# ПЕРЕДМОВА

Випуск дайджесту присвячено досвіду установ світу щодо зберігання і використання мікрофільмів та електронних носіїв інформації в сучасному інформаційному просторі.

У публікації «Микрография» розглянуто типову схему процесу мікрофільмування. Наведено переваги використання носіїв інформації на мікрографічних плівках з використанням сучасних технологій.

У публікації «Значение микроформ в сохранности фондов библиотек и архивов России (на примере деятельности фонда микроформ РНБ)» наведено історію розвитку мікрографії СРСР та страхового мікрофільмування. Розповідається про створення та функціювання фонду мікроформ Російської національної бібліотеки (РНБ). Зроблено висновки, що мікрографія, в останні роки, з другорядної підгалузі копіювально-розмножувальних процесів, перетворилась у самостійну галузь, яка відіграє важливу роль в збереженні, доступності та комплектуванні фондів бібліотек та архівів.

У публікації «Коллекции. Фонд изданий на микроформах. Российская национальная библиотека» розповідається про фонд мікроформ, який є спеціалізованим фондом системи основних документальних фондів Російської Національної бібліотеки.

У публікації «Методика выбора оптимальной СЭД – наш опыт» наведено типи систем що входять до складу СЕД, завдання, які повинна вирішувати обрана система, бізнес-критерії та технологічні критерії її оцінки. Визначено фактори які підвищують ймовірність успіху.

У публікації «Документооборот и BYOD: как мобильная версия СЭД помогает идти в ногу со временем» розповідається, що з новим поколінням працівників в сучасний офіс увірвалася концепція BYOD (Bring Your Own Device) – організація робочого процесу з використанням особистих мобільних облаштувань співробітників. Це доставляє багато клопоту в такій консервативній сфері, як документообіг. Впровадження СЭД ТЕЗА, яка має мобільний інтерфейс, дає можливість йти в ногу з сучасною тенденцією до мобільності і в той же час зберігати організаційні переваги електронного документообігу.

У публікації «Кибербезопасность в Украине. Дискуссия» розповідається про питання розглянуті на засіданні круглого столу, яке було проведено інститутом Горшенина за темою «Як узабезпечити Український кіберпростір?».

У публікації «Как защититься от вирусов-шифровальщиков?» наведено відгуки фахівців з інформаційної безпеки щодо атаки комп’ютерного вірусу Petya.A, та необхідні заходи з підвищення рівня захисту від вірусних атак в подальшому.

# МИКРОГРАФИЯ

Источник: http://nationscup2015.ru/6646/

Микрографию традиционно относят к репрографическим способам тиражирования документов, и до недавнего времени такая классификация соответствовала действительности. В самом деле, несмотря на чисто фотографический способ получения микроформы, ее можно назвать копией оригинала, значительно уменьшенной, но тем не менее факсимильной копией, точно воспроизводящей всю информацию, которую содержит оригинал. Дальнейшая работа с микроформой (тиражирование, получение увеличенных копий) связана с чисто копировальными процессами. Микрография – эффективное средство регистрации, хранения и обмена информацией. При помощи микрографии фиксируют практически любую документную информацию.

Если проанализировать техническую сущность микрографии, нетрудно заметить, что этот процесс представляет собой сочетание фотографии и репрографии (т. е. копировальных процессов).

Типовая схема процесса микрофильмирования заключается в следующем:

1. подготовка информации (документов) к микрофильмированию;
2. съемка материала на специальных камерах;
3. фотохимическая обработка (проявление и фиксирование микропленки);
4. контроль качества съемки и проявки (при неудовлетворительном качестве производится повторная съемка);
5. копирование микроформ в необходимых количествах;
6. укладка микроносителей в хранилище и рассылка пользователям;
7. изготовление (при необходимости) бумажных копий с микрофиш;
8. сканирование микроформ для передачи по техническим каналам связи и компьютерным сетям удаленному пользователю.

С появлением так называемых COM-технологий открываются новые возможности применения микрографии в офисной деятельности. COM-технология определена своим названием и расшифровывается как Computer Output Microfilming, т. е. технология, позволяющая производить микрофильмирование не документов, а данных, поступающих на вход системы с интерфейса компьютера, или данных, считанных с какого-либо магнитного и/или магнитооптического носителя. Особенностями такой технологии являются высокий фактор редуцирования – до 72X и скорость обработки документов – до 440 страниц в минуту, что в десятки раз превосходит скорость обработки документов при оптической съемке. При этом улучшается качество изображения на микроформе, количественно

уменьшается обращение бумажных документов и даже появляется возможность автоматически создавать образы документов, используя неформализованные данные с компьютерных систем.

Часто сравнивают COM-системы с принтером, с одним отличием – печать осуществляется на микрофотоноситель, и даже существует выражение «печать на микрофишу». Так же как и принтер, COM-система может быть использована в сетевом режиме, а за счет большой производительности – обслуживать одновременно несколько сетей. COM-системы работают в полном автоматическом режиме с закрытым способом обработки микрофотоносителей.

В настоящее время в практику работы офисов и электронных архивов внедряются гибридные системы, представляющие собой совмещенные комплекты оборудования сканирования микроформ (получение электронного образа) и печати микрофильмов. Современные сканеры микроформ имеют возможность работать в автоматическом режиме, в том числе и в режиме пакетного сканирования микрофиш, с автоматической покадровой разметкой и масштабированием.

Микрографическими архивами широко пользуются государственные структуры, государственные и коммерческие банки, национальные и публичные библиотеки, государственные архивы, научные и проектные учреждения, страховые компании, военные ведомства и т. д. Гарантированный срок хранения информации на микрографическом носителе, без потери качества, без специальных требований к условиям хранения и при невозможности несанкционированного внесения изменений, составляет не менее 100 лет, а объемы хранения сокращаются в сотни раз.

Новые образцы оборудования значительно расширили возможности работы с микроформами, сделав их практически сопоставимыми, в смысле оперативности, с электронными носителями. В результате микрографические хранилища оказались сегодня наиболее дешевыми, надежными и удобными при практической реализации. Любые данные микрографического носителя могут быть оперативно переведены в электронную форму, а данные, записанные в электронном виде, могут быть перенесены на микрографические носители, минуя бумажную форму представления. Правительства многих стран мира законодательно утвердили подлинность документов, снятых на микрофильм, а их юридическая сила приравнена к оригиналу.

# ЗНАЧЕНИЕ МИКРОФОРМ В СОХРАННОСТИ ФОНДОВ БИБЛИОТЕК И АРХИВОВ РОССИИ (НА ПРИМЕРЕ ДЕЯТЕЛЬНОСТИ ФОНДА МИКРОФОРМ РНБ)

Источник: http://docplayer.ru/30371853-Znachenie-mikroform-v-sohrannosti-fondov-bibliotek-i-arhivov-rossii-na-primere-deyatelnosti-fonda-mikroform-rnb.html

В мире накоплены и постоянно растут огромные информационные массивы, подлежащие долгосрочному хранению, начиная от библиотечных фондов и юридических документов и заканчивая чертежами атомных электростанций. Резко возросло количество пользователей информационными системами. Это потребовало развивать и совершенствовать средства технической обработки документальной информации электрофотографии, диазографии, малой офсетной печати и др.

Использование этих средств, привело к резкому потреблению бумаги, но не решило вопроса долговременной сохранности информации. Особым направлением стало внедрение систем электронной обработки данных. О положительных сторонах этого способа обработки информации говорить не приходится. Но вот вопрос о долговременности хранения такого рода записанной информации решить пока не удается. Для поддержания длительного доступа к цифровым документам нужны постоянные вложения на перекопирование и обновление цифрового носителя, что необходимо для того, чтобы он считывался новыми программно-аппаратными средствами.

Техническая база микрофильмирования остается прежней на протяжении уже нескольких десятилетий и не имеет альтернатив в практике сохранения и гарантированного извлечения информации.

*Таким образом одним из наиболее проверенных средств хранения и использования информации остается микрография.*

История ее развития неразрывно связана с развитием фотографических и химико-технологических процессов. Следует выделить три этапа: первый микрография на светочувствительных слоях на основе галогенов серебра; второй микрография на несеребряных светочувствительных слоях; третий микрография на несветочувствительных слоях.

Первый этап развития микрографии начался в 1839 году, когда Джон Данцер разработал основы технологического процесса микрофотографии и получил методом дагерротипии микрокопию. Была получена не только первая микрофотография объекта, но и первая микрофотография документа. Поточное производство микрокопий началось в годах.

Сначала микрофильмы делались на обычной кинопленке. С конца 1930-х годов для микрофильмов начала производится специальная пленка на ацетатной основе. Возникает индустрия миниатюризации информации, ее

поиска и воспроизведения. К 1950 году изготовление рулонных микрофильмов получило очень большое применение.

В СССР микрография стала профессионально развиваться в 1929 году после создания Научно-исследовательского кинофотоинститута (НИКФИ), а с 1934 года параллельно с НИКФИ проблемами микрофильмирования занялась Лаборатория реставрации и консервации документов АН СССР и ряд других организаций.

Со временем были созданы мощные микрографические центры: Производственно-издательский комбинат Всесоюзного института научно-технической информации (ВИНИТИ) АН СССР, Государственная публичная научнотехническая библиотека (ГПНТБ) СССР, Производственно-полиграфическое предприятие «Патент», Всесоюзный научно-технический информационный центр (ВНТИ-центр). Функционировали и активно развивались микрофотолаборатории при крупных библиотеках, архивах, научно-технических институтах и на предприятиях, как правило, оборонного значения.

1990-е годы для многих фотолабораторий оказались роковыми. Их финансирование было почти полностью прекращено. Оборудование демонтировано, частично утеряно. Уволились или были переквалифицированы опытнейшие операторы. (К сожалению, нет учебных заведений для овладения данной профессией, и поэтому особо важна цепочка преемственности и наставничества).

С начала XXI века интерес к микрофильмированию начинает резко возрастать. Повышается долговечность хранения микроформ. Расширяется развитие микрографии, связанное с использованием цветофотографических процессов. Растет количество разработок на голографическом методе. Все больше внимания уделяется производству традиционных микроформ как надежного и проверенного временем способа сохранения и передачи информации.

Выделяется особое направление в области использования микроформ для библиотек – страховое микрофильмирование. Так, например, американская национальная программа сохранности фондов предусматривает, что микроформы постоянного срока хранения, являющиеся страховыми копиями и предназначенные для передачи информации будущим поколениям, помещают в герметичные капсулы из нержавеющей стали (причем пленки предварительно кондиционируют при очень низкой влажности) и хранят под землей, в шахте, при температуре 10 ˚С. Считается, что такие условия обеспечивают сохранность страхового фонда в течение 100 лет и более.

Используя мировой опыт и опыт архивов, в этом направлении российские библиотеки создают свои страховые фонды.

Большую работу по формированию нормативно-технической базы подобных фондов проводит Тульский НИИ репрографии (Репроникс Лтд.). Постоянно пополняется российский регистр страховых микроформ, призванный регистрировать и координировать страховое

микрофильмирование библиотек России. Определяется юридическая база использования микроформ.

Микрография, как процесс сочетания фотографии и репрографии, довольно трудоемка. Для получения микроформ необходимо прежде всего сфотографировать документ с целью получения негатива микроформы 1-го поколения. Она пригодна для многих видов использования (с нее можно получить копию в масштабе 1х1, получить увеличенную копию в копировальном аппарате, ее можно читать при помощи читального аппарата, достаточно долго хранить при правильном режиме, сканировать.

Микроформа 2-го, 3-го и последующих поколений полученная с микроформы 1-го поколения на аппаратах контактного копирования, используется так же, как и микроформа 1-го поколения. Но она призвана защитить ее, как менее дорогая (хотя качество изображения на ней от поколения к поколению ухудшается).

Основными видами микроформ, которые чаще всего востребованы в библиотеках и архивах, являются рулонный микрофильм и микрофиша. Правильно выбранный вид микроформы обеспечивает ей наиболее оптимальные условия хранения и использования.

*Рулонный микрофильм* – наиболее распространенный вид микроформ. Аппараты, работающие на рулонной пленке, обладают более высокой производительностью, чем камеры для съемки на форматную пленку, кроме того в случае необходимости с рулонного микрофильма можно получить дубль в форме микрофиши, он более пригоден для сканирования на диски. Рулонный микрофильм может состоять из одного или несколько рулонов, что очень удобно в тех случаях, когда микрофильмируемый документ содержит большое число страниц. С другой стороны, один рулон может содержать микроизображения нескольких документов. (Как правило, применяют микрофильм длинною 30 м, но возможно применение и до 300 м).

Главными достоинствами рулонного микрофильма являются простота изготовления, возможность автоматизированной съемки большого числа кадров, невозможность утери части кадров.

Серьезным недостатком рулонного микрофильма является сложность поиска информации при значительной длине рулона (при этом возможна деформация микрофильма, появление зацепов, что в конечном итоге приводит к разрыву), необходимость многократной перемотки пленки при поиске информации для чтения или копирования. Для библиотек рулонный микрофильм полезен при съемке либо очень большого массива информации (например, съемка подшивок газет за большой промежуток времени), либо ограниченного по объему документа (например, книга, рукопись и т. п.).

Микрофиши относятся к плоским микроформам, которые получают покадровым экспонированием форматной пленки. По сравнению с рулонным микрофильмом микрофиша имеет ряд преимуществ, главные из которых возможность произвольного прямого доступа к отдельным частям массива большой емкости, большая сохранность микроформ при пользовании массивом, оперативное использование отдельных микрофиш (при чтении,

изменении информации или ее копирования), меньшие площади хранения, их простота и удобство использования, экономичность при пересылке. (На одной стандартной микрофише размещается 60 страниц формата А4, характерного для многих журналов, или 120 страниц наиболее распространенного книжного формата). Для удобства поиска микрофиша снабжается специальным полем размещения библиографического описания документа, читаемого невооруженным глазом.

Таким образом микрофиши являются так называемыми микрокнигами, выпускаемыми наряду с традиционными книгами и журналами. Необходимо отметить их высокую эффективность. При широком распространении микрографии расходы на один экземпляр публикации могут быть в 20 раз меньше, чем при печати на бумаге. В библиотеках микрофиши желательно применять при копировании журналов, альманахов, сборников научных трудов, словарей, справочников.

Апертурные карты (перфокарты) и кляссерные карты типа «джекет» большого применения в библиотеках не имеют.

Особо выделим такой важный фактор микроформ, как их компактность, что очень широко используется библиотеками при пересылке документов по международному (ММБА) и межгородскому (МБА) библиотечным абонементам, для сокращения потребности в помещениях, особенно депозитарных фондов. (При замене оригиналов изданий микроформами экономия площади хранения составляет 90-95%).

При микрофильмировании довольно часто встает проблема сохранности снимаемых документов. Зачастую съемка невозможна без расшивки оригиналов документов, иногда возникает необходимость в реставрации оригиналов после микрофильмирования. Тут особо следует подчеркнуть важность квалификации операторов, их опыт работы.

Начиная с 1960 – 70-х годов, когда всерьез была осознана проблема ухудшения физического состояния бумаги и резко возросла потребность в площадях для хранения, перед крупными библиотеками и архивами назрела необходимость перевода наиболее ценных документов на микроформы, как наиболее проверенные и надежные средства хранения и использования информации.

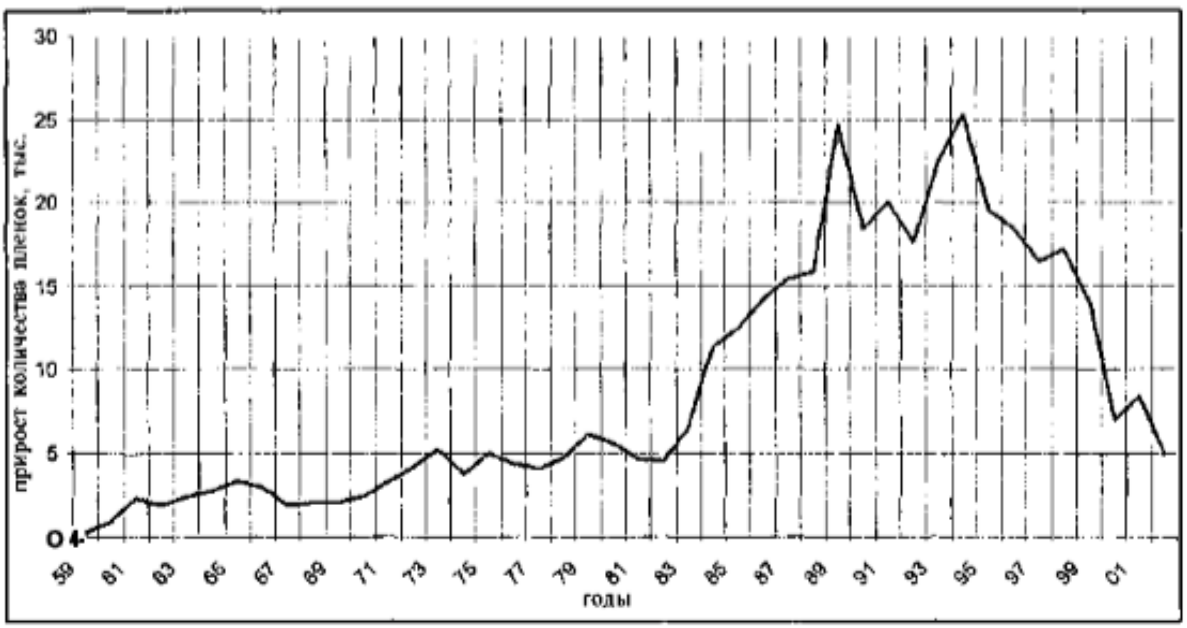
Так начали создаваться специализированные фонды фонды микроформ. Каждая библиотека или архив решали и решают организацию подобных фондов по-разному. Хотя основные задачи и проблемы в процессе их становления и развития во многом совпадают.

Характерным примером организации таких фондов может служить создание и функционирование фонда микроформ Российской национальной библиотеки (РНБ).

Организованный в 1959 году фонд микроформ является структурной частью системы основных фондов РНБ и предназначен для постоянного хранения микроформ и обслуживания ими пользователей библиотеки, для восполнения пробелов в фондах РНБ, защиты редких и ценных изданий от изнашивания, сокращения числа отказов пользователям библиотеки.

Первоначально штат фонда составляли 2 сотрудника. Читательских мест и аппаратов для чтения тоже было 2. Посещаемость за год составляла 226 читателей с выдачей 206 единиц хранения. Всего во вновь созданный фонд поступило 1127 единиц хранения.

В настоящее время фонд микроформ насчитывает более 450 тысяч единиц хранения, 40 читательских мест (с аппаратами для чтения) в собственном читальном зале.




Прирост фонда микроформ за 1959—2002 годы

За годы своего существования фонд развивался довольно равномерно, хотя необходимо отметить его стремительное накопление с 1984 по 1996 годы и заметное снижение поступлений в фонд с 1999 по 2002 годы. Наибольшее количество фонда составляют периодические издания (62,52%), и это вполне оправданно.

Наиболее востребованные документы, например, книги, в последнее время часто выходят в виде репринтных изданий, переиздаются. Да и сам процесс чтения книг «от корки до корки» меньше деформирует документ, чем чтение периодики, когда для поиска нужной информации требуется пролистать большое количество страниц. Книги носят более узконаправленный характер (есть, разумеется, и исключения), имеют свой круг читателей. Периодические издания же часто включают информацию по самым различным областям знания. Спрос на периодику прошедших лет трудно прогнозировать, он носит часто выборочный характер.

В фонд поступают отечественные и зарубежные микроформы всех видов документов, кроме рукописей (которые направляются в фонд Отдела рукописей). Рабочие копии (позитив) с изданий, хранящихся в специализированных отделах, направляются в соответствующие фонды. Есть микроформы копии с традиционных изданий и оригинальные издания, существующие только на микроносителях.

Источник комплектования фонда: покупка, обмен, дар, страховое микрофильмирование (к сожалению, в РНБ данное направление находится в самой начальной стадии, реальных страховых микроформ пока нет). Фонд комплектуется оригиналами документов, которые отсутствуют в библиотеке; документами с недостаточным количеством экземпляров, но пользующимися спросом пользователей РНБ, в целях защиты оригинала от быстрой изнашиваемости; наиболее ценными документами с исторической и научной точек зрения, независимо от спроса; наиболее актуальными текущими зарубежными периодическими изданиями, запрашиваемыми по МБА и ММБА, но по существующему положению не выдаваемыми в виде оригинала за пределы библиотеки.

В фонд поступают, как правило, негативная и позитивная микроформа. В исключительных случаях допускается изготовление еще одной или двух позитивных микроформ. До переезда в специальное хранилище (в Новое здание РНБ на Московском пр., 165) негативы и позитивы хранились вместе, хотя условия их хранения различны (это регламентируется ГОСТами).

Долгое время фонд не имел:

– специального хранилища с температурным и влажностным режимом;

– собственного читального зала (функционировал пункт выдачи);

– находился в неудобном для читателей месте (нередко в отдалении от основных фондов и читальных залов библиотеки);

– часто переезжал с одного места на другое;

– аппараты для чтения микрофильмов давно выработали свой рабочий ресурс, технически устарели.

При переезде в Новое здание условия хранения и эксплуатации микроформ существенно изменились. Предусмотрено кондиционирование хранилищ негативов, для хранения микроформ изготовлены специальные металлические шкафы, произошло отделение негативов от позитивов, появился большой читальный зал на 40 мест, оборудованный современными аппаратами для чтения микрофильмов и микрофиш, возросла культура выдачи и обслуживания микроформами, увеличилось количество пользователей фондом, увеличился штат сотрудников (на 1 ноября 2003 года в фонде работает 12 библиотекарей).

В настоящее время большую сложность представляет вопрос о судьбе микроформ, изготовленных во времена организации фонда. Многие из них из-за неправильного хранения и эксплуатации пришли в негодность. Они рассыпаются при первой же попытке работы с ними. Решением этой задачи видится повторная пересъемка оригинала документа, а не с негативной микроформы.

Российская национальная библиотека приняла «Программу обеспечения сохранности фондов РНБ на 2000 – 2005 гг.». Программой регламентируется комплекс всесторонних эффективных мер по обеспечению сохранности фондов РНБ. Устанавливается перечень документов приоритетного хранения в библиотеке.

Основными критериями при отборе таких документов являются уникальность, историко-художественная значимость и спрос (это устанавливается хранителями фондов), их физическое состояние (определяется специалистами Федерального центра консервации библиотечных фондов ФЦКБФ). В первоочередном порядке выполняется экспертиза документов приоритетного хранения. Понятно, что большинство этих документов должно быть микрофильмировано и поступить на обязательное хранение в страховой фонд и фонд микроформ.

Таким образом перед РНБ все больше встает необходимость по созданию своего страхового фонда микроформ. К сожалению, это очень дорогое удовольствие. К страховым копиям предъявляются повышенные требования. Являясь неприкосновенным, страховой фонд микроформ должен храниться, в территориально обособленном от оригиналов и запасных копий месте, в особой упаковке, с соблюдением особых режимов хранения.

Программа ставит задачу более тщательного комплектования и использования фонда микроформ РНБ. Документы, поступающие в этот фонд, должны отвечать требованиям ГОСТов, необходимо добиваться единообразия в их построении, качественного изготовления.

Постоянно возрастающее значение фондов микроформ, как защитных, требует организации их правильного использования.

Микроформам как нетрадиционным способам передачи информации требуются наличие специальных аппаратов для чтения, выработка необходимых навыков у хранителей фонда по работе с ними, выделенные особые места для чтения и хранения. Все эти факторы являются причиной создания специализированного единого фонда микроформ в библиотеках.

Однако интересы пользователей часто диктуют иной способ решения данной проблемы. Микроформы максимально приближены к месту хранения оригиналов. При этом способе размещения фонда значительно ускоряется процесс получения документа (в виде микроформы) пользователем, хранители оригиналов могут более подробно ответить на вопросы, возникающие при чтении, если необходимо, сличают оригинал и микроформу, его заменяющую, и в случае допущенного брака или пропуска микрофильмированных страниц направляют дефектную микроформу на пересъемку, более активно влияют на политику микрофильмирования своих фондов.

Последний вариант использования фондов микроформ имеет наибольшее распространение в мировой практике.

В РНБ с момента создания фонда микроформ наметился довольно своеобразный путь его использования.

В читальном зале фонда позитивные микроформы выдаются пользователям. Работники фонда следят за правильной эксплуатацией аппаратов (для их оперативного ремонта в читальном зале дежурит мастер), состоянием выдаваемых микроформ (в случае значительных дефектов направляют микроформы на дублирование или пересъемку в Отдел внешнего обслуживания РНБ), контролируют и постоянно пополняют справочный

аппарат фонда, который состоит из алфавитного каталога документов на русском языке и на иностранных языках, топографического каталога на негативные и позитивные микроформы.

При необходимости с позитивной микроформы для пользователя изготовляются микроформы, фотографии, ксерокопии.

Пользователи РНБ международного и межбиблиотечного абонемента также получают микроформы для чтения из фонда микроформ, разумеется, при условии, что в библиотеке заказчика есть необходимые аппараты для чтения (при необходимости они могут заказать дублетные микроформы для своих фондов, фотографии и т. д.). Новой формой использования микроформ для пользователей РНБ должна стать передача информации с микроформ по электронной почте.

Отдельно от фонда микроформ РНБ хранятся и используются микроформы (негатив и позитив) в Отделе рукописей РНБ и в архиве РНБ. Изготовление и выдача этих микроформ контролируется Государственной Архивной службой России. В газетном отделе, Отделе национальных литератур, в Отделе стран Азии и Африки имеются только позитивные микроформы (негативы хранятся в фонде микроформ РНБ). Такое решение продиктовано особенностями этих документов.

Таким образом в библиотеке функционирует фонд микроформ и его отдельные части непосредственно в специализированных фондах и читальных залах РНБ.

Интересы пользователей РНБ требуют расширения возможностей использования рабочих микроформ максимально ближе к месту хранения оригиналов документов. Это особенно стало актуально в связи с переездом фонда микроформ РНБ в Новое здание. Пользователи вынуждены читать оригиналы, которые не микрофильмированы, в одном здании, а микроформы – в другом. Это особенно неудобно при частичной съемке периодических изданий.

Учитывая интересы пользователей РНБ, фонду микроформ следует рассмотреть вопрос о создании отдельных пунктов выдачи с аппаратами, с дублирующей частью своего фонда (где будут храниться дополнительные дублетные позитивы микроформ).

Мне кажется, что в сложившейся практике деления фондов РНБ по видам документов (книга, журнал, газета, и т. п.) и закрепления их в конкретных читальных залах, не будет ошибкой функционирование единого фонда микроформ и его частей в других фондах и отделах РНБ. Сочетание централизованного и децентрализованного использования рабочих копий микроформ способствует обеспечению их наибольшей доступности для пользователей библиотеки, всестороннему раскрытию фондов.

Возможно, развитие техники в скором времени позволит решить эту проблему, наладив недорогой, но надежный способ передачи информации с микроформ на электронные виды носителей. Тогда проблема создания пунктов выдачи отпадет сама собой. Фонд микроформ все больше будет брать на себя функцию долговременной защиты оригиналов документов.

Основным способом сохранения фондов микроформ в РНБ должны стать правила консервации и эксплуатации негативов 1-го поколения (если негатив 1-го поколения поступает на хранение в страховой фонд, то негатива 2-го поколения или позитивной копии, его заменяющей).

Эти микроформы должны находится в особых условиях доступа, температурного и проч. режимах хранения. Практика их использования для текущего копирования должна быть сведена к минимуму, выдача пользователю категорически запрещена.

Очень осторожно и вдумчиво должен решаться вопрос количества необходимых фонду микроформ. Копии, полученные с негатива 1-го поколения, безусловно, должны взять на себя функцию защиты этой микроформы. Наличие двух таких копий желательно для сохранности и использования фонда (они могут применяться как для чтения пользователями РНБ, так и для копирования).

Такое количество микроформ, безусловно, сказывается на удорожании, увеличении площадей хранения фонда. Тут важно конкретно определять, насколько часто данный вид микроформ будет востребован в практической деятельности. На решение этого вопроса влияет подготовленность пользователя к чтению микроформ, качество аппаратов для их чтения и копирования, значимость оригинала, частота его использования.

Для сохранности фонда микроформ необходимо постоянное проведение работ по физико-химическому контролю, организации реставрационной и консервационно-профилактической обработки, защиты от плесневого поражения, поиску оптимальной упаковки для хранения микроформ, создание качественных микроформ (организация химического контроля качества поступающих на хранение документов), проведение документальной проверки фонда, результатом которой является выявление несоответствия содержания справочного аппарата и самих микроформ, ликвидация заставок и лакун фонда, пересъемка бракованных или пришедших в негодность документов.

Микрофильмирование дорогой и сложный способ хранения информации, требующий наличия хорошо налаженного, отработанного процесса от выявления необходимых документов для микрофильмирования до правильного их хранения и использования. Небольшие библиотеки и архивы не могут себе позволить возможности иметь постоянно действующую лабораторию для микрофильмирования своих фондов. Требуется государственный подход к этой проблеме.

Мне кажется, что если крупные фотолаборатории возьмут на себя микрофильмирование редких и уникальных документов небольших библиотек и архивов (в обязательном порядке) это позволит сохранить и восполнить фонды как крупных, так и небольших фондодержателей. (При условии, что дублетная микроформа должна обязательно поступать к хранителям оригиналов документов).

Микрофильмирование позволяет завершить долгую и кропотливую работу, проводимую библиографами по пути поиска недостающих номеров и

изданий, слияния архивных документов. Возможны договора о совместной собственности на созданные таким образом документы. Это позволит, при грамотной политике, частично оправдать затраты на микрофильмирование путем продажи созданных более полных комплектов зачастую очень уникальных и значимых документов. Большую работу в доукомплектовании своего газетного фонда за счет микрофильмирования и создания страхового фонда газет проводит Государственная Российская библиотека (РГБ). Газетному отделу РНБ и другим библиотекам России необходимо активно включаться в эту работу.

Библиотекам и архивам следует активнее использовать возможности покупок готовых копий микроформ как в России, так и за рубежом.

Микрофильмирование желательно более активно применять при проведении реставрационной, консервационной обработки документов. При этом для пользователя при необходимости возможен показ того, каким был документ до реставрации и каким стал после, с увеличением особо важных и значимых фрагментов документа. Оригинал после реставрации будет при этом сохранен и доступен для большего числа пользователей в виде микроформы. В случае повреждения или даже утраты документа в процессе реставрации может остаться микроформа, его заменяющая.

Отметим полярность мнений в вопросе создания страховых и пользовательских фондов библиотек и архивов в связи с появлением электронных носителей информации и места микроформ в этом процессе. В широкой палитре мнений и взглядов существует два крайне радикальных.

Первый из них заключается в следующем: в мире давно отработан процесс микрофильмирования документов, опыт хранения микрофильмов составляет десятки лет, поэтому не надо изобретать ничего нового, работать следует со страховой и пользовательской копией в виде микроформ.

Приверженцы второго крайнего мнения исходят из того, что микрофильмирование это безнадежно архаичный процесс, человечество с изобретением компьютера давно ушло далеко вперед, поэтому все, что можно, надо отсканировать и хранить в виде электронной базы.

Электронные архивы, безусловно, имеют массу привлекательных сторон:

– высокую скорость обработки запросов пользователей и выдачи документов;

– удобство и быстрота копирования документа или его части;

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

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

Однако не следует забывать и об отрицательных свойствах электронных носителей информации и созданных на их базе электронных архивов:

– высокая степень подверженности внешним воздействиям, особенно электромагнитным полям;

– опасность со стороны разного рода компьютерых вирусов;

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

– частая смена технической и программной базы в мировом компьютерном производстве (в ряде случаев приходится полностью менять оборудование, носители информации и переписывать созданный фонд заново).

Учитывая большие объемы, высокую значимость и ценность информации, «отмахнуться» от такого своебразия просто невозможно.

Истина, как всегда, находится посередине и заключается в оптимальном сочетании фиксирования информации на микроформах и на электронных носителях. Такой способ сохранения фондов ни в коем случае не исключает друг друга, а наоборот, дополняет, образуя органическую структуру, в которой документы в зависимости от необходимости переходят из одной формы хранения и использования в другую.

Возможность такого перехода обеспечивается современными техническими средствами, позволяющими оперативно конвертировать документы из микроформы в электронный файл и обратно. Это обеспечивается сканерами микрофильмов. Эти устройства позволяют быстро и эффективно сканировать все виды микроформ. Большой экран обеспечивает оператору возможность видеть документ во всех деталях и работать с ним осмысленно, что особенно важно при сканировании угасающих документов. Возможность масштабирования, поворота изображения, регулирование контрастности, очистка позволяют вытянуть даже очень плохо читаемые документы и сохранять их в обновленной качественной электронной копии.

Обратный переход от электронной формы хранения информации к микрофильму осуществляется с помощью так называемых COM-систем. Их еще иногда называют фотопринтерами по выполняемой ими функции. Они обеспечивают печать электронного файла на фоточувствительной поверхности микроформы. Основная функция COM-системы – это фиксирование документов на микроформах при их приоритетном существовании в электронном виде. Необходимо отметить, что эти системы хорошо работают как с галогенидосеребряными, так и с везикулярными пленками и могут быть укомплектованы соответствующим проявочным процессом. Таким образом, достаточно отправить по сети файл на COM-систему и тут же возможно получение микроформы для длительного хранения. Это позволяет микроформам усиливать свою страховую функцию, в деле сохранности фондов библиотек и архивов, не конкурировать с электронными видами носителей, а дополнять их.

Микрография не случайно в последние годы из второстепенной подотрасли копировально-множительных процессов превратилась, по существу, в самостоятельную отрасль, играющую важную роль в

сохранности, доступности и комплектовании фондов библиотек и архивов. Уверен, что она будет активно развиваться и совершенствоваться, находить все большие пути применения и использования.

## ЛИТЕРАТУРА


1. Миз К., Джеймс Т. Теория фотографического процесса. Л.: Химия,
2. Джеймс Т.Х. Теория фотографического процесса. Л.: Химия,
3. Чибисов К.В. Общая фотография. М.: Искусство,
4. Фотокинотехника: Энциклопедия / Под ред. Е.А.Иофиса. М.: Сов. энциклопедия,
5. Слуцкин А.А. Микрофильмирование. М: Наука,
6. Максимов Н.П., Сидоров Ф.В. Микрофильмирование карт и чертежей. М.: Недра,
7. Основные правила хранения и использования библиотечных фондов. М.: Рудомино,
8. ГОСТ Репрография. Микрография. Требования к документам, подлежащим микрофильмированию.
9. ГОСТ Репрография. Микрография. Основные положения.
10. ГОСТ Репрография. Микрография. Правила хранения микроформ.
11. ГОСТ Репрография. Микрография. Копии, полученные при увеличении с микроформ. Технические требования и методы контроля.
12. Репография. Мирография. Микроформы архивных документов. Общие технические условия.
13. Репрография. Микрография. Микрофильм документа на правах подлинника. Порядок изготовления, учета, хранения и применения.
14. ГОСТ Аппараты читальные и читально-копировальные. Типы.
15. ГОСТ Репрография. Микрография. Микрофиши. Типы.
16. Типовой технологический регламент изготовления микрофиш страхового фонда и фонда пользования. М.,
17. Йерв Г. Срок службы современных носителей информации // Библиотековедение и библиография за рубежом Сб С Агарков В.Г.
18. Роль и значение микрофильмирования документов с целью их сохранности и использования: (На примере деятельности фонда микроформ РНБ) // Консервация памятников культуры в единстве и многообразии: Материалы 4-й междунар. конф. (СПб., окт. 2003) / РНБ; СПб. Междунар. центр сохранения культурного наследия; Сост.: С.А.Добрусина и др. СПб.: [Изд-во РНБ),
19. С Беленький Ю.А., ЗАО «ДиМи-Центр». Сохранность библиотечных фондов микрофильм или электронный файл? (доклад прочитан на 4-й междунар. конф. СПб., окт. 2003).

# КОЛЛЕКЦИИ. ФОНД ИЗДАНИЙ НА МИКРОФОРМАХ. РОССИЙСКАЯ НАЦИОНАЛЬНАЯ БИБЛИОТЕКА

Источник: http://www.nlr.ru/coll/ofo/micro/collections.html

Фонд микроформ является специализированным фондом системы основных документальных фондов Российской Национальной библиотеки и формируется с целью докомплектования фондов РНБ, защиты оригиналов от преждевременного износа, удовлетворения повышенного спроса пользователей и замены оригиналов копиями на компактных носителях информации.

Фонд микроформ выделен по признаку вида носителя информации и имеет своей целью сосредоточение в едином собрании микрофотокопий документов для постоянного хранения и обслуживания пользователей библиотеки.

Фонд микроформ образует специализированный комплекс, состоящий из фонда пользования и запасных (архивного и страхового) фондов и включает в себя микрофотокопии оригиналов документов по всем отраслям знаний и годам издания, хранящимся в РНБ или поступающих из других источников, а также микроформы на правах подлинника при отсутствии бумажного оригинала.

Фонд микроформ один из крупнейших в стране. Он насчитывает около 500 тыс. экз. микрофильмов и микрофиш, которые являются копиями рукописных материалов, книг, журналов, газет, нот, эстампов и других видов печатных изданий на разных языках мира. Среди них — Остромирово евангелие; адресно-справочные книги, такие, как, например, "Весь Петербург" за 1894–1940 гг., "Общий Гербовник дворянских родов Всероссийской Империи", который был начат в 1797 г.; журнал "Нива" с 1870 по 1918 гг. и многое другое. На микрофишах полно представлена литература русского авангарда начала XX в., тематические подборки различных произведений 18-19 вв., объединенные общими названиями: "Россия глазами иностранца", "Популярные русские песни и сказания", "Россия и Святая земля" и другие. В фонде микроформ также собираются микрофотокопии документов, которые отсутствуют в печатной форме или существуют только на микроносителях. На правах оригинала, отсутствующего в Основном фонде РНБ, представлены различные периодические издания на иностранных языках, например: «Journal of the Optical Society of America»; «Tempo: a quart. rev. of modern music» и т.д.

В 1998 г. Институт «Открытое Общество» специально для Российской национальной библиотеки приобрел у известного германского издательства «K.G. SAUR» полный комплект «Всемирной биографической информационной системы» (издание на микрофишах – около 25 тыс.

микрофиш). Эта система состоит из отдельных «Биографических архивов», структурированных по национальному или территориальному признакам. Каждая запись о персоналии воспроизведена шрифтом оригинального текста. Записи расположены в алфавитном порядке имен. Необычность архивов состоит в том, что они включают в себя информацию не только о повсеместно известных политиках, великих ученых и писателях, внесших значительный вклад в области своей деятельности, но и о тысячах менее заметных людей, неизвестных за пределами своих стран, но действительно двигавших вперед науку, технику, политику и культуру.

Полноценной частью Мировой биографической системы стал «Русский биографический архив». Архив состоит из 12 частей и содержит более 500 микрофиш, каждая из которых вмещает около 450 страниц текста и изображений. Биографическая информация Архива охватывает период от эпохи Рюриковичей (IX в.) до 1917г. и содержит 75 000 персоналий. При составлении Архива использовано более 150 источников, опубликованных в 1827–1995 гг. в России и за рубежом. Статьи снабжены индексами согласно классификации Библиотеки Конгресса. В 2000 году начат выпуск биографического архива Советского Союза, являющегося логическим продолжением Русского биографического архива и охватывающем период с 1917 по 1991 год. Архив объединит около 170 000 биографических записей с информацией о 80 000 персоналий из истории Советского Союза. Оба этих архива насчитывают по 500 микрофиш.

**Коллекционные собрания**

- Мировой биографический архив от начала книгопечатания по настоящее время (микрофиши) [более 25.000 микрофиш]. Собрание "Мировой биографический архив" представляет собой аналитическую роспись публикаций из мировых источников, посвященную выдающимся деятелям различных областей знаний. Это универсальный персональный биографический словарь, в котором материалы сгруппированы по национальному и территориальному признакам. Он включает оригинальные издания, существующие только на микрофишах и представленные в РНБ в единственном экземпляре.
- Составной частью Мирового биографического архива является «Русский биографический архив», в который вошли 162 издания (271 том) не только на русском и других языках бывшей Российской империи, но также на английском, французском, немецком (более 10%). Это составило свыше 160 тысяч статей, посвященных 75 тысячам персоналий за период от Крещения Руси до 1917 г.

# МЕТОДИКА ВЫБОРА ОПТИМАЛЬНОЙ СЭД – НАШ ОПЫТ

Автор: Виктор Свистунов, Начальник отдела системной поддержки, ЗАТ «Компания РАЙЗ».
Источник: http://itdirector.org.ua/Bullet_VOO/Statji/?article=913

Кризис уже понемногу отступает, по крайней мере, все к нему уже как-то привыкли и эта тема уже просто приелась. Всё равно нужно жить дальше, работать, повышать эффективность труда, в чём, по моему мнению, и заключается основная задача ИТ.

Поэтому, уважаемые коллеги, в данной статье хочу поделиться своим опытом в таком деле как **выбор системы электронного документооборота (далее, СЭД).** Эта информация может быть полезной как тем, кто уже начал присматривать для своей организации подходящую СЭД, так и тем, кто ещё совершенно не знаком с этим вопросом.

Когда мы говорим о выборе (и последующем внедрении) какого либо ИТ-решения, нам, несомненно, следует учитывать особенности организации, в которой оно будет использоваться. Такими особенностями могут быть размер организации, перспективы её роста, наличие территориально удалённых офисов, зрелость ИТ-инфраструктуры и мышления сотрудников и, в первую очередь, руководства, поддержка этого самого руководства, наличие других информационных систем, объём хранимой информации и скорость её пополнения, длительность и надёжность хранения информации, доступность финансовых ресурсов, личные цели участников проекта внедрения и прочее-прочее. Всё это хорошо бы как-то учесть в процессе выбора системы.

Кратко опишу нашу ситуацию, чтобы вы, уважаемые читатели, представляли себе контекст, в котором происходила эта работа, могли сразу делать для себя поправки, учитывая специфику вашей организации.

Компания Райз работает в аграрном секторе. Имеет широкую филиальную сеть. Общее количество сотрудников – более 5 тыс. Количество компьютеризированных рабочих мест – более 1 тыс. Ожидаемый объем прироста электронной документации – 0,7- 1 Тбайт в год.

Прежде, чем перейти к сути вопроса, разрешите, как говориться, определиться с терминами. Под СЭД довольно часто представляют себе разные понятия. Автор под категорию СЭД подводит сразу четыре типа систем, которые, нужно отметить, могут мирно уживаться в рамках одной конкретной системы, расширяя её возможности. Итак, к СЭД относятся:

1. Системы делопроизводства
2. Электронные архивы
3. Workflow-системы
4. ECM-системы

«Идеальная» СЭД в той или иной степени должна сочетать в себе возможности всех этих четырёх типов, обеспечивая реализацию полного жизненного цикла электронных документов. См. диаграмму.


Под электронным документом понимают любой объект (или группа объектов), который может быть сохранён в электронном виде.

Руководство поставило перед будущей СЭД следующие задачи:

1. Формализация и обеспечение соответствующего инструментария для последующей оптимизация бизнес-процессов организации.
2. Обеспечение эффективного управления и прозрачности деятельности организации на всех уровнях.
3. Накопление информации, управление данными и регламентирование доступа.
4. Формализация деятельности каждого сотрудника.
5. Сокращение оборота бумажных документов. Экономия ресурсов за счёт сокращения расходов на управление бумажными потоками в организации.
6. Снижение стоимости хранения бумажных документов, облегчение их поиска
7. Поддержка системы контроля качества.

Наше стремление заключается в минимизации «шовных соединений» – мест интеграции различных систем. Чем их меньше, чем лучше мы смогли для себя подобрать систему, тем лучше – тем легче её в последствии будет поддерживать. Поэтому во многих случаях, по моему мнению, здесь

оправдана покупка системы с некоторым запасом функционала, «на вырост» так сказать. Именно так и мы размышляли.

Справедливости ради, стоит добавить, что особой ясности как именно следует выбирать СЭД в Компании РАЙЗ на момент начала этой работы не было ни у кого. Определенную ясность внесла выставка DocFlow'2008. Отдельное спасибо её организаторам и участникам! Результатом её посещения стала увесистая пачка материалов о более чем 20 представленных на ней СЭД и понимание того, что на этом всё дело не закончится. Поэтому, сразу же после завершения этой выставки мы приступили к анализу рынка решений СЭД. Обнаружилось ещё порядка 20 СЭД, доступных на рынке СНГ. Итак, мы стояли перед фактом, что выбирать есть из чего!

1. 1С Архив
2. Captaris Workflow
3. CompanyMedia-Делопроизводство
4. Corporate Business
5. DeloPro 4.0
6. Directum
7. DocLogix
8. DocsVision
9. EMC Documentum
10. FossDOC
11. Globus Professional
12. IBM FileNet
13. InTeam: Диловодство
14. iTs-Office
15. LanDocs
16. Megapolis.DocNet
17. Naumen DMS
18. OpenText Hummingbird
19. OPTiMA-WorkFlow
20. PayDox
21. Platina ECM
22. АСКОД
23. БОСС-Референт
24. ДЕЛО
25. Делопроизводство
26. ДОК ПРОФ 2.0
27. ЕВФРАТ-Документооборот
28. ИНТАЛЕВ: Корпоративные документы и процессы
29. Канцлер
30. Кодекс-Документооборот
31. Летограф
32. Мотив
33. Платформа ТетраSOFT
34. Решения на платформе Microsoft Dynamics CRM
35. Решения на базе Microsoft SharePoint Server 2007
36. Решения на базе IBM Lotus/Domino

Почерпнуть много полезной информации о различных СЭД Вы также сможете из следующих источников:

- Аналитический обзор рынка систем электронного документооборота по итогам 2007 года, DCC Consulting, 2008г. (437 стр.)
- Журнал «IT-Спец» (приложение журнала «Хакер») №12, 2008г. (32 стр.)
- Журнал «Корпоративные системы» №5, 2008г. (8 стр.)
- www.DOCFLOW.ru
- www.doc-online.ru
- www.iteam/publications/it/section_64/
- www.gdm.ru

Пришло самое время определиться а что же ожидает от нас бизнес-направление нашей компании (далее Бизнес).

Параллельно с проведением первых презентаций СЭД у нас формировались критерии первичного отбора. Таких встреч у нас было 16, т.е. в течение 3 недель каждый день мы встречались с представителями компаний-внедренцев той или иной СЭД. С нашей стороны, кроме ИТ-шников, в этих встречах приняли участие директор департамента управления персоналом, начальник канцелярии, директор департамента планирования и анализа, директор департамента торговых операций. Это очень помогло максимально вовлечь в процесс авторитетных людей, к мнению которых

прислушивается высшее руководство. …Увесистая папка материалов стала ещё увесистее раза в три. Пришло время систематизировать наши первичные требования и результаты первичного анализа. Так родились список первичных критериев, позднее были определены весовые коэффициенты критичности для каждого из них. Результаты оценки были сведены в первичная сводная таблица для удобства сравнения.

Наши первичные критерии можно представить следующим образом:

**Наши Бизнес-критерии оценки СЭД:**

1. Эргономические характеристики. Интерфейс пользователя
   - Интерфейс должен быть удобным, «резиновым», кастомизируемым, разработан с учетом требований Бизнеса.
   - Украинский интерфейс.
   - Наличие встроенных механизмов проверки рус. и укр. орфографии.
2. Интеграция с офисным ПО
   - СЭД должна интегрироваться с популярными офисными приложениями: MS Office, Open Office.
3. Масштабируемость (функционал и контент)
   - В рамках СЭД должна быть возможность реализации любого функционала, в том числе по управлению бумажными документами.
   - Отсутствие ограничений на хранение информации – документов
4. Соответствие требованиям
   - Возможность описания бизнес-процессов с помощью популярных нотаций (IDEF3, ARIS, UML диаграмма активностей, интеграция этого модуля с документооборотом.
   - СЭД должна обеспечить возможность реализации всех наших пожеланий, сформулированных начальником Канцелярии.
   - Контроль исполнения поручений.
   - Использование системы напоминаний по E-mail и SMS.
   - Гибкая система поиска по документам.
   - Поддержка версионности документов, многопунктовых документов.
   - Механизмы контроля повторных вводов документов.
   - Штрих-кодирование печатных документов.
   - Наличие графических средств для оформления аналитики.
   - Есть возможность формирования Базы Знаний на основе введённых документов.
5. Стоимость необходимого ПО и его внедрения (1 тыс.пользователей)
   - Выгодное ценовое предложение, гибкая ценовая политика на лицензии и на стоимость внедрения.
   - Конкурентный тип пользовательских лицензий.

**Наши технологические критерии оценки СЭД:**

1. Платформа
   - СЭД должна работать на промышленных серверах и БД (MS SQL).

- Хранение документов вне БД - на файл-сервере, в БД хранятся только ссылки на документы.
- Возможность работы с СЭД через Интернет, а также в терминальном режиме (через Citrix).

2. Архитектура, масштабируемость
   - Архитектура СЭД должна обеспечивать необходимый уровень быстродействия.
   - Производительность СЭД должна ограничиваться только аппаратными возможностями.
3. Поддержка основных ИС
   - СЭД должна поддерживать основные ИС, почтовые сервера, сервера приложений других систем (1С, SAP и т.д.).
4. Интеграционные возможности
   - СЭД должна иметь документированный API, для дальнейшей интеграции с другими ИС, к которым у нее нет интеграционного модуля.
5. Возможность доработки
   - Разработка в СЭД должна вестись с применением промышленных языков программирования.
6. Безопасность, отказоустойчивость
   - Наличие механизмов аутентификации, интеграция с Active Directory, а также собственные механизмы аутентификации (для пользователей НЕ членов Active Directory).
   - Поддержка ЭЦП.
   - СЭД должна поддерживать системы бэкапирования, а также возможность работы в кластере, в том числе и распределенном.
   - Должен обеспечиваться аудит всех действий пользователей в СЭД.
7. Поддержка, требования к компании-внедренцу
   - Качественная работа компании-внедренца на этапе подготовки Технического Задания, хорошая репутация и уверенность в том, что и «завтра он будет работать».
   - Опыт успешных внедрений в крупных (солидных) организациях, в т.ч. в государственных.
   - Офис компании-внедренца находится в г.Киев.
   - Свой собственный продукт.
   - Наличие инструментов для дистанционного обучения пользователей.
   - Наличие дополнительных преимуществ.

Для того, чтобы обеспечить хорошему делу успешное завершение, нужно как можно раньше определить факторы, повышающие вероятность успеха, и минимизировать возможные риски. В нашем случае это:

1. Чётко обозначенная цель проекта, проектный подход
2. Реальная потребность организации в СЭД
3. Осознание этой потребности Руководством, поддержка проекта

4. Доверительные отношения ИТ с Руководством (выстраиваются раньше)

5. Готовность ИТ-инфраструктуры (2-ой уровень зрелости и выше)

6. Вовлечение в процесс выбора СЭД команды единомышленников из НЕ-ИТ-шников, их мотивация. Они помогают установить правильные отношения с остальными пользователями, несут позитивную информацию руководству.

7. Правильный выбор СЭД:

- Сама платформа СЭД («на вырост», интеграционные возможности)
- Команда внедренцев
- Методология внедрения

8. Команда внедрения со стороны заказчика (мы)

9. Реальный план внедрения (тактика быстрых побед)

На втором этапе (в финале) мы имели дело уже только с 5 СЭД. Но мы понимали, что количество и качество имеющихся критериев явно недостаточны. Поэтому возникла необходимость их уточнения. Так родилась расширенная анкета из 514 вопросов, содержание которой согласовалось с финалистами нашего конкурса.

| | Platina ECM | Terrasoft | IBM FileNet | Documentum | Directum | ИДЕАЛ |
|---|---|---|---|---|---|---|
| 1. Требования к технической и программной инфраструктуре *(57 критериев)* | 84 | 92 | 97 | 91 | 103 | 114 |
| 2. ИТ-безопасность и аудит *(46 критериев)* | 81 | 82 | 77 | 78 | 83 | 92 |
| 3. Требования к управлению деловыми процессами (WorkFlow) *(50 критериев)* | 98 | 90 | 99 | 98 | 100 | 100 |
| 4. Требования к управлению электронными документами *(58 критериев)* | 109 | 101 | 104 | 111 | 110 | 116 |
| 5. Требования к работе с бумажными документами ("Канцелярия") *(40 критериев)* | 76 | 77 | 75 | 73 | 80 | 80 |
| 6. Требования к системе отчётности по документообороту *(25 критериев)* | 50 | 48 | 50 | 34 | 50 | 50 |
| 7. Требования к пользовательскому интерфейсу *(13 критериев)* | 26 | 21 | 26 | 24 | 25 | 26 |
| 8. Требования по модификации и развитию системы силами Заказчика *(26 критериев)* | 52 | 52 | 52 | 52 | 52 | 52 |
| 9. Требования к дополнительным функциональным возможностям и модулям, реализованным на базе системы *(см.следующую таблицу)* | | | | | | |
| 10. Требования по сопровождению, поддержке и обучению *(27 критериев)* | | | | | | |
| 11. Требования к опыту Внедренца и Розработчика, гарантии качественного исполнения проекта *(25 критериев)* | | | | | | |
| 12. Ценовое предложение* *(9 критериев)* | | | | | | |
| 13. Слабые стороны и угрозы *(5 критериев)* | | | | | | |

** В ценовое предложение входит: стоимость лицензий для 1 тыс. пользователей, стоимость ежегодной поддержки, стоимость работ по выполнению тестового задания "Бизнес-процесс Наказы"*

Например, если на первом этапе нас интересовало обеспечивает ли СЭД гибкий поиск документов в БД, то расширенная анкета содержала уже 22 критерия, определяющих ожидаемую гибкость поиска. Вопросы объединены в 13 групп, группы соответствуют известным рискам внедрения СЭД. Кроме расширенной анкеты финалисты получили подробно прописанный 1 бизнес-процесс (Прохождение приказов) для определения стоимости работ по внедрению этого блока работ. Все ответы финалистов попали в финальную сводную таблицу. Её укрупнённый вариант предоставляю Вашему вниманию. По просьбе компаний-внедренцев, здесь я не указываю размер предложенных нам скидок. Хотя их размер (возможно благодаря кризису) весьма впечатляющий.

Кроме этого следует взять во внимание дополнительные возможности, обеспечиваемые СЭД, которые рассматривались нами как некий бонус.

Кроме этого следует взять во внимание дополнительные возможности, обеспечиваемые СЭД, которые рассматривались нами как некий бонус.

| | Platina ECM | Terrasoft | IBM FileNet | Documentum | Directum | ИДЕАЛ |
|---|---|---|---|---|---|---|
| 9.1. ServiceDesk (продвинутый вариант HelpDesk - набор средств, реализующих ITIL) *(11 критериев)* | 22 | 22 | 11 | 0 | 0 | 22 |
| 9.2. CRM *(44 критерия)* | 81 | 83 | 53 | 0 | 70 | 88 |
| 9.3. Управление закупками *(14 критериев)* | 28 | 25 | 14 | 13 | 25 | 28 |
| 9.4. Управления проектами *(4 критерия)* | 7 | 7 | 4 | 8 | 8 | 8 |
| 9.5. Управление совещаниями *(5 критериев)* | 9 | 10 | 5 | 5 | 10 | 10 |
| 9.6. Автоматизация маркетинга *(6 критериев)* | 9 | 12 | 6 | 3 | 10 | 12 |
| 9.7. Управление рабочим временем *(13 критериев)* | 24 | 26 | 23 | 24 | 26 | 26 |
| 9.8. Автоматизация планирования деятельности *(6 критериев)* | 7 | 11 | 12 | 2 | 12 | 12 |
| 9.9. Подсистема массового ввода документов *(12 критериев)* | 13 | 12 | 24 | 24 | 23 | 24 |
| 9.10. Управление HR *(9 критериев)* | 16 | 15 | 9 | 0 | 12 | 18 |
| 9.11.«Мини-ERP» *(7 критериев)* | 9 | 12 | 0 | 0 | 0 | 14 |
| 9.12. Поддержка системы менеджмента качества согласно ISO 9000, OHSAS 18001 | 2 | 1 | 0 | 1 | 2 | 2 |
| 9.13. Встроенный клиент обмена мгновенными сообщениями | 0 | 1 | 0 | 2 | 0 | 2 |

Таким образом высшему руководству была представлена пятёрка финалистов (в порядке убывания привлекательности) с аналитическими материалами, на основании которых производилась оценка.

1. Platina ECM (Швеция), SIGMA в Украине, www.team.eclipse-sp.ua
2. Directum (Россия), LAN Service, www.directum.com.ua
3. Платформа Terrasoft (Украина), Terrasoft, www.terrasoft.ua
4. Documentum (США), EMC, www.documentum.ru
5. IBM FileNet (США), IBM, www-01.ibm.com/software/data/content-management/

И, напоследок, разрешите обратить Ваше внимание на те моменты, которые могут Вам помешать успешно завершить проект внедрения СЭД:

1. Отсутствие поддержки руководства.
2. Некачественный проектный менеджмент.
3. Спешка.
4. Неправильная оценка реальных потребностей организации.
5. Подпольное внедрение.
6. «Конкурс откатов».
7. Переход к Качественному этапу при незавершённом Количественном этапе.
8. Количество вариантов решений более 5 на Качественном этапе.
9. Недостаток финансовых ресурсов.

**Заключение**

Как заметил внимательный читатель, мы постоянно учились в процессе этой работы. Из состояния практически нулевого уровня знаний в области СЭД мы постепенно доросли до уровня четкого осознания того, что именно нам нужно. Вам же не обязательно идти этим длинным путём, достаточно взять на вооружение наш опыт и внести необходимые коррективы согласно специфики Вашей организации.

Если Вам потребуется дополнительная информация, буду рад ответить на Ваши вопросы.

# ДОКУМЕНТООБОРОТ И BYOD: КАК МОБИЛЬНАЯ ВЕРСИЯ СЭД ПОМОГАЕТ ИДТИ В НОГУ СО ВРЕМЕНЕМ

**Источник:** https://www.tezis-doc.ru/blog/dokumentooborot-i-byod-kak-mobilnaya-versiya-sed-pomogaet-idti-v-nogu-so-vremenem/

Не секрет, что мы живем в эпоху «всеобщей мобилизации». Переносному компьютеру — ноутбуку — в следующем году уже исполнится

тридцать пять, а мобильный телефон превратился из увесистого «кирпича» в карманный мини-компьютер всего за какое-то десятилетие. Пришла и схлынула волна PDA, за ней ушли в прошлое когда-то популярные нетбуки, очень быстро были вытесненные с рынка планшетами. А заодно выросло поколение молодых специалистов, которое социологи иронично прозвали «поколением большого пальца» («thumb generation» или «i-finger generation») – за неистребимую привычку не расставаться со смартфоном, набирая бесконечные сообщения, листая страницы в Интернете или играя в видеоигры.

Для молодежной части коллектива довольно размытым является понятие рабочего места. Благодаря мобильным устройствам «поколение большого пальца» имеет доступ к информации практически везде и всегда, и привычная концепция организации трудового процесса, когда у каждого сотрудника есть стол, стул, и компьютер, за которым он сидит, как приклеенный, современному молодому сотруднику неудобна. Молодые специалисты убегают работать «по удаленке» с домашнего ноутбука, набирают отчеты на личных планшетах, гуляя по офису, и общаются с начальником по Viber, сидя со смартфоном в кафе. Проще говоря, вместе с новым поколением работников в современный офис ворвалась концепция BYOD (Bring Your Own Device) – организация рабочего процесса с использованием личных мобильных устройств сотрудников.

Это стремление встать из-за рабочего стола доставляет немало хлопот в такой консервативной сфере, как документооборот. Документы «разлетаются» по личным устройствам сотрудников, как осенние листья, гонимые ветром. Эта ситуация, бесспорно, требует наличия в компании системы электронного документооборота, которая будет консолидировать документы в едином хранилище. Однако, и этого не вполне достаточно. СЭД в классическом формате рассчитаны именно на концепцию индивидуального рабочего места сотрудника со стационарным компьютером и чересчур тяжеловесны для мобильных устройств.

Решением проблемы могло бы стать создание мобильных приложений для документооборота. Именно поэтому СЭД ТЕЗИС имеет мобильный интерфейс, который развивается параллельно с основной системой. Он дает возможность идти в ногу с современной тенденцией к мобильности и в то же время сохранять организационные преимущества электронного документооборота.

**Мобильный документооборот — это удобно**

Из мобильных устройств в настоящее время наиболее популярны смартфон, планшет и ноутбук. И если последний достаточно консервативен в плане конструкции (что обуславливается необходимостью сохранять приемлемый вес), то смартфоны и планшеты находятся в вечной гонке за красотой дизайна, толщиной корпуса, размерами экрана, дюймами и пикселями. Линейка размеров экранов смартфона варьируется от трех дюймов, что соответствует разрешению 640×490, до 5,2-5,5 дюймов, что в разных моделях соответствует разрешению от 1280×720 до 1920×1080. А

между этими крайними значениями существует огромный разброс разрешений, который появился по прихоти дизайнеров мобильных устройств. Особенно выделяются в этом плане популярные устройства с «яблоком», которые «радуют» разработчиков веб-приложений оригинальными разрешениями типа 1334×750. Впрочем, и ноутбуки тоже не подарок – диагональ экрана колеблется от 10 до 18 дюймов для крупных ноутбуков, и от 7 до 11 дюймов – для нетбуков, которые у многих еще в ходу (не каждый готов оторвать от сердца, к примеру, 11-дюймовый MacBookAir).

Отдельным вопросом являются возможности мобильных устройств по отображению графики. Хотя смартфоны и планшеты (не без давления со стороны игровой индустрии) постоянно совершенствуются в этом плане, до мощностей видеокарт современных стационарных ПК графические процессоры мобильных устройств пока не дотягивают – даже топовые, выдающие частоты до 533 МГц. Вместе с мощностью графики сильно растет энергопотребление мобильного устройства, что снижает время его автономной работы, а прорыва в области производительности аккумуляторов пока не предвидится.

Таким образом, если в организации сосуществуют BYOD и СЭД, может обнаружиться, что веб-интерфейс системы, который так красиво смотрится на мониторе стационарного ПК, окажется неподъемным кошмаром на мобильном устройстве. Интерфейс, рассчитанный на ПК, подвержен тем же проблемам, которые возникают с любым веб-приложением или сайтом в мобильном браузере: элементы UI могут хаотично «поплыть»; интерфейс может оказаться слишком велик для мобильного экрана, и пользователю постоянно придется двигать область просмотра, чтобы отыскать нужные элементы; или UI просто не сможет обеспечить достаточное время отклика на маломощном мобильном устройстве, и все действия будут выполняться крайне медленно.

Именно поэтому наиболее приемлемым вариантом является использование специализированного мобильного интерфейса СЭД на таких устройствах, как планшеты и смартфоны. Мобильная версия СЭД ТЕЗИС, по сути, является легковесным адаптивным мобильным интерфейсом для доступа к данным в СЭД. Мобильная версия ТЕЗИС адаптирует свой интерфейс к любым размерам и разрешениям экрана мобильного устройства, позволяя эффективно использовать его ограниченное пространство. Кроме того, она учитывает ориентацию экрана – горизонтальную или вертикальную, и подстраивается под ее изменения. Помимо этого, все элементы интерфейса Мобильной версии адаптированы под управление методом touch-screen, который является основным способом взаимодействия с современными сенсорными моделями смартфонов и планшетов (именно он и породил выражение про «большой палец»).

Таким образом, использование мобильной версии СЭД является удобным в условиях широкого разнообразия мобильных устройств, применяемых сотрудниками в личных и рабочих целях. Мобильная версия ТЕЗИС учитывает аппаратные особенности каждого устройства, будь то

нетбук, смартфон или планшет, а также поддерживает все современные веб-браузеры для Android и iOS.

**Мобильный документооборот – это просто**

Современные СЭД предлагают массу функций. Помимо управления классическим документооборотом, контроля исполнительской дисциплины и ведения канцелярии, в СЭД могут быть реализованы как различные рабочие процессы (к примеру, организация совещаний), так и технические возможности (к примеру, потоковое сканирование и ввод документов, генерация отчетов, использование ЭП и так далее). Богатое функциональное наполнение современных СЭД является несомненным преимуществом, однако делает их чересчур громоздкими для использования на мобильных устройствах.

В случае мобильного интерфейса СЭД на передний план выходит не обширность функциональных возможностей системы, а простота и оперативность работы в ней. Часть функций, которые доступны в «десктопной» СЭД, на мобильном устройстве просто не имеют смысла — к примеру, потоковый ввод документов (вряд ли кому-то придет в голову подключать смартфон к сканеру). Другая часть оказывается нерабочей чисто технически — так, перспективы использования мобильной ЭП до сих пор остаются достаточно туманными. Кроме того, слишком большой набор функций сильно усложняет юзабилити мобильного приложения для документооборота. Поэтому разумным решением для удобства использования СЭД на мобильном устройстве является ограничение функциональности.

Мобильный интерфейс СЭД ТЕЗИС ограничен по функциональности таким образом, чтобы пользователь видел только те части бизнес-процессов, которые требуют его оперативного участия. Это, в первую очередь, поступающие к нему задачи, договоры и документы, присланные на ознакомление, согласование, утверждение, либо регистрацию. Также мобильный интерфейс позволяет получать уведомления о действиях по процессам, выполненным другими участниками. Таким образом, мобильная версия не содержит ничего лишнего, а просто позволяет быстро получать доступ к информации, по которой нужно произвести действия как можно быстрее.

Конечно, из-за ограничений функциональности СЭД на смартфоне или планшет можно использовать только как средство оперативного решения срочных вопросов. Однако, даже такой лимитированный доступ к системе документооборота будет полезен в условиях повсеместного BYOD. Сотрудник сможет участвовать в бизнес-процессах и реагировать на задачи как на рабочем месте, так и вне его. Для выполнения важнейших действий, на которые рассчитана СЭД, вполне достаточно экрана смартфона или планшета — например, чтобы поставить задачу или прочитать и согласовать документ. Мобильная версия СЭД позволит быстро решить производственный вопрос даже в отрыве от стационарного ПК или вне офиса, используя персональное мобильное устройство.

**Мобильный документооборот — это недорого**

Как показывает наш опыт, ранее существовала тенденция приобретать мобильные версии СЭД в основном для руководителей. Бесспорно, руководство компании в большинстве случаев более мобильно, чем рядовые сотрудники, и гораздо более нуждается в оперативном доступе к данным и документам. Кроме того, многие компании-заказчики не решались на массовое приобретение мобильных лицензий из соображений того, что это увеличит бюджет проекта внедрения СЭД. Поэтому мобильная версия СЭД приобреталась в небольших объемах для использования той частью коллектива, которая непосредственно участвует в принятии решений в ежедневной деятельности бизнеса.

Однако, распространение концепции BYOD в современных офисах привело к появлению прямо противоположной тенденции — к обеспечению оперативного выхода к электронным документам для всех сотрудников, которым это необходимо, без учета их положения в иерархии компании. Ведь подчиненные также стали мобильны, и точно так же нуждаются в оперативном получении задач от начальства, обмене документами с другими подразделениями, постоянном доступе к данным, связанным с работами определенных проектов. Таким образом, компания, внедряющая СЭД, оказывается перед выбором между экономией и удобством работы сотрудников, которые непосредственно выполняют работы по производству продуктов и услуг.

Решение данной проблемы возможно путем использования скидочных программ, предлагаемых компаниями-вендорами СЭД. Так, лицензии на мобильную версию СЭД ТЕЗИС продаются пакетами по 5, 10, 15 или 25 одновременных подключений. Общая стоимость пакета, соответственно, равняется цене, умноженной на количество подключений в пакете, причем чем больше лицензий в пакете, тем ниже цена за одно подключение. Такая схема лицензирования удобна как раз для того упомянутого случая, в котором лицензии приобретаются для ограниченной группы привилегированных сотрудников. Однако, с учетом растущего тренда BYOD, на мобильную версию СЭД ТЕЗИС была введена вторая схема лицензирования, специально рассчитанная на компании, которые хотели бы предоставить мобильный доступ к СЭД всем рядовым сотрудникам.

Если заказчик заинтересован, чтобы все сотрудники, которым это необходимо, могли оперативно использовать СЭД, он может приобрести для них лицензии на стандартную версию СЭД, предназначенную для использования на стационарных рабочих местах, а после этого — приобрести мобильные лицензии всего за 25% от общей стоимости приобретенных лицензий на «основную» версию системы. Во сколько обойдется «мобилизация» доступа к СЭД, таким образом, легко рассчитать при помощи калькулятора внедрения. Для примера: можно приобрести 10 лицензий на Стандартную редакцию системы за 100 тысяч рублей и отдельно – пакет мобильных лицензий на 10 подключений за 47,5 тысяч рублей. Воспользовавшись скидочной программой, можно приобрести 10 лицензий

на Стандартную редакцию системы за 100 тысяч рублей, и 10 мобильных лицензий уже за 25 тысяч рублей. Экономия в этом случае выражается десятками тысяч. Таким образом, массовой закупки мобильных лицензий не следует опасаться — всегда есть возможность обеспечить удобство работы своим сотрудникам и при этом сделать это выгодно.

**В заключение: мобильный документооборот — это необходимо**

Растущее распространение мобильных устройств, популяризация концепции BYOD, выход на рынок труда молодых сотрудников, привыкших к мобильным гаджетам, необходимость оперативного доступа к информации в СЭД с любого устройства и из любой точки мира, где есть Интернет – все это обуславливает необходимость наличия мобильных версий системы электронного документооборота в ИТ-инфраструктуре компании.

Мобильная версия СЭД ТЕЗИС дает компаниям такую возможность, предоставляя легковесный, не перегруженный лишними функциями мобильный интерфейс к СЭД ТЕЗИС, адаптирующийся к аппаратным возможностям мобильных устройств, таких как ноутбуки, смартфоны и планшеты. На мобильную версию ТЕЗИС действует выгодная скидочная программа, позволяющая приобретать лицензии массово и обеспечивать мобильным доступом к СЭД необходимое количество сотрудников.

Кроме того, в долгосрочной перспективе в дополнение к мобильному интерфейсу СЭД ТЕЗИС планируется выпустить нативные приложения для основных мобильных операционных систем, чтобы расширить возможности взаимодействия между СЭД и мобильным устройством. Таким образом, от работы с СЭД в отрыве от рабочего места продукт готовится перейти к полноценной автоматизации мобильных сотрудников.

# КИБЕРБЕЗОПАСНОСТЬ В УКРАИНЕ. ДИСКУССИЯ

Источник: http://ko.com.ua/kiberbezopasnost_v_ukraine_diskussiya_121089

Раскаты грома, вызванного недавней широкомасштабной атакой вируса-вымогателя из семейства Petya, до сих пор не утихли. Под их аккомпанемент Институт Горшенина организовал круглый стол, темой обсуждения которого был вопрос, как обезопасить украинское киберпространство? В круглом столе участвовали представители Национальной полиции Украины, СНБО и ИТ-бизнеса.

Дискуссию открыла директор по связям Института Горшенина Наталья Клаунинг, предложив Вячеславу Марцинкевичу, старшему инспектору по особым поручениям департамента киберполиции НПУ, описать последствия массового поражения компьютерных систем в Украине вирусом Petya. По его

словам, урон был нанесен колоссальный – от вируса пострадало очень много госпредприятий и компаний из частного сектора. Были выведены из строя как серверы, так и пользовательские компьютеры, работающие под управлением ОС Windows. Была парализована работа многих предприятий и организаций. До сих пор (на 20.07) многие компании не преодолели последствия этой атаки. Даже если они и начали работу в обычном режиме, то потребуется длительное время и огромные усилия по восстановлению потерянной информации и документов. Как отметил в заключение В. Марцинкевич, ситуацию осложняет недостаток специалистов в области кибербезопасности, особенно на госпредприятиях.

Вопрос о том, существует ли вообще какая-нибудь система кибербезопасности в Украине, был адресован государственному эксперту Службы по вопросам информационной безопасности аппарата СНБО Украины Надежде Литвинчук. По ее словам, этот вопрос является базовым для решения заданий кибербезопасности в государстве в целом. За все годы независимости, к этому вопросу, являющемуся таким критически важным, не было системного подхода. Конечно, была нормативная база, создавалась система защиты, но ключевые документы, на основе которых можно было выстраивать систему кибербезопасности, отсутствовали. Даже в законе про основы национальной безопасности были всего лишь очерчены угрозы в информационной сфере. Только в последнее время после известных событий состоялась цепочка рассмотрений СНБО вопросов, связанных с информационной безопасностью и кибербезопасностью. Известно, что в январе прошлого года СНБО наконец была одобрена стратегия кибербезопасности Украины, и Президент в 2016 г. своим Указом № 96 утвердил эту стратегию. Это дало толчок для решения других задач, поскольку сама стратегия определила цепочку направлений, по которым нужно в дальнейшем выстраивать национальную систему кибербезопасности.

Что же собой представляет национальная система кибербезопасности? Прежде всего, это субъекты, которые определены стратегией и входят в эту систему, в частности, Министерство обороны, Государственная служба специальной связи и защиты информации (ГСССЗИ), СБУ, органы разведки, НПУ, то есть органы, которые относятся к сектору безопасности и обороны, и которые будут обеспечивать кибербезопасность в государстве. Координатором во всей этой системе выступает, в соответствие со стратегией, СНБО. Однако СНБО является коллегиальным органом, а для того, чтобы функционировать в постоянном режиме и оперативно реагировать на инциденты, был создан Национальный координационный центр кибербезопасности. Его возглавляет секретарь СНБО. В Центре постоянно проводятся заседания и принимаются решения, которые координируют и становятся основой для решений СНБО и для деятельности всех органов государственной власти.

Для примера, первым шагом, который сделал Центр, - это определение заданий для формирования законодательной базы. Что здесь имеется в виду?

У государства есть информационные ресурсы, есть критическая инфраструктура. Однако если для государственных информационных ресурсов легче выстраивать систему кибербезопасности на основе действующей законодательной базы, то много объектов критической инфраструктуры, таких как ТЭС, входящие в систему жизнеобеспечения, находятся в частной собственности. Защитить вычислительные ресурсы таких объектов на сегодняшний день является большой проблемой. Поэтому сейчас создается перечень таких объектов и в законодательство введены предложения относительно перечисления объектов критической инфраструктуры. Четкий перечень телекоммуникационных систем этих объектов позволит «Госспецсвязи» Украины решать задачи относительно безопасности этих систем.

За годы независимости в системе НАН Украины работали 16 научных учреждений, которые занимались ИТ. Они насчитывали более 2 тыс. сотрудников. Это весьма существенный потенциал. Однако проблема в том, что эти учреждения использовали для построения своих ИС разные технологические решения, и объединение всех созданных баз данных и реестров является трудной задачей. Но сегодня уже существует решение СНБО, утвержденное президентским Указом 32, которое предусматривает создание единого ЦОД для обработки данных государственных информационных ресурсов. В целом же необходимо создавать мощную кибероборону, поскольку на Варшавской встрече G7 киберпространстов было признано пятым театром военных действий.

По мнению Александра Кардакова, главы наблюдательного совета компании «Октава Капитал», задачу построения киберзащиты нужно разделить, по крайней мере, на несколько частей. Есть государственные информационные ресурсы, которыми занимаются отдельные специальные государственные организации – это один полюс. Вторым являются частные системы. Их данные являются объектом атаки частных злоумышленников. Целенаправленных атак на такие объекты никто осуществлять не будет. Посередине остался большой пласт коммерческих предприятий с разной формой собственности.

Отрадным является факт, что СНБО начал серьезно относиться к безопасности объектов критической инфраструктуры. Так что эта проблема начала решаться. В то же время сегмент коммерческих предприятий составляют основу экономики Украины. И последняя атака была осуществлена именно на этот экономический потенциал Украины – коммерческие предприятия, которыми никто специально в государстве не занимался. Однако кто-то же должен это делать. Поскольку у государства и так есть чем заниматься, то должно быть сформировано некое сообщество, которое выступающий предложил назвать «Гражданская кибероборона». Оно должно заниматься созданием штабов, подготовкой соответствующего персонала компаний, выявлением угроз и т. п. По инициативе бизнеса должны быть созданы центры обмена информацией, которые будут сотрудничать друг с другом и со всеми государственными органами, чтобы

выработать метрики угроз, методологию защиты и т. п. вплоть до инструкций, что делать в случае взлома. Для тех компаний, у которых нет ИТ-отделов или соответствующих специалистов, нужно создать «горячий резерв», специалисты которого могли бы быть временно наняты для восстановления ИТ-систем.

Комментируя выступление А. Кардакова, Надежда Литвинчук отметила, что предложение очень интересное, и что государство для реализации этой инициативы должно создать необходимые условия. Однако, по мнению Вячеслава Марценкевича, никакие заседания, указы, «кибероборона» не дадут должного эффекта для предотвращения следующей массовой атаки, поскольку самыми слабыми местами в сети организаций являются их системные администраторы. Пока они не построят и правильно не сконфигурируют систему безопасности, никакие CERT или закупка дорогостоящего оборудования не помогут. Вирус Petya атаковал компьютеры изнутри организаций, и те, у кого была правильно сделана сегментация сети, установлены соответствующие политики доступа, пострадали в наименьшей степени.

Основатель компании RMRF Technology, разработчика средств киберзащиты, Андрей Пастушенко остановился на характеристиках современного кибероружия. По его словам, современное кибероружие можно сравнить со средствами массового поражения, но по отношению к компьютерам. Оно может одновременно вывести из строя множество объектов критической инфраструктуры как на уровне одного государства, так и на уровне объединения нескольких государств. Киберпространство - это среда взаимодействия разнообразных нестандартизованных уязвимых информационных систем, в которых используются чувствительные к взлому данные и коммуникационные возможности. Именно из этого и нужно исходить. Кибероружие нацеливается как на отдельные сегменты экономики и локальные компании, так и на отдельных граждан. Кибератаки очень тщательно подготавливаются. В 2011 г. исследователи киберугроз, выходцы из спецслужб США, разработали методологию kill chain, которая первоначально использовалась в военной концепции, относящейся к структуре атаки. Она содержит ряд последовательных действий, или цепочку фаз, нарушение любой из которой может прервать весь процесс. Большинство кибератак включают ряд этих фаз. Современные атаки подготавливаются таким образом, чтобы они не могли быть обнаружены и идентифицированы, а их действие было максимально длительным для достижения поставленных целей.

Какие выводы можно сделать из имеющегося опыта? По мнению выступающего, любые организационные действия, которые принимаются, сразу же устаревают. Это современная проблема защиты. Как только принимается какой-нибудь стандарт или метод противодействия, они сразу же становятся мишенью. И единственным эффективным противодействием является понимание этого на всех уровнях общества и государства. Поэтому должны создаваться центры любого формата, которые отслеживали бы

угрозы не только в стране, но и глобально, и оценивали их возможные последствия. Бизнес должен относиться к кибербезопасности, как к одному из направлений своей основной деятельности.

Необходимо повышать уровень информированности о кибербезопасности граждан в масштабе страны. Они должны понимать, что публикуют свои персональные данные в незащищенных сетях, и принимать необходимые меры безопасности. Нужно приучить бизнес резервировать критические данные, повышать уровень знаний о кибербезопасности своих сотрудников.

Однако есть мировой опыт, и он в той или иной мере может быть использован и в Украине. На этом вопросе остановился R&D-директор компании IT.Integrator Владимир Кург. Он подверг сомнению тезис о том, что атаки постоянно изменяются, и соответственно единого рецепта нет. Это так и не так, по мнению В. Курга. Если, к примеру, взять вирус Petya, то можно вспомнить 2012 г. и кибератаку на саудовскую нефтяную компанию Saudi Aramco. Как и в Украине, она стартовала перед выходными. Ее последствия были примерно такими же, как и у нас. По оценкам, за сутки были уничтожены данные на 30—35 тыс. компьютеров по всему Ближнему Востоку. Эта атака детально описана и приведены процедуры, как ее предотвращать и как ликвидировать последствия. Эти рекомендации были опубликованы CERT в том же 2012 г. В чем проблема Украины? В компаниях не отстроены процессы обеспечения кибербезопасности. Компании и, пожалуй, госорганы не задумывались о действиях в кризисных ситуациях, когда одной из причин является кибератака. Если говорить о мировых практиках, то они рекомендуют включать команду по кибербезопасности в общую команду кризисного реагирования предприятий.

Что выясняется при подобных кибератаках, - отсутствие отдельных департаментов кибербезопасности. Обычно этим занимаются ИТ-отделы. Но, как правило, у них нет кризисных регламентов, они не знают, как действовать в таких ситуациях. А там, где есть навыки быстрого реагирования, зачастую нет полномочий.

Что требуется? Первое, это система CERT, как это сделано в Европе. При этом необходимы специализированные CERT. К примеру, в США есть общий CERT, который занимается общей кибербезопасностью, есть ICS (Industrial Control System) CERT, который занимается объектами критической инфраструктуры, есть NERC, некоммерческая организация, занимающаяся вопросами безопасности в энергетике. Следующее, необходимо наладить обмен информацией. Компании, в основном, зациклены на отражении атак и ликвидации их последствий. В Европе и в США есть организации, которые выпускают документы по предотвращению атак, содержащие готовые рецепты.

Комментируя предложение о создании системы CERT, Надежда Литвинчук отметила, что в мире функционирует примерно 300 таких центров. В Украине также есть команда CERT-UA, которая работает под эгидой ГСССЗИ. После атаки на финансовый сектор в январе прошлого года

была поставлена задача о формировании и утверждения протокола совместных действий во время киберинцидента. Имеется в виду подведение нормативной базы, наделение полномочиями субъектов обеспечения кибербезопасности, чтобы они имели возможность быстро реагировать и взаимодействовать для противодействия атакам. Такой протокол сейчас находится на утверждении Кабинета Министров.

# КАК ЗАЩИТИТЬСЯ ОТ ВИРУСОВ-ШИФРОВАЛЬЩИКОВ?

Источник: http://ko.com.ua/kak_zashhititsya_ot_virusov-shifrovalshhikov_120953

Недавняя атака компьютерного вируса Petya.A имела серьезные последствия для ряда украинских предприятий и организаций. Фактически бизнес многих из них оказался парализован на довольно длительный срок. Между тем, разрушительных последствий можно было избежать при серьезном подходе к вопросам информационной безопасности.

**Мирослав Бондарь, руководитель департамента решений информационной безопасности группы компаний БАКОТЕК**

Интерес к системам безопасности за последние годы, безусловно, повысился. Если раньше более-менее системный подход наблюдался только в финансовом секторе и телекоме, то сейчас перечень сфер деятельности заказчиков расширился. Например, мы видим повышенный интерес со стороны промышленников, а также в госсекторе. Соответственно, растет и число компаний, которые задумываются о внедрении полноценных систем информационной безопасности (ИБ).

Спрос на услуги консалтинга в этой сфере также повышается. Хотя и не так быстро, как следовало бы. Компании начинают понимать, что любой серьезный проект в области ИБ должен стартовать как раз с комплексного аудита ИТ-безопасности, что важно правильно оценить существующие риски, и что консалтинг нужен не только на этапе выбора решения, но и во время внедрения и эксплуатации системы.

К сожалению, подход к ИБ у многих отечественных компаний осуществляется по принципу «пока гром не грянет». Его раскатами стали атаки на несколько облэнерго с использованием трояна BlackEnergy, на ЦИК и ряд госструктур, на Министерство финансов, на Госказначейство, распространение вымогателя WannaCry. Настоящая же стихия разбушевалась, когда началась массовая атака с использованием зловреда Petya, направленная сразу на множество предприятий и организаций

Украины. Только подобные события приносят руководству многих компаний и госструктур понимание того, что кибератаки – это не мнимая угроза и не страшилка из фильмов, а нечто вполне реальное, от чего надо защищаться.

Способа сделать так, чтобы подобных атак не было, не существует. Как и невозможно на 100% гарантировать защиту от них. А вот минимизировать риски посредством комплексного подхода к построению системы ИБ реально. Она состоит из трех ключевых компонентов – это внедрение технологий, обучение персонала и правильная организация процессов. Естественно, грамотно выстроенная система ИБ и ее поддержка стоит денег. Но эти расходы целесообразны, ведь пренебрегая ими можно потерять намного больше, вплоть до полного уничтожения бизнеса.

Множество заказчиков, с которыми мы работаем, избежали заражения вирусом Petya. Это клиенты из финансового и госсектора, и многие другие. Их уберегло соблюдение элементарных правил ИТ-гигиены, таких как сегментирование сетей, закрытие неиспользуемых портов, отсутствие привилегированных прав у пользователей, а также грамотная настройка решений безопасности. Расходы на защиту зависят от масштабов компании, имеющейся инфраструктуры и конкретных целей. В нашем портфеле есть решения для предприятий с разными бюджетами, начиная от малого бизнеса и заканчивая корпорациями.

**Владимир Илибман, специалист по информационной безопасности компании Cisco**

Последние несколько лет, даже в условиях кризиса, украинский рынок ИБ продолжал расти и становится более зрелым. Традиционно ИБ находится в фокусе банков, государственных структур и крупных промышленных компаний. Все эти организации обычно имеют выделенных специалистов по ИБ и достаточно планомерно развивали это направление. Последние атаки, которые мы наблюдали в Украине, коснулись компаний разных отраслей и размеров, заставив задуматься о пересмотре подхода к ИБ от ситуативного к более комплексному.

Доля услуг в области ИБ растет, включая консалтинг, аутсорсинг мониторинга и обслуживания систем. Спектр вопросов по ИБ, который возникает перед организациями, бывает настолько сложным, что самостоятельно разобраться и выбрать направления развития безопасности практически невозможно.

Основной тенденцией является наличие реальных киберугроз и большего количества атак, с которыми сталкиваются организации в Украине. Среди инцидентов последнего года можно отметить целевые атаки на объекты критической инфраструктуры (включая финансовые, энергетические и транспортные компании), Mirai (DDoS-атаку, связанную с Интернетом вещей), WannaCry и червя-вайпера Neytya/Petya.A (которого иногда путают с обычным шифровальщиком Petya). Атака Neytya стала поистине уникальной для Украины и всего мира, совместив WannaCry и шифровальщика с технологиями распространения через доверенного поставщика (Supply Chain). Neytya поставил антирекорд по масштабам и скорости, уничтожив за

несколько часов данные на сотнях тысячах компьютеров. Большая часть пострадавших устройств находилась в Украине.

Защита от комплексных целевых атак, к которой относится Petya.A, требует адекватного подхода на уровне защиты операционных систем, сегментации сети и выстраивания четких процедур мониторинга безопасности, реагирования на инциденты и резервного копирования. Он подразумевает объединение, как технических решений, так и правильно выстроенных процессов. С точки зрения новых технологий, перспективны решения, которые ориентируются на анализ поведения компьютеров и серверов. Потому что обычные антивирусы реагировали на Petya.A с опозданием в несколько часов (фактически после окончания активной фазы заражения). Новые системы анализа поведения используют облачный интеллект для более быстрого реагирования, время которого измеряется уже в минутах. Такой подход делает решения нового поколения сравнимыми с традиционными антивирусами (или даже дешевле) в части расходов на внедрение и поддержку.

Исходя из результатов общениям с десятками организаций, которые столкнулись с атакой Neytya, можно сделать выводы, что структуры с правильно построенной архитектурой безопасности избежали заражения либо ограничились временной потерей небольшого процента ПК, на которых находилось уязвимое бухгалтерское ПО. При этом комплексный подход не всегда требовал существенных затрат – обновление операционных систем, правильная настройка прав доступа и безопасная конфигурация существующей сети уже были способны значительно снизить ущерб от атаки.

**Мирослав Мищенко, менеджер по работе с ключевыми клиентами в Украине и Беларуси компании Fortinet**

Рынок информационной безопасности в Украине растет несколько последних лет. Все больше заказчиков в своих планах определяют ИБ как одно их приоритетных направлений развития.

Исторически наиболее «дисциплинированным» в этом смысле был финансовый сектор, где Национальный банк Украины проводит политику рекомендаций, в том числе и в области ИБ. Важно отметить, что подобный подход постепенно находит применение и в государственном секторе. Для коммерческих компаний политика определяется приоритетами бизнеса. И предприятий, которые не уделяют этой проблеме должного внимания, все еще очень много.

К сожалению, для рынка ИБ характерен подход – пока гром не грянет, мужик не перекрестится. ИБ направлена на снижение потерь и зачастую владельцы бизнеса не видят прямой выгоды и причин зачем им это нужно. Но такой подход актуален до первого инцидента. После этого приходит понимание важности и необходимости.

Из наиболее нашумевших эпидемий я бы акцентировал внимание на WannaCry и Petya. Причем WannaCry, несмотря на то, что была глобальной, затронула и Украину. Это был первый звоночек, что подобные эпидемии

ближе к нам, чем многим заказчикам кажется. После WannaCry было время, чтобы сделать выводы, пересмотреть и актуализировать имеющиеся политики безопасности. А потом пришел Petya и последствия нам всем известны.

Рекомендации как строить информационные системы и обеспечивать их защиту существуют давно. И это не является тайной за семью замками. Проблема состоит в том, что этап проектирования многие заказчики проигнорировали. И причин здесь может быть масса – от отсутствия необходимого бюджета до временных ограничений по его освоению, когда сразу переходят к спецификациям оборудования для закупки и проектную документацию не разрабатывают. Да, риск, что вас взломают злоумышленники, все равно остается, но потери будут минимальными. И если говорить о том, соизмеримы ли расходы на внедрение и поддержку с потенциальными потерями – прежде чем что-то внедрять, необходимо разработать несколько сценариев и сделать просчет потенциальных потерь. Если они значительно выше, чем стоимость решения, то ответ очевиден.

Думаю те заказчики, кому удалось избежать заражения Petya, с радостью сами расскажут об этом. Если же говорить о необходимом бюджете, то он будет зависеть от каждого конкретного заказчика и задач, которые нужно решить. Совместно с нашими партнерами мы практикуем индивидуальный подход и, исходя из этого, формируется бюджет проекта.

**Александр Савушкин, директор по развитию бизнеса компании Check Point Software Technologies в странах СНГ**

Компании в Украине уделяют кибербезопасности больше внимания, но, к сожалению, по-прежнему недостаточно. Это стало особенно очевидно вследствие последней вредоносной кампании, связанной с шифровальщиком Petya. Она показала, что многие организации слабо защищены и до сих пор практикуют реактивный подход.

Сейчас интерес к ИБ, безусловно, очень высокий. У нас появилось немало потенциальных заказчиков. Важно отметить, что активность Petya в Украине дала значительный эффект и в других странах СНГ – некоторые организации даже переписывают тендеры, добавляя в них решения для предотвращения угроз. Конечно, не совсем правильно, что это произошло уже после масштабной вредоносной кампании. Между тем, не может не радовать, что в подходе к кибербезопасности в нашем регионе наконец-то начал происходить прогрессивный сдвиг.

Мы получаем запросы от самых разных структур, включая компании среднего бизнеса. Традиционно решениям Check Point отдают предпочтение корпоративные заказчики, однако сегодня безопасностью озаботились многие организации из всех секторов экономики.

Характерно, что именно в текущем году повысился интерес к консалтингу. У нас есть уже несколько таких заказчиков в Украине. Хотя еще год назад спроса не было совершенно. Мы рассчитываем провести ряд проектов, получить положительные рекомендации и расширить базу действующих и потенциальных заказчиков по этому направлению.

Из заметных событий последних лет без сомнений можно выделить три: Black energy, WannaCry и Petya. Вероятно, их разрушительность очевидна для всех. При этом если WannaCry так или иначе прошелся по всему миру, то Petya был направлен именно на украинские организации. Check Point уже много лет рассказывает о важности защиты от целевых атак, уязвимостей «нулевого дня», о решениях для предотвращения угроз. Сегодня становится ясно, что это не пустые слова, а необходимость для организаций во всем мире. С каждым годом атаки будут только усложняться, поэтому нужно готовиться к худшему. Важно, что украинские предприятия начали понимать это.

Подходы для защиты бизнеса от атак, конечно же, существуют. Как я уже говорил ранее, мы активно предлагаем нашим заказчикам решения для защиты от шифровальщиков, от угроз «нулевого дня» и т.д. И можно с уверенностью заявлять, что они полностью стоят своих денег. Поскольку простой бизнеса, вызванный заражением, обходится гораздо дороже. В частности, в Украине многие организации вынуждены были прервать работу после атаки Petya. Сегодня они думают о том, как предотвратить такие ситуации в дальнейшем и считают покупку систем безопасности оправданной инвестицией.

Решения Check Point обеспечивают надежную защиту от зловредов, подобных Petya, как и от многих других. К сожалению, мы не можем раскрывать информацию по конкретным заказчикам. Однако можно отметить, что реально подобрать оптимальные решения под самый разный бюджет и потребности. Главное для организации – перестать полагаться на одни лишь антивирусы и вовремя обратиться к профессионалам.

# ЗМІСТ