной Коммисии Украины:

```
www.cvk.gov.ua/postanovy/p1299_2004_d1.doc Analyzing
D:\UST\2prepare\metadata\p1299_2004_d1.doc
Document Name: p1299_2004_d1.doc
Path: D:\UST\2prepare\metadata
Built-in Document Properties:
Built-in Properties Containing Metadata: 3
Title: ВИБОРИ ПРЕЗИДЕНТА УКРАЇНИ
Author: Кавун
Company: ЦВК
Document Statistics:
Document Statistics Containing Metadata: 6
Creation Date: 15.12.2004 3:28
Last Save Time: 15.12.2004 3:30
Time Last Printed: 15.12.2004 9:44
Last Saved By: user92
Revision Number: 3
Total Edit Time (Minutes): 2 мин.
Last 10 Authors:
Has Last 10 Data
user92[ \\captain\work$\Відділ обробки інформації\Oper\Vladimir
```

Som\Postanovy2004\p1299_2004_d1.DOC

Что мы имеем:

имя пользователя: user92

сервер в сети: captain

скрытая рабочая директория для документов: work\$

Человек, ответственный за ее подготовку: Vladimir Som

Если бы хакер проник внутрь сети, этой информации ему хватило бы чтобы знать, где искать документы. Так как время пребывания в системе зачастую ограничено, а при большом объеме данных и размере имеющихся хостов провести полный анализ всех данных при поиске определенной информации весьма затруднительно. И наверняка сотрудники ЦИК и не подозревают, какая информация содержится в публикуемых ими документах. И куда только смотрит Служба Безопасности Украины...

А вот и полный путь который проделал другой документик ЦИКа:
www.cvk.gov.ua/postanovy/p0042_2004_d.doc

Last 10 Authors:

Has Last 10 Data

БАБЕНКО ПОЛІНА? \\Major\Mashburo\$\МОИ ДОКУМЕНТИ
2004\Постанови\Додатки\1304.DOC Шикута?

Mashburo20 R:\МОИ ДОКУМЕНТИ
2004\Постанови\Додатки\1304.DOC

Mashburo2T C:\WINNT\Profiles\Mashburo2.CICHND\Application
Data\Microsoft\Word\Автокопия 1304.ASD

Шикута? \\MAJOR\MASHBURO\$\МОИ ДОКУМЕНТИ
2004\Постанови\Додатки\1304.DOC БАБЕНКО ПОЛІНА

C:\TEMP\Автокопия 1304.ASD

OlgaY \\captain\work\$\Відділ обробки інформації\Oper\Vladimir
Som\Postanovy2004\p042_2004_d.DOC

Olga: \\major\intraserver\$\wwwroot\Postanov\2004\p042_2004_d.DOC

Что новенького кроме имен пользователей и имен хостов? Имя домена!
Mashburo2.CICHND - следовательно домен CICHND (следуя именованию пользователей в домене).

Кроме вышеприведенных способов и методов существуют десятки других, я лишь показал самые простые и интересные. Специалисты по тестированию на проникновение владеют ими, как и многочисленные хакеры. Be attention, не давайте сопернику узнать то, что хотите узнать сами. Мне представляется, что разведка в сфере бизнеса не является каким-то особым исключением для сегодняшней России. Сейчас у нас в России, как принято считать, все сложно, плохо и т.д. И в этих условиях эта тема особенно актуальна. Мне представляется правильным, что в любом бизнесе, при любых условиях, прежде чем вкладывать деньги, развивать или изменять направление бизнеса, выбирать партнеров по бизнесу, необходимо активно собирать информацию для принятия решения.

Мне представляется, что специалисту по тестированию на проникновение крайне важна вся информация об исследуемой сети, ибо в

компании, в которой система информационной безопасности актуальна и уровень обеспечения ИБ максимально приближен к 100% любая мелочь может быть решающей в осуществлении проникновения.



ЕВРОПЕЙСКОЕ АГЕНТСТВО ПО КИБЕРБЕЗОПАСНОСТИ ENISA ОПУБЛИКОВАЛО АНАЛИЗ СТАНДАРТОВ, КАСАЮЩИХСЯ ПОСТАВЩИКОВ УСЛУГ ДОВЕРИЯ

Источник: сайт ENISA

https://www.enisa.europa.eu/publications/tsp_standards_2015

Автор: Наташа Храмцовская

Сайт Европейского агентства по кибербезопасности ENISA (European Union Agency for Network and Information Security) 1 июля 2016 года проинформировал о публикации версии 1.1 (2016 года) отчета, в котором анализируются стандарты, относящиеся к поставщикам услуг доверия, а также устанавливается соответствие между положениями существующих стандартов и требованиями европейского законодательства eIDAS об электронной идентификации и услугах в области доверия, в том числе об электронных подписях (Electronic identification and trust services regulation – о нём см. http://rusrim.blogspot.ru/2014/09/blog-post_95.html - Н.Х.).

Документ объёмом 80 страниц доступен по адресу https://www.enisa.europa.eu/publications/tsp_standards_2015/at_download/fullReport

В отчете, с одной стороны, анализируются касающиеся стандартов требования eIDAS, а с другой - анализируются имеющиеся в настоящее время стандарты, и результаты анализа сравниваются. Такое сопоставление ориентировано на требования, содержащиеся в различных статьях eIDAS. По его итогам можно сделать вывод о том, что, как правило, имеющиеся стандарты частично или полностью охватывают многие требования eIDAS.

По мнению авторов отчета, может быть одобрено (с определенными ограничениями) применение существующих стандартов в рамках законодательства eIDAS.

Также выявлен ряд пробелов, где вопросы исполнения определенных требований eIDAS еще предстоит проработать в стандартах Евросоюза (ETSI / CEN / CENELEC) или в международных стандартах.

Мой комментарий: Содержание отчета следующее:

Резюме для руководства

1. Введение
2. Требования eIDAS

3. Перечень стандартов

4. Сопоставление и анализ

5. Выводы – выявленные пробелы

Приложение А: Проанализированные стандарты и другие документы

Приложение В: Сокращения

В число проблемных попали следующие области:

- Требования к квалифицированным поставщикам услуг доверия (Qualified Trust Service Provider, QTSP), оказывающим услуги валидации;
- Требования к квалифицированным поставщикам услуг доверия, оказывающим услуги по обеспечению долговременной сохранности;
- Требования к квалифицированным поставщикам услуг доверия, оказывающим услуги зарегистрированной доставки сообщений;
- Требования к квалифицированным поставщикам услуг доверия, выдающим сертификаты для аутентификации веб-сайтов;
- Доверенные системы и продукты;
- Квалифицированные устройства для создания подписи (Qualified Signature Creation Device, QSCD);
- Проверка подписей;
- Усиленные подписи и печати.

Отчет, в частности, может послужить неплохим справочником по существующим и готовящимся европейским стандартам и предстандартам, касающихся электронных подписей.



США: ОПУБЛИКОВАНА НОВАЯ РЕДАКЦИЯ АВТОРИТЕТНОГО СТАНДАРТА ПО ЗАЩИТЕ ДОКУМЕНТОВ NFPA 232

Источник: лист рассылки RECMGMT-L / сайт NFPA

<https://lists.ufl.edu/cgi-bin/wa?A2=ind1606C&L=RECMGMT-L&P=R1852&D=0>

<http://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards?mode=code&code=232>

Автор: Наташа Храмцовская

В США не так много уважаемых стандартов в сфере управления документами, и одним из них является стандарт американской Национальной ассоциации по защите от пожаров (National Fire Protection Association, NFPA) NFPA 232-2012 «Стандарт по обеспечению защиты документов» (Standard for the Protection of Records, <http://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards?mode=code&code=232>). Естественно, в стандарте в первую очередь делается акцент на обеспечение защиты

документов от пожаров, когда они могут пострадать как от огня и дыма, так и от воды и других средств тушения.

До сих пор действовала редакция 2012 года. 18 июня 2016 года известный американский специалист Хью Смит (Hugh Smith) на международном форуме (листе рассылки) специалистов по управлению документами RECMGMT-L порадовал коллег (см. <https://lists.ufl.edu/cgi-bin/wa?A2=ind1606C&L=RECMGMT-L&P=R1852&D=0>) информацией о том, что на сайте NFPA в настоящий момент свободно доступна новая редакция стандарта 2017 года (при условии бесплатной регистрации на сайте), см. ссылку на странице <http://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards?mode=code&code=232>. 2 июня 2016 года стандарт был одобрен в качестве американского национального стандарта.

Хью Смит отметил, что в стандарте NFPA 232-2017 дано новое определение понятия «электронный документ»:

3.2.14.1.1 Electronic Record. A record on information technology equipment or communications equipment (as defined by NFPA 75) or on off-line storage media such as computer tape, magnetic disk drives, optical disks and flash drives.

3.2.14.1.1 Электронный документ. Документ на ИКТ-оборудовании (согласно определению в стандарте NFPA 75) или на автономном носителе информации, таком как компьютерная лента, магнитный диск, оптический диск или флеш-накопитель.

3.3.14.1.2 Hardcopy Record. A record whose information or value is usable without the aid of support equipment or tools. Examples include paper records and art.

3.3.14.1.2 Неэлектронный документ. Документ, содержащаяся в котором информация или иная ценность может использоваться без помощи вспомогательного оборудования и инструментов. Примерами могут служить бумажные документы и произведения искусства.

Как отмечается в самом документе, данный стандарт содержит минимальные требования в отношении защиты документов от угроз, связанных с пожарами, к оборудованию для защиты документов, а также к зданиям и помещениям.

Он устанавливает требования для следующих категорий сред хранения документов, в порядке возрастающей толерантности к риску и уменьшения требований к защите:

- Высокозащищённые хранилища (vaults)
- Архивы;
- Комнаты для хранения документов (file room);
- Секционированные центры хранения документации;
- Не разделенные на секции центры хранения документации.

Данный стандарт также содержит требования к применению упомянутых в нём типов оборудования для защиты документов.

Содержание стандарта NFPA 232-2017 следующее:

Глава 1. Общие вопросы

- Глава 2. Литература
- Глава 3. Определения
- Глава 4. Общие требования
- Глава 5. Строительное оборудование и здания
- Глава 6. Стандартные защищённые хранилища документов
- Глава 7. Архивы
- Глава 8. Комнаты для хранения дел и документов
- Глава 9. Документы
- Глава 10. Оборудование для защиты документов
- Приложение А: Пояснения
- Приложение В: Характеристики пожаров
- Приложение С: Спасение поврежденных водой библиотечных материалов
- Приложение D: Борьба с пожарами
- Приложение Е: Системы предупреждения и тушения пожаров
- Приложение F: Информационные ссылки



ИТАЛИЯ: НОВОЙ ПРОБЛЕМОЙ В ОБЛАСТИ ЭЛЕКТРОННОЙ СОХРАННОСТИ СТАНОВЯТСЯ «ДОКУМЕНТЫ БЕЗ ФОРМАТА»

Источник: сайт электронного издания «Форум электронного правительства»
<http://www.forumpa.it/pa-digitale/conservazione-digitale-la-nuova-sfida-e-il-documento-senza-formati>

Автор: Наташа Храмцовская

Документ уходит от классической формы «привязанного» к носителю непосредственно воспринимаемого объекта, в котором информация зафиксирована при помощи знаков (res signata), принимая флуктуирующую форму содержащего его объекта, которая меняется при изменении технологий. Нам следует думать не о столько о переводе документов в электронный вид, сколько об их «де-документализации» (dedocumentalizzazione), когда соответствующий контент становится независимым от носителя информации и от форматов, которые используются для его представления.

Формирование нормативной базы, устанавливающей технические правила электронного правительства, можно считать завершённым. Все её элементы можно улучшать и совершенствовать, но в целом агентство «Электронная Италия» (L'Agenzia per l'Italia Digitale, AgID) проделало замечательную работу. Теперь для колеблющихся органов государственной

власти уже больше нет никаких оправданий: мы должны внедрить изначально-электронные документы. Это необходимо сделать, и мы имеем в своем распоряжении все необходимые юридические и технические инструменты для того, чтобы правильно действовать.

Ссылаясь на их жизненный цикл, нам скорее следует говорить о «рождённых электронными» (born-digital) (а также, возможно, о «рождённых, чтобы быть электронными», born to be digital?) документах, чем о «преимущественно электронных» (digital first). Несмотря на то, что в названии ряда онлайн-курсов обучения всё ещё встречаются слова «замещающее сохранение» (conservazione sostitutiva – *т.е. сохранение электронных копий взамен уничтожаемых бумажных оригиналов*), мы сейчас решительно переходим на использование документов, которые рождаются, живут и умирают в электронно-цифровой среде. Мы поэтому будем говорить об обеспечении долговременной сохранности электронных документов как об обычной деловой практике.

Набор технических правил сформирован

В окончательном варианте технические правила для электронного правительства устанавливаются тремя нормативными документами:

- Распоряжение Президента совета министров Италии (Decreto del Presidente del Consiglio dei Ministri, DPCM) от 3 декабря 2013 года об управлении документами и электронных журналах регистрации (см. http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/dpcm_3-12-2013_protocollo.pdf , вступило в силу в октябре 2015 года - о нем см. также http://rusrim.blogspot.ru/2015/10/blog-post_28.html);
- Распоряжение Президента совета министров Италии от 3 декабря 2013 года об обеспечении сохранности электронных материалов (см. http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/dpcm_3-12-2013_conservazione.pdf , вступило в силу в октябре 2015 года, о нём см. также http://rusrim.blogspot.ru/2014/04/blog-post_8.html);
- Распоряжение Президента совета министров Италии от 13 ноября 2014 года об электронных документах (см. http://www.agid.gov.it/sites/default/files/regole_tecniche/dpcm_13_11_2014.pdf , вступает в силу с августа 2016 года, о нём также см. http://rusrim.blogspot.ru/2015/01/blog-post_76.html).

Формально это три отдельных нормативных документа. С содержательной точки зрения, однако, это единый порядок, регламентирующий весь жизненный цикл документов и описываемый с трех точек зрения.

Регламентация начинается с момента формирования документа в текущей деловой деятельности (DPCM от 13 ноября 2014), переходит к регистрации, управлению документопотоками, управлению активными документами в соответствии с законодательно-нормативными требованиями (tenuta legale nell'archivio corrente) и депозитарному хранению (DPCM от 3 декабря 2013 об электронных журналах регистрации), завершаясь вопросами «электронной сохранности» архивных документов длительного и

постоянного срока хранения в соответствии с моделью OAIS, описанной в стандарте Международной организации по стандартизации ISO 14721 (DPCM от 3 декабря 2013 года об обеспечении сохранности электронных материалов).

Все эти три нормативных документа требуют радикального пересмотра внутренних процессов органов государственной власти, а также разработки – но не рабского копирования - двух основных инструментов:

- Руководство по управлению электронными журналами регистрации (protocollo informatico);
- Руководство по электронной сохранности (conservazione digitale).

Как мы уже сказали, нужна концептуальная проработка этих документов, а не «копипастинг». К тому же, если руководство по электронной сохранности является новым инструментом, то руководство по управлению электронными журналами регистрации появилось с момента принятия Распоряжения Президента совета министров (DPCM) от 31 октября 2000 года (см. <http://www.interlex.it/testi/dpc001031.htm> , которое утратило силу и было заменено новыми техническими правилами, введенными DPCM от 3 декабря 2013 года). Проблема заключается в том, что лень итальянской бюрократии нередко приводит к тому, что часто методологические и стратегические возможности, связанные с пересмотром их деловых процессов, реализуются чисто формально.

На майское 2016 года заседание «Форума электронного правительства» мы пригласили два муниципалитета – Лоано (Loano) и Лендинара (Lendinara); два университета – Инсубрии (Insubria) и Падуи (Padova), научно-исследовательское учреждение (Национальный институт астрофизики, INAF, <http://www.inaf.it/en>) и территориальное управление здравоохранения Болоньи (ASL Bologna), чтобы они представили свои проекты и достижения в области управления документами.

В качестве примеров были продемонстрированы руководства по управлению электронными журналами регистрации муниципалитета Лоано (http://www.procedamus.it/images/pdf/Manuale_Riviere_LOANO2016.pdf) и университета Инсубрии (http://www.procedamus.it/images/pdf/MdG_Insubria_ver01_23_mag_2016.pdf), которые можно скачать на сайте Procedamus (<http://www.procedamus.it/>), пользующемся поддержкой «Форума электронного правительства».

Подтверждением тому, что Руководство не является статичным инструментом и развивается вместе с организационными и правовыми моделями, является то, что все такие руководства государственных органов должны быть обновлены к следующему августу, в соответствии с положениями DPCM от 13 ноября 2014 года. С учетом внесенных последним Распоряжением изменений, потребуется внести не менее дюжины поправок, прямо предусмотрено его 17 статьями. Показательно, что более половины этих изменений связаны именно с Руководством. Нельзя не отметить и то, что придётся заново сформулировать раздел о документах, которые в обязательном порядке создаются в электронном виде – проблема в проблеме.

От дематериализации к дедокументализации

Новые технические правила предписывают также пересмотр самой концепции документа. В соответствии с новым законодательством Евросоюза по вопросам электронной идентификации и услугам в области доверия (eIDAS, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG - в частности, регламентирует использование электронных подписей, печатей и отметок времени), «электронным документом является любой контент, сохраненный в электронной форме, в частности, текст, звук, видео- или аудиовидеозапись».

Для справки: п.35 ст.3 «Определения» базовой английской редакции eIDAS сформулирован следующим образом: «‘electronic **document**’ means any content stored in electronic form, in particular text or sound, visual or audiovisual recording;». В английском языке термин document (в отличие от **record**) означает всего-навсего электронный объект, которым можно индивидуально управлять (говоря по простому, файл) – который может быть, а может и не быть документом.

В итальянской редакции текста (<http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32014R0910&from=EN>) допущена грубая ошибка, которой часто грешат и наши переводчики – английский термин document переведен похожим, но имеющим совершенно иной смысл итальянским термином documento. Отсюда и революционные «новшества»)

Как это уже произошло с революционным и имеющим глобальное значение изменением определения понятия «административный документ» (documento amministrativo), содержащимся в ст. 22 закона 241/1990, такое определение меняет нормативную точку зрения государств-членов Евросоюза. Документом считается «любой» контент.

Для справки: К слову упомянут Закон Италии от 7 августа 1990 года №241 «Новые правила, касающиеся административных процедур и права доступа к административным документам» (La legge 7 agosto 1990, n. 241 "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi"), см. http://archivio.digitpa.gov.it/sites/default/files//normativa/Legge_241_1990.pdf .
Определение менялось следующим образом:

- **Первоначальное:** Административными документами являются любые графические, фотокинематографические, электромагнитные представления или представления в любом другом виде содержания актов, в том числе внутренних, сформированных органами государственного управления или так или иначе использованных в целях административной деятельности.

- **Новое, с 2005 года:** Под «административным документом» понимается любое графическое, фотокинематографическое, электромагнитное или любого иного рода содержание актов (в том числе внутренних или не связанных с конкретными процедурами), которые сохраняются органами государственного управления и касаются

деятельности, представляющей общественный интерес, независимо от публичного или частного характера их регулирования.

Таким образом, разрушились наши привычные представления (и внедрение информатики подрывало их в течение двадцати лет) - понятие традиционно понимаемого документа. Конечно же, понятие документа по-прежнему охватывает акты (*atti – юридически значимые документы*), но оно также охватывает и просто контент.

Документ уходит от классической формы «привязанного» к носителю непосредственно воспринимаемого объекта, в котором информация зафиксирована при помощи знаков (*res signata*), принимая флуктуирующую форму содержащего его объекта, которая меняется при изменении технологий. Речь идёт о революции, во многом инициированной в Италии, но сейчас осуществляемой Европейским Союзом. Нам следует думать, таким образом, не о столько о переводе документов в электронный вид, сколько об их «де-документализации» (*dedocumentalizzazione*), когда соответствующий контент становится независимым от носителя информации и от форматов, которые используются для его представления. Мир изменится, и государственное управление не может не меняться вместе с ним. Чтобы всё это осуществить, мы должны действовать сообща.



ИНСТРУМЕНТЫ АНАЛИЗА ФОРМАТОВ ДЛЯ АРХИВИСТОВ

Источник: блог «Mad File Format Science» <https://lwn.net/Articles/688396/>

Автор: Гэри МакГэф

Обеспечить долговременную сохранность файлов не так легко - недостаточно просто записать их на носитель информации. Как достаточно тонко подметил сайт [xkcd](http://xkcd.com/1683) (см. <http://xkcd.com/1683>), здесь возникает ряд других проблем. Будет ли программное обеспечение будущего в состоянии читать сегодняшние файлы без потери информации? Если да, смогут ли люди определить, что эти файлы содержат и каково их происхождение?

Электронные архивы и библиотеки хранят файлы для будущих поколений точно так же, как их физические аналоги хранят книги, фотографии и произведения искусства. Электронные учреждения несут похожую ответственность за обеспечение сохранности электронных документов. В некотором смысле электронные данные создают больше проблем, поскольку файловые форматы изменяются быстрее, чем естественные языки. С другой стороны, эффективное использование метаданных позволяет файлу «нести свою историю» вместе с собой.

По этим причинам важно иметь возможность в деталях определить особенности структуры файлов. Для этой цели недостаточно просто использовать команду "file" [в Linux], поэтому разработчики создали ряд инструментов с открытым исходным кодом для проверки качества поступающих в архивы документов. Эти инструменты анализируют файлы, сообщая о тех из них, которые явно повреждены или могут вызвать проблемы, а также показывают, насколько подробно или сдержанно файлы описывают сами себя. Можно выделить следующие проблемные вопросы:

- **Точная идентификация формата:** Недостаточно знать MIME-тип. Разница в версиях может иметь значение для совместимости программного обеспечения, к тому же для форматов устанавливаются различные "профили" - ограничения формата при использовании его для определенных целей. Например, PDF/A – это профиль формата PDF, требующий наличие у файла определенных структурных свойств и не допускающий внешних зависимостей. Формат PDF/A лучше подходит для целей архивного хранения (на это, собственно, указывает индекс A), чем большинство других разновидностей формата PDF.

- **Долговечность формата:** Программное обеспечение, способное читать любой конкретный формат, постепенно морально устаревает, если нет достаточной заинтересованности в его обновлении. О том, какие форматы окажутся самыми долговечными, можно лишь гадать, но надежнее делать ставку на открытые и широко распространенные форматы, чем на проприетарные или малоизвестные.

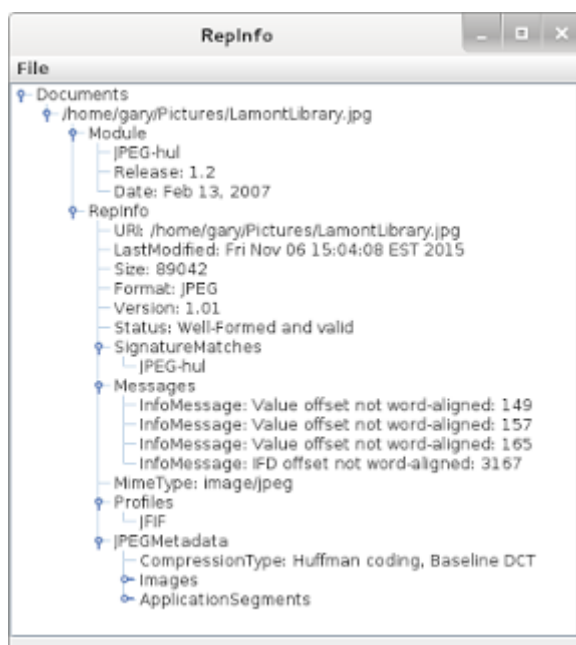
- **Строгая проверка соответствия спецификациям:** Многие программные проекты следуют закону Постеля (Postel's Law): «Будьте либеральны в том, что Вы принимаете, и консервативны в том, что отправляете». Архивное программное обеспечение, однако, в этом отношении стоит по обе стороны баррикад. Оно принимает файлы для последующего их представления аудитории, которая в данный момент еще даже не существует. Это означает, что оно должно быть консервативно в отношении того, что принимает.

- **Извлечение метаданных:** Файл с большим количеством идентифицирующих метаданных, такой, как XMP или Exif, является более подходящим кандидатом для принятия на архивное хранение, чем файл с минимальными метаданными. Архив становится намного полезнее, если предоставляет богатые метаданные, по которым можно ввести поиск.

Эти проблемы решаются рядом приложений с открытым исходным кодом, и о некоторых из них будет рассказано ниже. Большинство этих приложений создано разработчиками программного обеспечения, являющихся членами библиотечного сообщества и сообщества специалистов по обеспечению долговременной сохранности. Некоторые решения работают с небольшим количеством форматов, но зато очень глубоко и детально; другие охватывают много форматов, но анализируют их не столь подробно. Если одни приложения просто идентифицируют файловые форматы, то другие также извлекают содержащиеся в файлах метаданные.

ЖНОВЕ

Изю всех инструментов ЖНОВЕ (JSTOR-Harvard Object Validation Environment – среда валидации объектов для электронного архива JSTOR и библиотеки Гарвардского университета) является самым требовательным и одержимым. Он охватывает небольшое число форматов, и очень придирчив, что полезно для исключения проблем у программного обеспечения в будущем. Он очень подробно исследует структуру файлов, проверяя их на предмет соответствия спецификациям, идентифицируя версии и профили и извлекая множество метаданных. Я работал над этим инструментом в течение десяти лет, подключившись в 2003 году к проекту библиотеки Гарвардского университета, написав основную часть кода и продолжая поддерживать его и после того, как я ушёл из Гарварда. Теперь проект находится в руках фонда «Открытая сохранность» (Open Preservation Foundation, <http://openpreservation.org/>), который только что выпустил версию 1.14.



ЖНОВЕ написан на языке Java и доступен на условиях лицензии GNU LGPL license (версия 2.1 или позже). Инструмент включает в себя модули для пятнадцати форматов для графических изображений, звукозаписей, текстовых материалов, а также форматы семейства PDF. Новым в версии 1.14 (это пока не отражено в документации) является поддержка форматов PNG, GZIP и WARC.

Каждый из модулей детально анализирует файлы соответствующего типа в поисках нарушений спецификаций. Файл, который соответствует синтаксическим требованиям, считается «правильно сформированным» (well-formed). Если он также удовлетворяет семантическим требованиям, то рассматривается как «правильный» (valid). Например, XML-файл правильно сформирован в том случае, когда все его теги соответствуют друг другу,

правильно вложены и т.д., и правилен, когда он соответствует своей схеме, если таковая имеется.

Если формат не идентифицирован, то принимается, что это «поток байтов» (Bytestream) – просто последовательность байтов или, другими словами, файл любого формата. В конфигурации по умолчанию JHOVE пробует применить к файлу все свои модули и выдает результат по итогам работы первого из них, который определит файл как правильно сформированный и правильный. Если файл не соответствует ни одному из модулей, то он классифицируется как «поток байтов». Также возможно запускать JHOVE в режиме проверки соответствия спецификациям конкретного формата. Это полезно при работе с поврежденными файлами, поскольку будут выданы сообщения, показывающие, почему те некорректно сформированы или неправильны – что гораздо полезнее, чем объявлять их «потоками байтов».

Если файл правильный, то JHOVE сообщит версию формата, профили формата (если есть), которым он соответствует, и выдаст многочисленные метаданные файла. Вывод может быть как в виде простого текста, так и в формате XML. При использовании графического интерфейса результаты представляются в виде раскрываемой схемы; и поддерживается их сохранение в простом текстовом формате и в формате XML.

Команда для исследования TIFF-файла `example.tif` с выдачей результатов в формате XML может выглядеть следующим образом:

```
jhove -m TIFF -hul -h xml example.tif
```

Другие JAVA-приложения могут вызывать JHOVE через его API-интерфейс прикладного программирования.

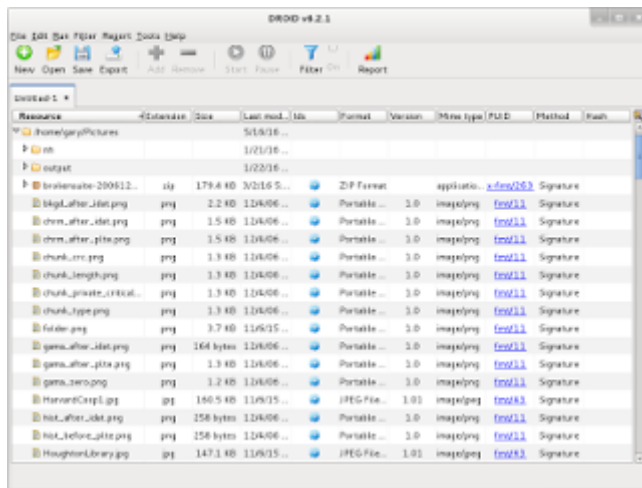
JHOVE строг, но он анализирует только структуру файла и не анализирует потоки данных в файле. Например, в TIFF-файле, сжатом с использованием алгоритма LZW, инструмент проверит правильность и соответствие всех тегов, в том числе тегов `StripOffset` и `StripByteCount`, но не будет проверять, вляются ли сами сжатые данные о пикселях правильно сформированными данными LZW. Таким образом, хотя JHOVE способен отлавливать тонкие ошибки, но не гарантирует выявление всех дефектов.

DROID и PRONOM

Архивистам часто нужно обрабатывать большие пакеты файлов, и им нужна общая картина того, с чем они имеют дело: им нужно знать, сколько имеется файлов в каждом из форматов, сколько подверженных риску файлов, какова статистика использования форматов по годам и месяцам, в какой мере используются старые версии форматов, и т.д. В этом эффективен такой инструмент, как DROID, который распространяют Национальные Архивы Великобритании по лицензии BSD. Главная задача данного инструмента - проверять и идентифицировать файлы при их вводе в архивную систему. DROID использует разработанную Национальными Архивами базу данных о форматах PRONOM, идентифицируя форматы файлов на основе их сигнатуры или «магического числа».

Хотя по функциям он похож на команду «file», DROID проводит более детальное различие между форматами. Например, PRONOM различает в рамках формата TIFF основанный на TIFF универсальный формат для цифровых фотокамер DNG, TIFF-FX для факсимильных изображений и файлы Exif, представляющие собой TIFF-метаданных в отсутствие изображения.

DROID хорош при обработке больших пакетов файлов. Анализ проводится в два этапа. Сначала пользователь «профилирует» набор файлов, собирая информацию о них в единый документ. В командной строке пользователь может указать фильтры, говорящие DROID о том, какие файлы следует профилировать. К сожалению, в языке фильтров сложно разобраться, а документация не столь полезна, как могла бы быть, но, к счастью, существует Google-группа (<https://groups.google.com/forum/#!forum/droid-list>), участники которой могут ответить на возникающие вопросы.



На втором этапе формируется отчет. Одна команда может выполнить сразу оба этапа. Вот относительно простой пример команды с фильтром, отбирающим только PDF-файлы, создающей отчет в виде CSV-файла: **droid.sh -p "result1.droid" -e "result1.csv" -F "file_ext contains 'pdf'"**

Проще запускать DROID через графический интерфейс. В этом случае профилирование и формирование отчета - отдельные этапы.

DROID мало занимается проверкой формата и извлечением метаданных, его сильной стороной является идентификация файловых форматов по их сигнатурам. Это ценно при обработке большого количества поступающих на архивное хранение файлов, с целью отсеять файлы в неподходящих форматах.

ExifTool

Иная направленность у инструмента ExifTool, разработанного Филом Харви (Phil Harvey, см. <http://owl.phy.queensu.ca/~phil/exiftool/>). Его специальность - манипулирование метаданными и, несмотря на свое название, он знает о метаданных очень многих типов, а не только об Exif. Он может просматривать и модифицировать файлы, и способен на такие ловкие

трюки, как назначение автора группе файлов или корректировка метки времени, относящейся к неправильному часовому поясу. Для архивистов он наиболее интересен своей способностью захватывать метаданные из файлов и сообщать о них.

Инструмент в основном «знает» об аудио-, видео- и графических форматах (но не только). Он проводит простую идентификацию формата по его сигнатуре, а также проверку структуры, достаточную для выделения метаданных в файле. ExifTool доступен по лицензии Perl.

Это многоцелевой программный инструмент, с широкими возможностями написания сценариев. Perl-приложения могут использовать его посредством конструкции **Image::ExifTool**. Другой программный код может использовать интерфейс командной строки инструмента в качестве API, используя флаги **-@** и **-stay open** для передачи команд через стандартное устройство ввода или через файл аргументов. Кроме того, прилагаемая библиотека поддерживает использование интерфейса командной строки в программах на языке C++.

ExifTool рассматривает все свойства и метаданные файла в качестве «тегов». Команда может запросить конкретные теги или их группы. Приведенная ниже команда выдаст тип файла, MIME-тип и обычное расширение формата:

```
exiftool -filetype -mimetype -filetypeextension sample.png
```

Выдача команды будет выглядеть следующим образом (если предположить, что это действительно PNG-файл):

```
File Type           : PNG
MIME Type           : image/png
File Type Extension : png
```

Поддерживается ряд вариантов экспорта результатов, в том числе в файлы формата HTML, RDF XML, JSON и в простой текст. Выходные данные могут быть отсортированы, и для некоторых тегов есть варианты форматирования.

Складываем всё вместе: FITS

Что делать, если вы хотите узнать второе мнение о файле? Может быть, даже третье или четвертое?

Существует множество свободно используемых программных средств для идентификации файловых форматов и извлечения метаданных, и ограниченный объём статьи не позволяет упомянуть их все. В их числе такие инструменты, как MediaInfo (<https://mediaarea.net/en/MediaInfo>), который извлекает метаданные из аудио- и видеофайлов, инструмент извлечения метаданных (Metadata Extraction tool, <http://meta-extractor.sourceforge.net/>) Национальной Библиотеки Новой Зеландии (NLNZ), специализирующийся на нескольких подходящих для архивного хранения форматах, и Tika фирмы Apache (<https://tika.apache.org/>), способный извлекать метаданные из более чем тысячи форматов.

Все эти приложения выдают разную информацию, не всегда соглашаясь друг с другом. Некоторые осуществляют более детальную

идентификацию, чем другие, а некоторые придирчивее других при оценке правильности файла. Желательно использовать несколько инструментов, на случай, если один из них не лучшим образом справляется с определенными задачами. Инструментальный набор библиотеки Гарвардского университета для получения информации о файлах (File Information Tool Set, FITS, <http://projects.iq.harvard.edu/fits>) позволяет совместно использовать дюжину различных инструментов.

FITS первоначально служил – и до сих пор служит – в роли «привратника» Службы электронного хранилища Гарвардской библиотеки (Digital Repository Service, DRS). Сейчас им пользуются и другие учреждения. Я лишь недолгое время поработал с FITS, но мои усилия сыграли значительную роль в превращении его из специфического для Гарварда инструмента в инструмент, используемый и поддерживаемый значительно более широким сообществом. Он доступен под лицензией LGPLv3.

DROID, ExifTool и JHOVE входят в число поддерживаемых FITS инструментов, равно как и Tika, **file**, MediaInfo, NLNZ Metadata Extractor, а также неподдерживаемый, но до сих пор иногда полезный инструмент под названием **ffident** (<http://web.archive.org/web/20061106114156/http://schmidt.devlib.org/ffident/index.html>) и несколько инструментов собственной разработки.

При всей его сложности, использовать FITS довольно просто. Ниже приведен простейший вариант полезной команды, которая анализирует файл с использованием всех модулей:

fits -i sample.png

Сочетать различные инструменты сложно по нескольким причинам. Они написаны на разных языках - FITS на Java, и он вызывает созданные не на Java программы, такие, как ExifTool, через интерфейс командной строки. Результаты выдаются в различных форматах, и каждый инструмент использует свою собственную терминологию.

В тех случаях, где поддерживаемые инструменты могут выдавать результаты в формате XML, FITS использует XSLT для преобразования его в «FITS XML», а затем объединяет результаты в один XML-файл. В качестве дополнительной возможности он может конвертировать FITS XML в схемы метаданных, обычно используемые архивами и библиотеками, такие как MIX (<http://www.loc.gov/standards/mix/>), TextMD (<https://www.loc.gov/standards/textMD/>) и AES Audio Object (<http://www.aes.org/publications/standards/search.cfm?docID=84>).

Часто инструменты не вполне согласны в своей оценке файла, и FITS пытается разрешать конфликты. В разделе «Идентификация» выдачи в формате FITS XML перечислены инструменты, которые идентифицировали файловый формат; если они не разошлись во мнениях, то у него будет атрибут **status=CONFLICT**. Те, кто хочет получить однозначный ответ, могут установить приоритеты для инструментов и установить флаг выдачи

сведений о конфликтах в значение **false**. Первый давший ответ инструмент выигрывает.

Поскольку FITS агрегирует в одном приложении так много инструментов, у каждого из которых имеется собственный цикл разработки, это сложное для управления программное обеспечение. Иногда FITS вынужден пользоваться более старыми версиями инструментов до тех пор, пока его разработчики не настроят его для работы с последней версией инструмента.

Завершающие мысли

Идентификация форматов и характеристика файлов - сложное дело. Технические спецификации могут порой быть неоднозначными. Практика, отклоняющаяся от буквы спецификаций, может стать общераспространенной; например, сейчас требование TIFF о выравнивании адресов на четную границу считается архаичным. Люди по-разному смотрят на то, какое число ошибок можно считать приемлемым. Чрезмерная придирчивость может привести к тому, что в архивы не будут допущены вполне пригодные к использованию файлы.

Специалисты увлеченно ищут ответы, и часто из них невозможно четко выделить единственно правильный. Поэтому совсем не удивительно, что конкурируют различные инструменты на основе различной философии, и что наилучшим подходом может быть их совместное использование и объединение выдаваемых ими результатов.



ВЕЛИКОБРИТАНИЯ: АРХИВЫ ДЛЯ БУДУЩЕГО - НОВОЕ ВИДЕНИЕ

Источник: блог Национальных Архивов Великобритании
<http://blog.nationalarchives.gov.uk/blog/archives-future-new-vision/>

Автор: Наташа Храмцовская

11 июля 2016 года Национальные Архивы Великобритании начали этап взаимодействия с общественностью, проведя первый из запланированных четырех круглых столов, с тем, чтобы совместно сформировать новое видение архивов (см. также <http://www.nationalarchives.gov.uk/archives-sector/whats-happening-now/developing-a-future-vision-for-archives/>).

Мероприятие, которое прошло в Историческом центре Уилтшира и Суиндона (Wiltshire and Swindon History Centre), привлекло широкий круг участников, представлявших архивы коммерческих организаций, местных органов власти, университетов, а также независимые архивы и фонды.

***Мой комментарий:** Как отмечается на странице сайта Национальных Архивов, на которую выше дана ссылка, процесс разработки*

нового видения пройдёт в 5 этапов. Публикация итогового документа запланирована на март 2017 года. Новое видение должно сделать архивы более готовыми к проблемам, с которыми предстоит столкнуться в будущем, особенно в таких вопросах, как электронно-цифровая трансформация, инновации и финансовая устойчивость, кадры и их подготовка, а также лидерство и партнерские отношения.

Я почувствовал реальный аппетит людей к переменам и их желание воспользоваться теми возможностями, которое предоставит новое видение для отрасли. Это было очевидно по оживленной дискуссии, продолжавшейся в течение всего времени работы круглого стола.

Меня впечатлил огромный уровень ответственности, чувствующийся в зале. Ощущалось глубокое понимание и готовность приложить усилия для укрепления архивной отрасли в качестве ключевого партнера как в сфере культуры и сохранения культурно-исторического наследия, так и за её пределами.



Участники первого из четырех круглых столов

Было отрандно видеть определенное единство мнений в том, что специалисты считали необходимым для усиления воздействия архивов. Участники вели обсуждение высокоуровневых вопросов с акцентом на формирование видения, а не детального плана действий. Они оценили то, что мы действительно были очень заинтересованы в том, чтобы с самого начала вовлечь их в решение вопроса о будущем архивов.

Предусматривается множество возможностей для того, чтобы в течение лета заинтересованные лица смогли внести свой вклад в разработку видения, включая, в том числе онлайн-опрос, проведение собеседований с представителями архивной отрасли и сессии вопросов и ответов в Твиттере. Дальнейшая информация будет рассылаться через наши регулярные каналы связи, такие, как электронная новостная рассылка, jiscmail и новости партнеров, так что продолжайте взаимодействовать с нами, используя адрес электронной почты: ArchivePolicy@nationalarchives.gsi.gov.uk

Для подключения к онлайн-обсуждению в Твиттере, используйте хештег **#ArchiveVision** (можно воспользоваться также ссылкой <https://twitter.com/search?q=%23ArchiveVision&src=typd>).

Мой комментарий: Хороший пример, который, к сожалению, вряд ли будет повторен у нас (если только Росархив неожиданно не получит хорошую «встряску» и новых энергичных руководителей, ещё не думающих о пенсии).



ПЕРЕЛІК МІЖНАРОДНИХ СТАНДАРТИВ, ЯКІ ОПРАЦЬОВАНО ТА ПРОАНАЛІЗОВАНО НДІ МІКРОГРАФІЇ ЗА І ПІВРІЧЧЯ 2016 РОКУ

Автор: Шевченко І. І.

У зв'язку з виконанням зобов'язань, які взяла на себе Україна через набуття членства у Світовій організації торгівлі, а також положень Угоди про асоціацію між Україною та Європейським Союзом, пріоритету набуває прийняття міжнародних та європейських стандартів як національних для усунення зайвих технічних бар'єрів у торгівлі. Таким чином, актуальним стає проведення аналізу матеріалів міжнародних стандартів та систематизація й узагальнення отриманої інформації для розроблення рекомендацій щодо гармонізації нормативної бази державної системи страхового фонду документації (далі – СФД) у частині відповідності проектам міжнародних стандартів та використання їх у науковій і науково-технічній діяльності.

Науково-дослідний, проектно-конструкторський та технологічний інститут мікрографії (далі – НДІ мікрографії) проводить науково-дослідну роботу з дослідження та аналізу міжнародних стандартів ISO та розроблення рекомендацій щодо гармонізації нормативної бази державної системи СФД з міжнародною.

За І півріччя 2016 року проведено аналіз 19 міжнародних стандартів міжнародних технічних комітетів стандартизації:

- ISO/TC 42 «Фотографія»;
- ISO/TC 46 «Інформація та документація»;
- ISO/TC 171 «Управління документообігом»;
- ISO/TC 292 «Безпека», з якими НДІ мікрографії веде співробітництво та є їх членом.

Перелік міжнародних стандартів, які проаналізовано за поточний період:

1. ISO/NP 19264 Фотографія – Архівні системи – Аналіз якості зображення – Частина 1: Світловідбивальні оригінали (Photography – Archiving systems – Image quality analysis – Part 1: Reflective originals);
2. ISO/SR 424 Фотографія – Хімікати для фотообробки – Технічні умови на безводний карбонат натрію і карбонат натрію моногідрат (Photography – Processing chemicals – Specifications for anhydrous sodium carbonate and sodium carbonate monohydrate);
3. ISO/DIS 2108 Інформація та документація – Міжнародний стандартний номер книги (ISBN) – (Information and documentation – International standard book number (ISBN));
4. ISO/DIS 3901 Інформація та документація – Міжнародний стандартний код запису (Information and documentation – International standard recording code);
5. ISO/SR 3297 Інформація та документація – Міжнародний стандартний серійний номер (ISSN) – (Information and documentation – International standard serial number (ISSN));
6. ISO/DTR 15801 Управління документообігом – Збереження інформації в електронному вигляді – Рекомендації для достовірності та надійності – (Document management – Electronically stored information – Recommendations for trustworthiness and reliability);
7. ISO/SR 10198 Мікрографія – Мікрофільмувальний апарат динамічного знімання для 16-мм мікроплівки – Механічні та оптичні характеристики (Micrographics – Rotary camera for 16 mm microfilm – Mechanical and optical characteristics);
8. ISO/NP 21740 Безпека та відмовостійкість – Настанова з процесу оцінки складності з метою підвищення безпеки та відмовостійкості (Security and resilience – Guideline for complexity assessment process to improve security and resilience);
9. ISO/NP 21499 Система завчасного попередження зсуву за підтримки місцевого самоврядування (Security and resilience – Community-based landslide early warning system);
10. ISO/DTR 19247 Фотографія – Настанови для надійного випробування цифрових фотокамер (Photography – Guidelines for reliable testing of digital still cameras);
11. ISO/DIS 12234-3 Електронне відображення фотознімка – Змінний пристрій пам'яті – Частина 3: XMP для цифрової фотографії (Electronic still picture imaging – Removable memory – Part 3: XMP for digital photography);
12. ISO/DIS 17068 Інформація та документація – Сховище довірчої третьої сторони для цифрових записів (Information and documentation – Trusted third party repository for digital records);
13. ISO/SR 23081-1 Інформація та документація – Процеси управління записами – Метадані для записів – Частина 1 – Принципи (Information and documentation – Records management processes – Metadata for records – Part 1: Principles);

14 ISO/SR 12029 Управління документообігом – Машиночитані паперові форми – Оптимальний проєкт для забезпечення зручності користувачів і систем електронного управління документообігом (EDMS) (Document management – Machine-readable paper forms – Optimal design for user friendliness and electronic document management systems (EDMS));

15 ISO/CD 19475-1 Управління документообігом – Мінімальні вимоги для зберігання документів – Частина 1: Фіксація (Document management applications – Minimum requirements for the storage of documents – Part 1: Capturing);

16. ISO/CD 19475-3 Управління документообігом – Мінімальні вимоги для зберігання документів – Частина 3: Видалення (Document management – Minimum requirements for the storage of documents – Part 3: Disposal);

17. ISO/SR 10244 Управління документообігом – Основи та аналіз бізнес-процесів (Document management – Business process baselining and analysis);

18. ISO/SR 28003 Системи управління безпекою для мережі постачань – Вимоги до органів, які проводять аудит і сертифікацію систем управління безпекою мережі постачань (Security management systems for the supply chain – Requirements for bodies providing audit and certification of supply chain security management systems);

19. ISO/SR 25111 Управління безперервністю бізнес-процесів – Настанова із соціальних аспектів забезпечення безперервності бізнес-процесів (Business continuity management – Guidance on human aspects of business continuity).

Результати аналізу 7 міжнародних стандартів запропоновано фахівцям НДІ мікрографії щодо розгляду можливості застосування в наукових роботах, які виконують згідно з Тематичним планом прикладних досліджень та дослідно-конструкторських (технологічних) робіт НДІ мікрографії на 2016 рік та під час виконання робіт у перспективі.

Також матеріали чотирьох міжнародних стандартів за напрямом «Безпека» рекомендовано працівникам Українського науково-дослідного інституту цивільного захисту під час розроблення нормативних документів.

Міжнародні стандарти надають можливість отримувати нові наукові знання для досягнення суспільно корисних результатів у сфері СФД, забезпечити якісну та кваліфіковану роботу працівників установ СФД, впровадити науково-практичні результати в наукову діяльність НДІ мікрографії.

ШИРОКОФОРМАТНЫЕ СКАНЕРЫ

Источник: <http://www.storage-systems.ru/scanners/largescanners/>. Продолжение, начало в Информационных бюллетенях № 3, № 4 и № 5 за 2016 год.

Широкоформатные сканеры используются для сканирования карт, чертежей и других документов большого формата, обеспечивая высочайшее разрешение и точную цветопередачу даже при компактных размерах.

ScannTECH 600i-fb

Плоскостной сканер большого формата с высоким разрешением



ScannTECH 600i-fb — это быстрый, производительный плоскостной сканер большого формата с высоким разрешением для получения четких изображений документа. Современный плоскостной сканер ScannTECH 600i-fb задает новые направления в скорости и качестве.

Современное освещение белыми светодиодами гарантирует высокое качество изображений при низком уровне воздействия на оригинал. Светодиоды без ультрафиолета и инфракрасного излучения имеют срок службы 50000 часов и обеспечивают высокое качество картинки.

Камера также является передовой технологией. Корпус камеры, не пропускающий пыль, ССD-система, запатентованный метод совмещения и оптическое разрешение 600x600 dpi гарантируют высокое качество.

Преимущества сканера

- От трех до четырех снимков А0 в минуту
- Оптическое разрешение 600x600 dpi
- Высокая геометрическая точность сканирования
- Сканирование по сети
- Высокая экономия благодаря конструкции, практически не требующей обслуживания
- Современное светодиодное освещение

Технические характеристики

Оптическое разрешение	180° 600 dpi
Размер активного сканирования	Ширина 914 мм, длина 1220 мм, форматы больше DIN А0 могут сканироваться по частям
Размер документа	Автоматический формат, DIN, пользовательские форматы с областями интереса до 600 мм
Программное обеспечение	PROView
Экспозиция и оптика	Белые светодиоды по IEC 60825-1: класс 1 без УФ/ИК-излучения
Цвет и обработка изображения	Гамма, яркость и контраст (для каждого цветового канала), точка черного и точка белого
Функции	Цифровой баланс цвета, автоматический или ручной порог черного, коррекция, автоматический баланс белого, встроенные ICC-профили
Глубина цвета	36 бит, 12 бит в оттенках серого
Выходные режимы	24 бит цвета RGB, 8 бит оттенки серого, монохром
Глубина фокуса	5 см
Ножная педаль	Для запуска сканирования
Толщина и масса оригинала	15 см и 20 кг
Выход данных	JPEG, PNM, TIFF без сжатия, TIFF G4 (CCITT), PDF и все стандартные форматы изображения
Интерфейс	1 гигабит Ethernet с TCP/IP
Камера	3 ССD-линейки в пылезащищенном корпусе, 68000 пикселей
Размеры (Д x Ш x В)	172 x 112 x 106 см
Масса	90 кг
Электропитание	100-240 В, 50/60 Гц

Температура	от 5 до 40°C
Относительная влажность	20—80% (без конденсата)
Минимальные требования к ПК	Рабочая память 4096 Мб, гигабитное Ethernet-подключение, Современный процессор Intel/AMD, Windows XP, Windows Vista, Windows 7

book2net Hornet
буктунет Хорнет
Широкоформатный сканер



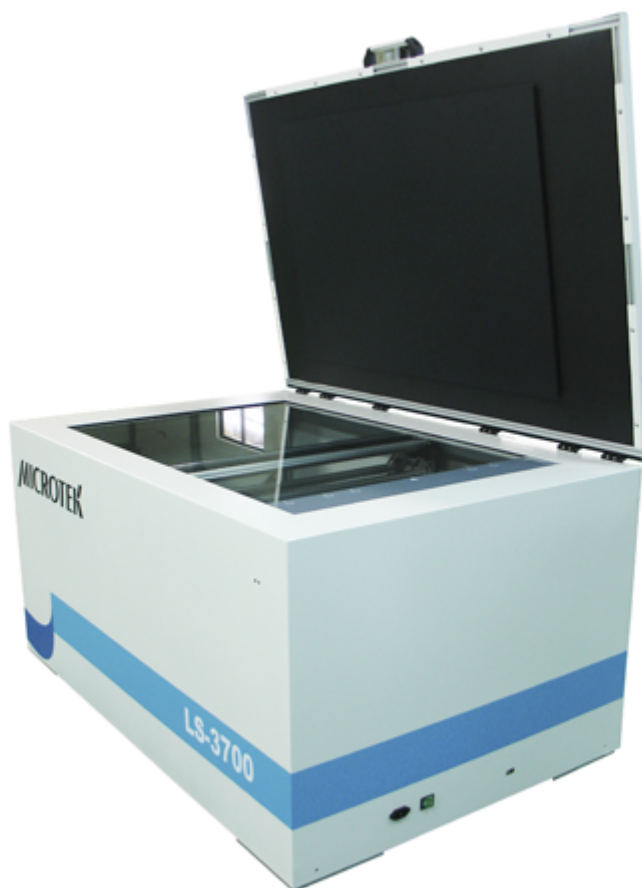
Широкоформатный сканер book2net HORNET AO - это устройство с высокой производительностью, предназначенное для оцифровки большого количества крупноформатных, неудобных в обращении и особо тяжёлых изданий, которое гарантирует максимально бережное обращение с оригиналами. Благодаря двойной лазерной системе сканер book2net HORNET способен за считанные секунды настроить оптимальный уровень резкости.

Главное о широкоформатном сканере Book2net Hornet

- Разрешение 300 / 400 dpi (600 dpi по запросу)
- Скорость сканирования 0,3 сек.
- Стандартная скорость обработки данных 3,2 сек.
- Высокая производительность

- Длительный срок эксплуатации
- Оптимальное соотношение сигнал/шум
- Высокая эргономичность
- Легкость в эксплуатации (ручное и педальное управление)
- Регулируемая высота рабочей плоскости
- Полуавтоматизированная система (ПЛК и линейный привод, книжная колыбель с электроприводом, прижимное стекло с электроприводом, ручное, полуавтоматическое или автоматическое управление по выбору пользователя)
- Система щадящего светодиодного освещения

Microtek LS-3700
Микротек ЛС-3700
Крупноформатный планшетный сканер



Microtek LS-3700 - идеален для больших документов: цветных постеров, архитектурных чертежей, инженерных и технических синек. Более того, он также может сканировать одежду, текстиль, переплетенные книги, хрупкие материалы, произведения искусства и другие оригиналы. LS-3700 оснащен цветной CCD матрицей с оптическим разрешением 600 dpi, гарантирующей высочайшее качество сканирования. Двусторонний светодиодный источник света ликвидирует тени при сканировании объемных

объектов, а также не требует времени на прогрев, сканер готов к работе сразу после включения.

Главное о широкоформатном сканере Microtek LS-3700

- Большая область сканирования
- Планшетный дизайн подходит для самых разных нужд
- Двухсторонняя светодиодная лампа подсветки, уменьшающая влияние теней на изображения
- Единый CCD сенсор (бесшовное сканирование)
- Оснащен четырьмя колесиками с изменяемым уровнем, что позволяет без труда перемещать и хранить сканер
- Промышленный передаточный механизм
- Глубина фокуса 10 мм
- Специальное ПО ScanWizard LS

Технические характеристики широкоформатного сканера

Microtek LS-3700

Название	LS - 3700
Тип сканера	Крупноформатный планшетный сканер
Тип сенсора	Цветной линейный CCD
Разрешение	600 dpi
Источник света	Светодиод
Область сканирования	635 мм x 940 мм
Скорость сканирования	45 с при 300 dpi, A1 цвет
Глубина цвета	Ввод: 48-бит Выход: 24-бит
Размер бумаги	>A1
Подключение	Hi-Speed USB 2.0
Тип сканирования	На отражение
Поддерживаемые типы файлов	TIF, JPG, BMP
Поддержка ОС	Windows 7 / 8 (X64)
Размер	133 см x 87 см x 72 см (без крышки)
Вес	170 кг
Источник электроэнергии	Постоянный ток 100В - 240В, 50 / 60 Гц, макс. 1,7А (Ввод)
Энергопотребление	37,5 Ватт
Системные требования (ПК)	CD-ROM привод (для установки ПО) Цветной дисплей с поддержкой 24-битного цвета 4 Гб или более ОЗУ Процессор Intel Core i5 3.0 GHz или лучше с портом Hi-speed USB (USB 2.0)

	Microsoft Windows 7 / 8 (X64)
ПО в комплекте	ScanWizard LS



СКАНЕРЫ МИКРОФОРМ

Сканеры микроформ незаменимы при работе с микрографическими архивами, они позволяют преобразовывать в цифровую форму микрофиши и рулонную микроплёнку всех распространенных форматов, в том числе и в полностью автоматическом режиме.

Краткие описания наиболее популярных моделей сканеров микроформ, предлагаемых компанией АКТЕК XXI, представлены ниже.

Эклипс

Высокопроизводительный сканер микроформ



Высокопроизводительный сканер рулонных микрофильмов Eclipse разработан для пользователей, перед которыми стоит задача сканирования больших объемов информации в кратчайшие сроки при минимальных затратах.

В сочетании с программным обеспечением NextStar, реализующим инновационную, запатентованную методологию сканирования, Eclipse достигает скорости сканирования 590 кадров в минуту. При этом он может эксплуатироваться 24 часа в сутки, демонстрируя уникальную надежность.

Среди множества инноваций, использованных в сканере Eclipse, необходимо отметить уникальную оптическую систему, позволяющую достигать невероятной скорости сканирования и высокой точности при меньших значениях освещенности.

Преимущества сканера Eclipse

- Использование волоконной оптики устраняет случайные засветки, делает изображения резче. Автофокус и специальные чистящие ролики обеспечивают максимальное качество оцифровки микрофильма.

Программное обеспечение NextStar, поставляемое в комплекте с Eclipse, реализует новую технологию обработки изображений Ribbon Scanning, обеспечивающую создание единого файла, включающего все

- отсканированные изображения с целого рулона. Это дает возможность снизить затраты на сканирование при увеличении его скорости. NextStar позволяет пользователю убедиться, что все кадры были правильно отсканированы, и определяет любой проблемный кадр. Изображения таких кадров могут быть затем скорректированы в процессе просмотра.

NextStar полностью устраняет необходимость в повторном сканировании кадров, обусловленную проблемой плотности или определения границ кадра, увеличивая, таким образом, системную производительность сканера.

- Программное обеспечение NextStar дает возможность пользователю управлять процессом оцифровки от начала до конца. Этот продукт имеет модульную расширяемую структуру и позволяет реализовывать системы оцифровки различного уровня сложности – от единичного автономного рабочего места на базе сканера Eclipse до сложных систем, в которых программные компоненты объединяют различные платформы, а работа распределена между несколькими операторами.

Технические характеристики сканера Eclipse

Сканируемые микроформы	16 и 35 мм рулонный микрофильм /негатив, позитив/серебряная, везикулярная, синяя и черная диазо/ ориентация вертикальная и горизонтальная/Duplex, Duo, Blipped-Unblipped
Характеристики документов	До формата А0 с разрешением 200 dpi, длинные документы типа каротажных кривых и электрокардиограмм
Кратность	от 7х до 72х
Оптическое	100 - 600 dpi

разрешение	
Скорость сканирования	При разрешении 200dpi до 590 кадров/мин
Форматы выходных файлов	TIFF monochrome, TIFF uncompressed, Multi Page TIFF, JPEG, CALS, PDF и JPEG 2000
Сканирующая система	1 пылезащищенная CCD-линейка, 8192 pix
Оптическая система	Высококачественная оптика, формирование плоского светового пучка с помощью оптического волокна
Программное обеспечение	NextStar
Функции программного обеспечения	Автоматическая коррекция светового потока лампы, в частности, гамма-функции, в процессе загрузки и работы; Вращение, зеркалирование, обрезка, доворот, устранение пятен, улучшение отображения краев; Автоматический порог для бинарных изображений; Независимые фильтры обработки для каждого выходного изображения; Мультистраничный выход в различных форматах; Распознавание трехуровневых блип-меток; Наименование файла и индексирование последовательности файлов.
Интерфейс	1 Gbit Fast Ethernet with TCP/IP
Габариты	711 x 482 x 558 мм
Вес	34 кг
Электропитание	100 – 240 В, 50/60 Гц
Опции	Ribbon Storage Device (RSD) устройство для временного хранения отсканированной информации. Данное устройство позволяет хранить большие объемы информации и увеличивает скорость доступа к ней. Доступны 2,4,8 и 16ТВ

ФлексСкан

Универсальный скоростной сканер микроформ



Высокопроизводительный универсальный сканер микроформ FlexScan позволяет оцифровывать 16/35мм рулонную микропленку, микрофиши и апертурные карты с высочайшей скоростью и удобством. FlexScan с его уникальной совокупностью характеристик изменяет представление о качестве сканирования и позволяет Вам сканировать рулонную пленку 16/35 мм со скоростью более 240 изображений в минуту, а микрофишу 105*148 мм со скоростью до 125 изображений в минуту.

Преимущества сканера FlexScan

Для полноценного функционирования сканера не нужна рабочая станция.

- Сетевое подключение позволяет передавать данные в любую точку Вашей сети.

Встроенное программное обеспечение NextStar обеспечивает надежность и простоту просмотра изображений, адаптивное управление скоростью и параметрами сканирования, допускает исправление любых ошибок на стадии предварительного просмотра.

Технические характеристики сканера FlexScan

Сканируемые микроформы	16 и 35 мм рулонный микрофильм, микрофиши, аппертурные карты /негатив, позитив/ серебряная, везикулярная, синяя и черная диазо
Характеристики документов	До формата А0 с разрешением 200 dpi, длинные документы типа каротажных кривых и электрокардиограмм
Кратность	от 7х до 72х
Оптическое разрешение	100 - 600 dpi
Скорость сканирования (200 dpi, 24х)	Рулонный микрофильм 16/35 мм - 240 кадров/мин Микрофиша - 125 кадров/минуту
Форматы выходных файлов	TIFF monochrome, TIFF uncompressed, Multi Page TIFF, JPEG, CALS, PDF и JPEG 2000
Сканирующая система	1 пылезащищенная CCD-линейка, 8192 pix
Оптическая система	Высококачественная оптика, формирование плоского светового пучка с помощью оптического волокна
Программное обеспечение	NextStar
Функции программного обеспечения	Автоматическая коррекция светового потока лампы, в частности, гамма-функции, в процессе загрузки и работы; Вращение, зеркалирование, обрезка, доворот, устранение пятен, улучшение отображения краев; Автоматический порог для бинарных изображений; Независимые фильтры обработки для каждого выходного изображения; Мультистраничный выход в различных форматах; Распознавание трехуровневых блип-меток; Наименование файла и индексирование последовательности файлов.
Интерфейс	1 Gbit Fast Ethernet with TCP/IP
Габариты	711 x 482 x 558 мм
Вес	34 кг
Электропитание	100 – 240 В, 50/60 Гц
Опции	Ribbon Storage Device (RSD) устройство для временного хранения отсканированной информации. Данное устройство позволяет хранить большие объемы информации и увеличивает скорость доступа к ней. Доступны 2,4,8 и 16ТВ

Викс энд Вилсон 7750 Микрофиш Сканстэйшн
Поточный сканер микрофиш Scanstation



Компания Wicks and Wilson представляет устройство 7750 Scanstation – новое поколение автоматизированных сканеров микрофиш. Усовершенствованные функции облегчают автоматизированную оцифровку микрофиш. Файлы цифровых изображений создаются со всех форматов микрофиш. Максимальная производительность, минимальные усилия.

Сканер 7750 компании Wicks and Wilson предназначен для оцифровки и обработки изображений в оттенках серого и черно-белых тонах с микрофиш различных форматов. В этом высокопроизводительном сканере используется надежная система автоматической подачи закрытого типа. Такая система не допускает пропуск микрофиш, их повреждения или заедания во время автоматического сканирования.

На выходе можно получить как отдельные изображения с микрофиши, так и цифровой архив (сканированное изображение всей микрофиши). Программное обеспечение Virtual Scanstation компании Wicks and Wilson предназначено для последующего редактирования цифровых архивов. Проверка качества каждого кадра может выполняться на отдельном компьютере без замедления или остановки потокового сканирования.

Преимущества сканера микрофиш Wicks and Wilson 7750 Microfiche Scanstation

- Устройство разработано специально для сканирования микрофиш: сменные объективы, голографический рассеиватель и 12-битная линейка обеспечивают высокое качество изображения для микрофиш всех типов.

- Специальные алгоритмы обработки изображений компании Wicks and Wilson выполняются на мощном многоядерном графическом процессоре nVIDIA®, любые изменения отображаются в реальном времени без повторного сканирования.

- Надежная система автоматической подачи фиксирует микрофишу во время сканирования. Возможна дальнейшая доработка для поддержки увеличенных микрофиш.

- Новые инструменты редактирования и обработки изображений облегчают и ускоряют сканирование микрофиш любых форматов.

- Интерактивная графическая настройка позволяет подобрать параметры сканирования для всех типов микрофиш без многократных предварительных проверок.

- Функция автоматической калибровки обеспечивает высокое качество на выходе.

- Оптимизированный змеевидный процесс сканирования значительно повышает производительность при работе с джеккетами.

- Доступны различные варианты наименования файлов: одностраничный, многостраничный, по индексу ячейки или ручной. Точность индексации фиши обеспечивается пользовательскими полями с двойным ключевым вводом.

- Поддержка журналирования для создания полные отчеты о процессе потокового сканирования.

Технические характеристики сканера Wicks and Wilson 7750 Microfiche Scanstation

Разрешение	100—600 dpi
Редукционный коэффициент кратности (фиксированный фокус)	От 7,5х до 50х (изменяемая кратность изображения)
Проверка поддержки печати	Да
Точность масштабирования	±1%
Типы пленок (148×105 мм)	Позитивные/негативные, серебряные/везикулярные/диазотипные, односторонние/двусторонние, лист/джеккет, СОМ, АВ микрофиша, вертикальные/горизонтальные
Формат микрофиши/джеккета	Все обычные форматы (колонки, столбцы с отношением до 50), включая смешанные форматы
Размер картриджа	Стандартный, либо для увеличенных микрофиш
Скорость (при разрешении 200 dpi)	295 кадров в минуту
15x18СОМ микрофиши	105 кадров в минуту

48х 7х14 микрофиши 24х 5 рядный джеккет 24х	94 кадров в минуту
Выходные форматы файлов для черно-белых изображений	TIFF, G3 или G4 (одностраничный и многостраничный), CALS, PDF (одностраничный и многостраничный)
Выходные форматы файлов для изображений в оттенках серого	JPEG, BMP, JPEG 2000, RAW TIFF, PDF (одностраничный и многостраничный)
Сертификаты соответствия	CE, UL, cUL
Соответствие RoHS	Да
Габаритные размеры (Ш×Г×В)	570×360×471 мм
Масса	36 кг
Электропитание	120/230 В, 1/0,5 А
Интерфейс подключения к ПК	Специальная карта PCI Express X1 (в комплекте), требуется полноразмерный слот
Операционная система	Windows 7 Professional (32-разрядная)
Спецификация управляющего ПК	Требования к ПК указаны на сайте компании WWL www.wwl.co.uk

ЗМІСТ

Передмова.....	1
Использование легальных методов промышленного шпионажа в сетевой разведке.....	2
Европейское агентство по кибербезопасности ENISA опубликовало анализ стандартов, касающихся поставщиков услуг доверия.....	9
США: Опубликована новая редакция авторитетного стандарта по защите документов NFPA 232.....	10
Италия: Новой проблемой в области электронной сохранности становятся «документы без формата».....	12
Инструменты анализа форматов для архивистов.....	16
<u>Великобритания: Архивы для будущего - новое видение.....</u>	23
Перелік міжнародних стандартів, які опрацьовано та проаналізовано НДІ мікрографії за I півріччя 2016 року.....	25
Широкоформатные сканеры:.....	28
ScannTECH 600i-fb.....	28
book2net Hornet.....	30
Microtek LS-3700.....	31
Сканеры микроформ.....	33
Эклипс.....	33
ФлексСкан.....	36
Викс энд Вилсон 7750 Микрофиш Сканстэйшн.....	38

