



## ПЕРЕДМОВА

Випуск дайджесту присвячено досвіду архівних установ світу щодо довгострокового зберігання електронних інформаційних ресурсів.

У публікації «К вопросу об организации защиты информации при длительном хранении документации с использованием интегрированных (гибридных) технологий» розглянуті переваги і недоліки комп'ютерних технологій і традиційних мікрографічних технологій при тривалому зберіганні документації.

У публікації «Система маркировки электронных носителей в страховом фонде документации» описуються принципи маркування електронних носіїв в страховому фонді документації, наводиться структура маркування, а також пропонуються додаткові сучасні технічні засоби маркування та ідентифікації електронних носіїв.

У публікації «Технология микрофильмирования для долговременного хранения электронных документов» детально опрацьовується питання про статус мікрофільму документа як оригіналу, і робиться висновок про можливість застосування мікрофільмування з метою довготривалого зберігання електронних документів.

У публікації «Создание электронных архивов — актуальная задача сегодняшнего дня» розповідається про те, як виглядає сьогодні ситуація з архівним збереженням електронних документів, які тут бачаться перспективи, які є труднощі і як їх можна і треба долати.

У публікації «Оцифровка – не гарантия вечной сохранности» розповідається про те, що всі кошти, які ми сьогодні вкладаємо в оцифровку, будуть втрачені, якщо ми регулярно не будемо нести витрати по підтримці досягнутого результату.

У публікації «Меры и способы сохранения информации» запропоновано кілька методів забезпечення збереження машино читаних даних і способів оптимізації методів зберігання електронних інформаційних ресурсів.

У публікації «Больших Данных больше не будет. Забудьте!» розповідається про поділ загального терміна «Великі дані» на кілька практичних напрямків, використовуючи для цього більш "змістовні" назви.

У публікації «Skype for Business — новый уровень поддержки деловых коммуникаций от Microsoft» розповідається про випущений компанією Microsoft продукт Skype for Business (SfB).

У публікації «О решении класса “безопасность как сервис” (SECaaS)» розповідається про рішення щодо підвищення безпеки інфраструктури підприємства, перенесеної в сторонній ЦОД.

У публікації «Оптимизация работы с документами: как снизить расходы на треть» розповідається про впровадження проектів MDS, що дозволяє скоротити пов'язані з документообігом витрати в середньому на 30-35%.



## К ВОПРОСУ ОБ ОРГАНИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ДЛИТЕЛЬНОМ ХРАНЕНИИ ДОКУМЕНТАЦИИ С ИСПОЛЬЗОВАНИЕМ ИНТЕГРИРОВАННЫХ (ГИБРИДНЫХ) ТЕХНОЛОГИЙ

Источник: <http://cyberleninka.ru/article/n/k-voprosu-ob-organizatsii-zaschity-informatsii-pri-dlitelnom-hranenii-dokumentatsii-s-ispolzovaniem-integrirovannyh-gibridnyh#ixzz3IKQw1Vhy>

Авторы: А.К. Талалаев, О.В. Чечуга

*Рассмотрены преимущества и недостатки компьютерных технологий и традиционных микрографических технологий при длительном хранении документации. Анализ каждого из этих методов показал, что оптимальным способом хранения информации является использование так называемых интегрированных микрографических технологий для создания и использования СФД.*

До последнего времени в нашей стране создание и использование страхового фонда документации (СФД) осуществляется на базе микрографических технологий. Однако в настоящее время у этих технологий появилась альтернатива - компьютерные технологии, которые в принципе позволяют решить все задачи, которые вытекают из целей создания СФД. Этими задачами, как и в случае использования микрографических технологий, являются:

- запись на носитель информации;
- хранение носителя информации в течение длительного времени (не менее 75 лет);
- обеспечение доступа (использование) к информации.

Для того чтобы сделать какой-либо вывод о целесообразности использования компьютерных технологий, необходимо рассмотреть их преимущества и недостатки.

Если говорить о традиционных микрографических технологиях, то к их достоинствам следует причислить:

- 1) микроформа - общепризнанный архивный носитель информации, который обеспечивает и приемлемую длительность хранения (гарантированно не менее 75 лет), и юридический статус информации;
- 2) существование отработанной нормативной базы;
- 3) наличие на мировом рынке возможности приобретения всего необходимого оборудования, созданного на современной элементной базе;
- 4) использование самого универсального вида информации - визуального восприятия человеком с помощью простого и недорогого читального аппарата.

К недостаткам микрографических технологий следует отнести:

- 1) большие затраты времени при осуществлении доступа к информации, так как большинство операций выполняется вручную;
- 2) осуществление доступа к информации только с помощью микроформ второго и последующих поколений, что приводит к некоторому снижению качества информации (каждое копирование приводит к снижению разрешения изображения на 5..10 %);
- 3) более низкое качество бумажной копии документа, полученного с микроформы, по сравнению с возможностями принтера по качеству печати.

Главные преимущества компьютерных технологий:

- 1) обеспечивается минимальное время доступа к информации, причём храниться информация может на удалённом компьютере;
- 2) повышается качество информации путём обработки цифрового изображения;
- 3) достигается очень высокое качество бумажной копии документа;
- 4) обеспечивается качественное многообразие форм передачи и распространения информации.

К недостаткам компьютерных технологий следует отнести следующее:

- 1) машиночитаемые носители информации не обеспечивают условий архивного хранения. Это означает, что, во-первых, нет достоверных данных о возможности полного сохранения информации на каком-либо существующем машиночитаемом носителе в течение хотя бы 50 лет и, во-вторых, бурное развитие компьютерных технологий способствует быстрому устареванию (3 – 5 лет) оборудования и программного обеспечения, что накладывает ограничения на использование информации вплоть до полной фактически её потери;
- 2) цифровая копия документа до настоящего времени не имеет юридического статуса оригинала;
- 3) не разработана в достаточной степени нормативная база.

Конечно, при использовании компьютерных технологий можно избежать ограничения сроков архивного хранения информации следующим образом. Для этого необходимо обеспечить перезапись архива через каждые 5 – 10 лет, разумеется, на новом оборудовании и с использованием нового программного обеспечения. Однако создание и использование СФД на такой основе потребует огромных финансовых средств.

Идея создания системы, которая бы интегрировала все преимущества и не имела недостатков, предполагает совмещение этих технологий, т.е. использование так называемых интегрированных микрографических и компьютерных технологий для создания и использования СФД. Это означает, что хранение информации осуществляется на микроформе (рулонный микрофильм, микрофиша и т. д.), а обращение информации – в цифровом виде. Тогда в общем случае технологический процесс выглядит следующим образом:

1. Запись информации на микроформу может производиться двумя способами при условии, что исходное представление информации - бумажный документ:

- микрофильмированием;
- сканированием бумажного документа (получение цифрового изображения) и затем записью на микроформу.

Первый способ - это традиционный микрографический технологический процесс.

Второй способ реализуется с помощью сканера бумажных документов и СОМ-системы, обеспечивающей запись цифровой информации с персонального компьютера на микроформу. Этот способ даёт возможность перед записью на микроформу улучшить качество изображения путем использования специализированных программ. Учитывая, что в настоящее время техническая документация на бумажном носителе, должна удовлетворять требованиям ГОСТ 13.1.002-80 «Репрография. Микрография. Документы для съёмки. Общие требования и нормы», такая обработка будет необходима для нескольких единиц процентов документации. Кроме того, такой двухступенчатый процесс является более дорогим. Таким образом, выбор должен быть сделан в пользу первого способа. Однако для документации, создаваемой в цифровом виде, более целесообразным с экономической точки зрения является изготовление микрофильма с помощью СОМ-системы (микрографического плоттера).

2. Хранение микроформ осуществляется по микрографической технологии.

3. Переход информации в различные формы осуществляется следующим образом. В цифровую форму информация с микроформы преобразовывается с помощью сканера, путём:

- печати на бумаге;
- записи на машиночитаемый носитель;
- передачи по телекоммуникационным линиям;
- записи на микрографический носитель с помощью СОМ-системы.

Как уже отмечалось выше, в настоящее время применение компьютерных технологий при создании и использовании СФД не нормируется. Это требует обоснования основных требований к процессу преобразования информации с микроформы в цифровой вид (иначе, к сканеру микроформы) по той причине, что этот процесс является ключевым для обеспечения качества информации при её дальнейшем обращении.

Основными параметрами сканера являются:

- способ оцифровки изображения;
- разрешающая способность;
- виды обработки изображения.

Для документов СФД, а это, как правило, техническая графика и текст, наиболее приемлемым способом оцифровки изображения является способ получения однобитного изображения, который означает, что при оцифровке каждая точка изображения (пиксель) принимается либо чёрной, либо белой

при сравнении с задаваемой величиной порога белое/чёрное. Это даёт возможность сократить до минимума размер изображения в цифровом виде, что обеспечивает приемлемое время оцифровки изображения и минимальные требования к величине памяти для хранения информации по сравнению с другим известным методом оцифровки - изображение в оттенках серого. Наличие такого способа является необходимым для получения высококачественной цифровой копии полутонового изображения.

Важным параметром, влияющим на качество изображения, является приведенное к первичному носителю (бумажный документ) разрешение, с которым проводится сканирование. Для выработки требования к этому параметру необходимо определить критерий. Учитывая, что, в конечном счёте, цель микрографических и компьютерных технологий - представить информацию для восприятия человека, за указанный критерий целесообразно принять качество изображения, полученного после сканирования (цифровое изображение). А качество цифрового изображения, как в микрографических технологиях, целесообразно определить показателем предела читаемости, который находится по цифровому изображению тест-объекта на экране монитора после сканирования кадра микроформы с тест-объектом. Из-за искажений, вносимых сканером, в количественном отношении показатель предела читаемости должен быть на одну группу выше для микроформы и определяется ГОСТ 13.1.102-94 «Репрография. Микрография. Микроформы на галогенидосеребряных плёнках. Общие технические требования и методы контроля». Эксперименты показывают, что для выполнения этого требования разрешающая способность, приведенная к бумажной копии, должна составлять 350 - 400 dpi.

Обработка изображения при сканировании необходима для повышения качества. К основным, широко используемым видам обработки изображения, следует отнести следующие:

- компенсация неравномерности фона;
- регулировка контраста изображения;
- уменьшение зашумлённости изображения.

В настоящее время оборудование, удовлетворяющее всем требованиям для получения высококачественного изображения, уже создано и предлагается на мировом рынке для практического использования интегрированных микрографических и компьютерных технологий. Кроме того, прогнозируется, что на предприятиях России (хоть и с отставанием от развитых стран) через 5 - 7 лет более 50 % документов будет создаваться и обращаться в цифровом виде. Таким образом, задачи внедрения новых технологий при создании и использовании СФД является весьма актуальной.

Список литературы:

1. Наймарк А. Микрофототехника - предмет и практика. М. : Мир 1974. 75 с.
2. Талалаев А. К. Диалоги о репрографии. Тула : Пересвет, 2001. 109 с.



## СИСТЕМА МАРКИРОВКИ ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ В СТРАХОВОМ ФОНДЕ ДОКУМЕНТАЦИИ

Источник: <http://cyberleninka.ru/article/n/sistema-markirovki-elektronnyh-nositeley-v-strahovom-fonde-dokumentatsii#ixzz3lK3iehI7>

Авторы: Е.Е. Евсеев, А.К. Талалаев, Н.Е. Проскуряков, П.Е. Завалишин

*Описываются принципы маркировки электронных носителей в страховом фонде документации, приводится структура маркировки, а также предлагаются дополнительные современные технические средства маркировки и идентификации электронных носителей - машиночитаемый линейный штрих-код, двухмерный матричный штрих-код типа QR и др.*

В современном обществе одним из основных факторов влияния научно-технического прогресса на все сферы деятельности человека является широкое использование информационных технологий. Под влиянием новых информационных технологий происходят коренные изменения в системе управления документами - автоматизируются процессы обоснования и принятия решений, организация их выполнения, появляются новые виды документов, стремительно возрастает электронный документооборот. Количество и объёмы используемых в современном мире документов растут. Причём соотношение электронных и бумажных документов со временем меняется в пользу последних. На данный момент, согласно статистическим данным, объём корпоративной электронной информации каждые три года удваивается.

Можно с уверенностью сказать, что отказаться полностью от бумажных документов не удастся никогда, однако, по мнению опытных в этой области экспертов в будущем доминировать всё же будет использование электронных вариантов.

Все виды документов являются важнейшим информационным ресурсом и продуктом любого рода деятельности современного общества. В современном мире они имеют не только информационное, но и юридическое значение, подтверждая имущественные, социальные и другие права различных субъектов общественных отношений. В документах накапливается, хранится и передается потомкам научно-техническое, культурное и историческое наследие.

Обеспечение возможности быстрого восполнения необходимой для общественных и государственных нужд документации, уничтоженной, безвозвратно утраченной или недоступной в условиях особого периода, чрезвычайных ситуаций, террористических актов и других форс-мажорных обстоятельств, является одной из важных задач государства по обеспечению его военной, экономической и информационной безопасности. Информационное содержание и юридическая сила утраченных документов

могут быть эквивалентно восполнены (возмещены) в приемлемые для особого периода и чрезвычайных ситуаций сроки только в виде заранее изготовленных на компактных носителях информации и надежно хранимых страховых (резервных) копий этих документов, достоверно воспроизводящих их информационное содержание и юридический статус [1].

Важность работ по созданию и сохранению стратегических страховых информационных ресурсов в Российской Федерации подтверждается действующими Постановлениями Правительства Российской Федерации от 18.01.1995 г. № 65 «О создании единого российского страхового фонда документации» и от 26.12.1995 г. №1253-68 «Об обеспечении создания единого российского страхового фонда документации», а также другими утвержденными правовыми и нормативными документами, касающимися различных аспектов создания и использования страхового фонда документов.

В соответствии с Постановлением Правительства Российской Федерации от 26.12.1995 г. №1253-68 основной целью создания системы единого российского страхового фонда документации (далее - ЕР СФД) является своевременное, гарантированное и надежное обеспечение пользователей страховыми копиями документов при наступлении чрезвычайных обстоятельств [2].

Страховой фонд документации представляет собой массив целенаправленно изготовленных на компактных носителях информации упорядоченных и надежно защищенных от различных факторов уничтожения и разрушения страховых копий важнейших видов документов. Совокупность находящихся в государственной собственности Российской Федерации страховых фондов документации различного назначения, создаваемых, надежно хранимых и используемых по установленным государством нормам и правилам, образует ЕР СФД. В настоящее время основными носителями долговременного хранения страховых копий документов в системе ЕР СФД являются галогенидосеребряные микрографические носители информации (далее - МН).

Одним из требований к функционированию системы ЕР СФД являются оперативная обработка поступающих заявок и поиск необходимых носителей по ключевым идентификационным признакам. При этом важными факторами, влияющими на скорость работы системы, являются наличие базы данных страховых документов, использование поисковых модулей, а также применение единой для ЕР СФД универсальной структуры маркировки носителей и средств их хранения.

Существующие принципы унифицированного обозначения МН в системе ЕР СФД основаны на единой структуре обозначения микрофильмов, которая установлена в одном из ГОСТ класса 33. К основным элементам данного обозначения относятся шифр документации, номер МН, ведомственная принадлежность, индекс состава, индекс структуры и др.

Информация, закодированная в данном обозначении, записывается на сам МН в виде специального трафарета и вручную дублируется на коробках для хранения МН. Дополнительно коробки с МН в зависимости от

назначения МН - основной или запасной - помечаются разными цветовыми метками.

Таким образом, в существующей системе хранения МН в ЕР СФД сам МН и коробка представляют собой уникальную единицу хранения и учета информации. Действующая система маркировки МН позволяет осуществлять поиск МН, их учет, проверку состояния и т.п., а также служит основой для ведения базы данных ЕР СФД на МН [3].

Однако в последние годы неуклонно увеличивается объем документации, выполненной в электронном виде, которая требует долгосрочного сохранения в ЕР СФД. Данная документация в организациях хранится, как правило, на различных электронных носителях (далее - ЭН), обозначение которых не унифицировано, наносится в произвольной форме и не имеет определенной структуры шифров-идентификаторов.

Кроме этого, существуют специфические виды электронных документов, такие как программная документация, трехмерные модели изделий, полученные в системах автоматизированного проектирования, аудио и видео документация и т.п., которые не могут быть сохранены на традиционных микрографических носителях и требуют сохранения в исходной цифровой форме.

Учитывая потребность в страховом сохранении электронных документов, специалистами ФГУП «НИИР» были исследованы возможности установления единых требований к обозначению ЭН, предназначенных для предполагаемой закладки в ЕР СФД, и унификации ее элементов с существующей системой обозначения МН. Это позволило бы объединить информацию о документах на ЭН и документах на МН с целью создания единой базы данных документов ЕР СФД, включающую в себя и документы, хранимые в электронном виде.

При этом предложено адаптировать структуру обозначения МН к системе маркировки ЭН. Также предложены дополнительные современные технические средства маркировки и идентификации ЭН, к которым относятся машиночитаемые линейный штрих-код, двухмерный матричный штрих код типа QR и др. Современные технологии позволяют идентифицировать уникальный ЭН путем присвоения ему линейного или двухмерного матричного штрихового кода, т.е. представить текстовые и цифровые атрибуты объекта, подлежащего автоматической идентификации, виде штрихов и пробелов, размеры и последовательность которых формируется по заранее определенным правилам.

Штриховой код в отличие от других информационных знаков не только выполняет функции идентификационного и информационного характера, но и несет в себе ряд дополнительных функций, таких как автоматизированная идентификация носителя с помощью считывающих устройств, автоматизированный учет и контроль массивов носителей, оперативное управление процессом работы с носителями, повышение скорости обслуживания пользователей, снижение административных расходов и т.д.

Предлагаемая система маркировки ЭН представлена на рис. -1. Необходимо отметить, что перед использованием в системе ЕР СФД каждый ЭН должен проходить обязательную сертификацию.

Предлагаемая система маркировки ЭН для ЕР СФД должна содержать следующие элементы:

1. Элемент защиты ЭН от подделки. Может представлять собой голографическое изображение с элементами защиты.
2. Наименование ЭН, например « Сертифицированный электронный носитель Единого российского страхового фонда документации».
3. Уникальный серийный номер ЭН.
4. Обозначение типа и скорости записи ЭН.
5. Дата выпуска ЭН.
6. Информация о производителе ЭН.
7. Обозначение ЭН в системе ЕР СФД (в том числе штрих-код, основной/запасной).
8. Машиночитаемая запись (двухмерный QR-код) с информацией о записанных на ЭН данных. Применение QR-кода даст возможность на сравнительно маленьком изображении кода поместить большое количество информации, допускающей ее машинное считывание.

Следует сказать, что большинство из современных машиночитаемых элементов маркировки ЭН позволяют наносить их и на существующие средства хранения МН, в частности на применяемые сейчас в ЕР СФД коробки для хранения микрофильмов, что в перспективе позволит организовать автоматизацию хранения ЭН и МН в системе ЕР СФД, а также в последующем перейти к роботизации поиска носителей и изъятия их из фонда [3].

Кроме этого, применение предлагаемой системы маркировки для всех видов находящихся в ЕР СФД носителей дает возможность создать общую базу данных МН и ЭН, которая обеспечит единое управление фондом и позволит повысить оперативность поиска информации, усовершенствовать учет документов, оптимизировать процессы планирования и отчетности.

Необходимо добавить, что предложенные принципы формирования маркировочных шифров ЭН могут применяться с учетом отраслевой специфики для создания архивных фондов и фондов пользования в различных системах хранения и обработки электронной информации, в том числе и в системе Росархива.

Конечной целью проводимых исследований является разработка проекта нормативного документа для системы ЕР СФД уровня ГОСТ, в котором будут регламентированы единые правила обозначения и маркировки всех видов носителей, находящихся в едином российском страховом фонде документации.



- Элемент защиты сертифицированного электронного носителя от подделок
- Наименование сертифицированного электронного носителя
- Уникальный серийный номер сертифицированного электронного носителя
- Обозначение типа и скорости записи сертифицированного электронного носителя
- Дата выпуска сертифицированного электронного носителя
- Обозначение электронного носителя в системе ЕР СОД (в том числе штрих-код, основной/запасной)
- Информация о производителе сертифицированного электронного носителя

Рис. 1 – Предлагаемая система маркировки ЭН

### Список литературы:

1. Чечуга О. В., Евсеев Е. Е., Завалишин П. Е. Современные подходы к обеспечению гарантированной безопасности важнейших видов государственных информационных ресурсов // Известия ТулГУ. Технические науки. Вып. 3. Тула: Изд-во ТулГУ, 2014. С. 189-197.
2. Постановление Правительства Российской Федерации от 26.12.1995 г. № 1253-68 «Об обеспечении создания единого российского страхового фонда документации» [Электронный ресурс]. Режим доступа: [http://gov.ru/upload/Postanovlenie%20Pravitelstva%20RF\\_410](http://gov.ru/upload/Postanovlenie%20Pravitelstva%20RF_410) (дата обращения: 03.09.2014).
3. Евсеев Е.Е., Завалишин П.Е., Талалаев А.К., Проскураков Н.Е., Ануфриева А.Ю. Основные принципы и технологии универсальной маркировки средств хранения в системе страхового фонда документации // Известия ТулГУ. Технические науки. Вып. 5. Тула: Изд-во ТулГУ, 2014. С. 168-180.



# ТЕХНОЛОГИЯ МИКРОФИЛЬМИРОВАНИЯ ДЛЯ ДОЛГОВРЕМЕННОГО ХРАНЕНИЯ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ

Источник: <http://vestarchive.ru/2014-1/3094-tehnologiiia-mikrofilmirovaniia-dlia-dolgovremennogo-hraneniia-elektronnyh-dokumentov.html>

Автор: А.Е. КУРЦЕР

Вопрос долговременного хранения подлинников документов является крайне актуальным на сегодняшний момент.

Документы, созданные на различных носителях с помощью различных средств записи информации, с течением времени теряют свои эксплуатационные свойства в силу ряда факторов: неблагоприятных условий хранения, аварийных и чрезвычайных ситуаций, некорректного использования.

Поэтому задача сохранения информационных ресурсов, предотвращения последствий, связанных с утратой документационного фонда, исключительно важна.

При решении этой задачи используются как технологии сохранения собственно документа, то есть подлинника, так и технологии хранения содержания документа, а именно, конвертации информации в формат, отличный от формата подлинника, такой формат, который позволяет обеспечить долговременное хранение документов, обладающих юридической силой, а также страховой фонд, реализующий доступность информации при любых непредвиденных обстоятельствах, включая чрезвычайные.

**История вопроса.** Микрофильмирование появилось почти одновременно с изобретением фотографии в первой половине XIX в. Первый шаг в его создании сделали англичане Джон Гершель и Джеймс Стюарт, которые предложили в 1853 г. «хранение публичных документов в сжатой форме на микроскопических негативах» и применили этот метод в своей практике.

В 1906 г. Павел Отле и Роберт Гольдшмидт предложили использовать микрофильмы для хранения на них библиографических данных. Преимуществом микрофишей считался стабильный и прочный формат, недорогой, простой в использовании, чрезвычайно компактный, а также легкость воспроизведения документов с этого носителя. При этом главной целью Отле уже тогда было создание Всемирной библиотеки юридической, социальной и культурной документации.

Датой рождения страхового фонда документации как понятия можно считать 1925 г., когда Джордж Маккарти, вице-президент нью-йоркского банка, запатентовал ротационную микрофильмирующую камеру для автоматического копирования банковских документов.

Научно-технический прогресс вызвал резкое увеличение объема научно-технической документации на бумажных носителях, что, в свою очередь, обусловило широкое использование микрофильмирования в

библиотечном и архивном делопроизводстве. Этот путь был проложен через длительное изучение информационно-технологических аспектов работы с документами. В российской науке микрофотокопирование как способ широкого распространения архивной информации впервые было подробно рассмотрено в трудах К. Б. Гельман-Виноградова, который в отношении комплектования архивов микрофотокопиями декларировал «принцип расширения возможностей использования документальных материалов всех государств мира».

В 1950–1960 г.г. была предложена и реализована концепция использования микроформ для активных информационных систем. При этом микроформа использовалась как основной носитель для сохранности информации и ее использования. В это время состоялось значительное улучшение технологий микрофильмирования документации.

В середине восьмидесятых годов прошлого столетия был разработан ряд государственных стандартов, среди которых и стандарты военного назначения, составивших класс 33 «Страховой фонд документации», в которых основным носителем определен микрофильм. В последнее десятилетие этот класс пополнился новыми документами.

Целью исследования являются теоретические аспекты долговременного хранения подлинников электронных документов. Исследуется история возникновения и развития микрофильмирования и микроформы как основного носителя для сохранности информации и ее использования. Изучаются вопросы создания страховых фондов документации, как общероссийских, так и отраслевых, а также нормативные документы, регламентирующие создание, хранение и применение подлинников таких фондов. Тщательно исследуется нормативно-правовая база создания страховых фондов документов на объекты повышенного риска (потенциально опасные объекты) и объекты систем жизнеобеспечения. Подробно прорабатывается вопрос о статусе микрофильма документа как подлинника, и делается вывод о возможности применения микрофильмирования в целях долговременного хранения электронных документов. На основании анализа изменений в Основах законодательства Российской Федерации о нотариате делается предположение об участии нотариусов в процессе создания подлинников электронных документов на бумажном носителе (удостоверение подлинности) в целях долговременного хранения, в том числе для единого российского страхового фонда документов, юридически значимых электронных документов, заверенных электронными подписями. Указывается возможность использования цифровых хранилищ документов в качестве источника исходных материалов для микрофильмирования и преимущества такого использования.

Полностью материал публикуется в российском историко-архивоведческом журнале ВЕСТНИК АРХИВИСТА.



## СОЗДАНИЕ ЭЛЕКТРОННЫХ АРХИВОВ — АКТУАЛЬНАЯ ЗАДАЧА СЕГОДНЯШНЕГО ДНЯ

Источник: <http://www.pcweek.ru/ecm/article/detail.php?ID=178940>

Автор: Андрей Колесов 20.10.2015

*Переход к безбумажному документообороту связан с необходимостью поддержки полного жизненного цикла электронных документов (речь идет об электронных подлинниках) от момента их создания до уничтожения. И если эта проблема применительно к документам с относительно небольшим сроком хранения (5 – 10 лет) сегодня уже относится с технической точки зрения к категории сугубо рутинных операций и ее решение упирается лишь в необходимость получения «добро» со стороны нормативно-законодательных требований, то вопросы, касающиеся документов с большими, а тем более «вечными» сроками хранения, продолжают оставаться спорными и во многом до сих пор нерешенными. Хотя актуальность поддержки долгосрочного цикла хранения электронных подлинников хорошо осознают сами представители архивных структур страны, в том числе и потому, что обеспечение сохранности растущих объемов бумажных хранилищ требует все более значительных затрат.*

*О том, как выглядит сегодня ситуация с архивным хранением электронных документов, какие здесь видятся перспективы, какие есть трудности и как их можно и нужно преодолевать, с директором Центрального архива атомной отрасли Госкорпорации «Росатом» Юлией Великой беседовал обозреватель PC Week/RE Андрей Колесов.*

**PC Week:** Давайте начнем наш разговор с пояснения: какое положение ваша организация занимает в структурах «Росатома» и Росархива?

**Юлия Великая:** Наш архив является структурой Госкорпорации «Росатом» в форме частного учреждения (ЧУ), на которое возложено решение задач обеспечения сохранности, комплектования, учёта и использования архивных документов атомной отрасли, в том числе документов Архивного фонда РФ. «Центратомархив» входит в общую систему архивов страны и в нормативно-методическом плане должен выполнять требования Росархива.

Госкорпорация «Росатом» – это огромная отрасль, сотни предприятий разного профиля – производственные, эксплуатационные, исследовательские, управляющие. И, соответственно, у большинства предприятий есть свои архивные структуры. То есть в Госкорпорации «Росатом» есть сеть архивов, каждый из которых организационно входит в состав своей компании, нормативно-методическое сопровождение и контроль за их деятельностью осуществляет ЧУ «Центратомархив».

Между Госкорпорацией «Росатом» и Росархивом заключен договор, на основании которого «Центратомархив» и архивные структуры организаций корпорации имеют право на депозитарное хранение документов у себя сроком до 100 лет, после чего документы Архивного фонда РФ должны передаваться на постоянное архивное хранение в государственные архивы. Разумеется, речь пока идет о подлинниках на традиционных бумажных носителях. В рамках этого договора передачи документов в Росархив пока не было, так как самые ранние даты находящихся на хранении документов – это 20-е годы прошлого столетия. Но я хочу обратить внимание: у нас есть право именно на депозитарное хранение, т. е. не на «вечное», а на временное. Хотя, конечно, понятно, что если речь идет о периодах в 100 лет, то с технической и законодательной точки зрения это уже фактически тот же уровень качества хранения, что и «вечное».

**РС Week: Как организовано у вас архивное дело с точки зрения работы с бумажными и электронными документами и взаимодействия архивов с текущим документооборотом?**

**Ю. В.:** Архив – это не застывшая структура, его задачей является не только управление некоторым фиксированным объемом хранения, но и его постоянное комплектование, при этом одним из основных источников пополнения фондов являются системы текущего делопроизводства. И это постоянное взаимодействие является двунаправленным: с одной стороны, в делопроизводстве должны выполняться требования к документам с точки зрения их последующего архивного хранения, с другой – мы должны в своей работе учитывать развитие современных СЭД.

В Госкорпорации «Росатом» еще несколько лет назад была внедрена централизованная СЭД на базе Documentum, которая охватывает половину территории страны, это одна из крупнейших подобных систем в Европе. Сегодня в ней хранятся документы более 150 организаций и их филиалов, она обслуживается специализированной отраслевой компанией – ЗАО «Гринатом», все вычислительные ресурсы размещены в централизованном дата-центре с сетевым доступом к ним.

Что касается бумажных и электронных документов, то на сегодня все подлинники архивных документов являются бумажными, это просто последствия нормативных требований Росархива вплоть до недавнего прошлого. Если о технических аспектах перехода на электронные подлинники для документов долгосрочного хранения можно спорить, то «закон – есть закон». Но даже в этой ситуации вопрос создания архива электронных копий для нас всегда являлся актуальным. Дело в том, что архив – это не только обеспечение сохранности документов, хотя это одна из основных наших задач, не очень простая и достаточно затратная. Мы должны обеспечивать возможность работы с этими документами и их использования, причем не только для специалистов отрасли, но и широкой общественности. Для нашей отрасли эта функция является особенно важной. Специфика атомной промышленности такова, что у нас даже документы 50 – 70-летней давности могут представлять не только исторический или

юридический интерес, но и обладать реальной технической ценностью сегодня. Там могут быть, например, зафиксированы идеи и проекты, которые в свое время не были реализованы, но вполне актуальны сейчас (например, появились технические возможности для их реализации). Атомная сфера всегда была и остается весьма закрытой, для нас очень важным направлением является работа по рассекречиванию и популяризации.

То есть у нас документы не просто лежат на стеллажах, с ними нужно постоянно работать, и, конечно, электронные методы, пусть даже создание фонда пользования электронных копий архивных документов, очень нужны. Опять же есть «атомная» специфика. Например, у нас есть так называемый Чернобыльский архив, в состав которого входят документы, в том числе кадровые, подтверждающие участие граждан в ликвидации последствий аварии на Чернобыльской АЭС в 1986 – 1987 гг. и, соответственно, право на социальные льготы. Но дело в том, что многие из этих документов имеют радиоактивный фон, поэтому этот архивный фонд полностью оцифрован. Именно с электронной версией работают специалисты «Центратомархива», а бумажные подлинники хранятся в изолированном хранилище специализированной отраслевой организации.

На сегодняшний день актуальной задачей является полная оцифровка унаследованного бумажного архива. Это весьма трудоемкая работа, полномасштабно она у нас началась только с прошлого года, и тут нам еще предстоит большой путь.

**PC Week: А в вашей СЭД используются только бумажные подлинники или есть и электронные? В каком виде поступают оттуда документы к вам в архив?**

**Ю. В.:** В СЭД Госкорпорации «Росатом» есть и электронные подлинники, но документы, которые подлежат архивному хранению, пока представлены в виде электронных скан-копий на традиционных носителях. Сейчас мы подошли к моменту передачи на архивное хранение документов, созданных в отраслевой СЭД. Как известно, платформа Documentum имеет все необходимые для этого функции, пока они у нас были задействованы в минимальной степени, но как раз сейчас мы будем использовать их более масштабно.

**PC Week: То есть у вас сегодня реализуется традиционная двухконтурная работа с документами, когда их юридическая значимость обеспечивается бумажными подлинниками, а для оперативной работы используются их электронные копии. А каковы ваши планы по переходу к одноконтурной схеме, без дублирования, когда можно будет обходиться без бумажных подлинников?**

**Ю. В.:** Как раз сейчас этот вопрос прорабатывается. До конца этого года мы должны сформулировать наше конкретное видение такой организации архивной работы, выявить проблемы на этом пути и найти методы их решения, а также в первом приближении определиться с проектом, в том числе по этапам его реализации, срокам и затратам.

В последнее время растет число видов документов, которые допускается использовать в электронном формате, но при этом порой возникает некоторое противоречие с тем, что сохраняется в существенной мере неопределенность с обеспечением их долгосрочного хранения. При этом для ряда категорий имеется прямое законодательное требование хранения только в бумажном виде.

Но как бы то ни было тенденция на переход работы архивов в электронном виде уже не просто видна, она становится реальностью. Так, с 21 сентября вступили в силу новые «Правила организации хранения, комплектования, учёта и использования документов Архивного фонда Российской Федерации и других архивных документов в органах государственной власти, органах местного самоуправления и организациях» (приказ об их утверждении в Минкультуры был подписан в марте, но регистрация приказа в Минюсте прошла только сейчас), в соответствии с которыми мы получаем законную возможность хранить электронные документы с постоянным сроком хранения.

То есть мы получили сейчас необходимую нормативную базу для создания электронных архивов, теперь нужно уже заниматься вопросами технической реализации, в том числе это касается подтверждения электронной подписи, проблем недолговечности электронных носителей, наличия аппаратно-программных средств, способных работать с этими носителями.

Все это нужно делать, не откладывая в дальний ящик, в том числе и потому, что существующие мощности по хранению бумажных носителей близки к исчерпанию, их расширение потребует дополнительного серьезного финансирования.

**РС Week: Насколько я знаю, в упомянутых вами новых Правилах скорее содержатся положения, разрешающие хранение электронных документов, но нет описания конкретных регламентов – как это делать.**

**Ю. В.:** Да, там конкретики недостаточно, но уже сегодня есть методические рекомендации Росархива по хранению электронных документов и обеспечению сохранности электронных носителей, которые должны быть в ближайшее время дополнены в соответствии с новыми Правилами.

**РС Week: Так, разрешение Минкультуры и рекомендации Росархива есть. Когда же вы будете готовы принимать на хранение подлинники электронных документов?**

**Ю. В.:** Архив – это не просто хранилище файлов, а система управления ими, включая целый набор функций, в том числе учета, поиска и многого другого. Документы, кроме собственно некоторого содержания, включают наборы метаданных, в том числе формируемых ИТ-системами. В Госкорпорации «Росатом» в настоящее время проводятся работы по расширению возможностей общекорпоративной системы электронного документооборота в плане усиления функций архивного хранения. Одновременно решаются проблемы, о которых шла речь и ранее:

подтверждения электронной подписи, миграции данных и сохранности метаданных, разграничения прав доступа пользователей к архивным документам.

Вполне вероятно, что уже в следующем году мы сможем создать нужную нормативную базу и технологическую инфраструктуру в рамках реализации этого проекта. При этом и сама система документооборота Госкорпорации «Росатом» должна перейти на работу в большей степени с подлинниками электронных документов.

**РС Week: Мне кажется, что, хотя вы ссылаетесь на уже имеющиеся правила и рекомендации Росархива, вам придется самостоятельно решить целый ряд задач технического и методического характера.**

**Ю. В.:** Да, мы понимаем это. Ситуация сегодня такова, что мы уже не можем ждать, когда нам принесут все нужные решения в готовом виде. Нам дали формальную возможность перехода на работу с электронными документами, и мы должны воспользоваться этим. Я уверена, что создание электронного архива нам вполне по плечу, и мы будем готовы поделиться своим опытом и достижениями в этой сфере со всеми архивистами страны.

**РС Week: Спасибо за беседу.**



## **ОЦИФРОВКА – НЕ ГАРАНТИЯ ВЕЧНОЙ СОХРАННОСТИ**

Источник: <http://www.goethe.de/ins/ru/pet/bib/bw/ru3616481.htm>

Эйфория по поводу возможностей оцифровки велика. Доктор Мартин Лухтерхандт, старший советник Земельного архива в Берлине, предостерегает от того, чтобы рассматривать оцифровку как универсальное средство сохранения материалов.

*Господин Лухтерхандт, оцифровка превозносится многими, и прежде всего – библиотеками. Вы достаточно скептически относитесь к этому. Почему?*

Я рассматриваю этот процесс как бы с двух позиций и вовсе не абсолютно скептически отношусь к оцифровке. Я скептически отношусь к тому, как оцифровка используется сегодня, и какие цели мы перед ней ставим.

*Что именно вызывает Ваш скепсис?*

Оцифровка имеет огромные преимущества для ежедневного использования архивных материалов или библиотечных фондов, но она не подходит для долгосрочного хранения. Все прекрасно осознают, что цифровая продукция быстро изменяется и очень нестабильна. Ее невещественность открывает буквально фантастические возможности для использования. Однако электронные источники информации все же не вечны

или, иначе говоря, их сохранение требует очень больших затрат. В этом смысле электронные образы являются слишком дорогим удовольствием.

*Не могли бы Вы подробнее рассказать об этих затратах?*

Это касается всех электронных источников информации. Все, что регулярно не поддерживается в порядке, в конце концов нельзя будет использовать. Все средства, которые мы сегодня вкладываем в оцифровку, будут потеряны, если мы регулярно не будем также нести расходы по поддержанию достигнутого результата.

Например, сканируя сегодня документ, Вы используете технические стандарты, которые через 20 лет устареют. Для того чтобы через 20 лет можно было вновь работать с этим документом, Вы должны иметь соответствующее программное обеспечение.

Необходимо постоянное техническое совершенствование. И если Вы хотя бы один раз этим пренебрежете, возможны потери. Сегодня, например, это технические проблемы, которые вынуждены решать сотрудники комиссии под руководством Марианны Биртлер при работе со старыми электронными записями «Штази», службы госбезопасности бывшей ГДР.

*Недооценка высоких и рассчитанных на длительный срок расходов, связанных с использованием цифровой техники - это всеобщая тенденция?*

Во-первых, никто вообще еще точно не знает, сколько это стоит, а во-вторых, по умолчанию исходят из того, что деньги на это потом будут найдены. Шведский архивист Йонас Пальм попытался приблизительно подсчитать эти расходы. В своей статье “The Digital Back Hole” («Электронная черная дыра») он исследует известные факторы. Какова динамика цен на технику? Сколько стоит сохранение одного терабайта данных? Каковы необходимые затраты на обслуживание? Вывод: цены растут. Никто еще не нашел решения этой проблемы, но между тем техника активно используется и на этом базируется большая часть нашей экономики.

*Что же, по Вашему мнению, следует делать?*

Следует больше думать о перспективах. Об этом необходимо думать каждый раз при использовании оцифровки: понадобится ли это в будущем? И если да - какое решение существует для сохранения необходимой информации в стабильном состоянии на длительное время? Какая форма сохранения материала есть у меня еще на случай, если от электронной формы я однажды захочу или вынужден буду отказаться?

*Что конкретно Вы предлагаете?*

**Для архивных документов и культурных ценностей рекомендуется двойное сохранение. Необходим микрофильм как страховая копия и электронный образ для ежедневного использования материала.**

**В любом случае необходимо разделять две цели – удобное использование и длительное хранение. Ни одна из форм не может одновременно оптимально решить обе эти задачи: фильм не очень удобен в использовании, а оцифровка не подходит для сохранения на века.**

*Какие преимущества имеет микрофильм?*

Техника, необходимая Вам для использования микрофильма, очень проста. В принципе, достаточно даже лупы и источника света. Такую технику можно сделать очень быстро, если возникнет необходимость. В противоположность этому, можно представить себе многочисленные ситуации, когда использование электронных образов невозможно. Что Вы будете делать с диском с прекрасными цветными электронными образами в технически плохо оснащенной стране?

*Так что же, назад к микрофильму?*

Да, если речь идет о хранении. Микрофильм в течение десятилетий был единственной формой репродуцирования. Но старый метод не становится плохим только потому, что он уже так долго используется. Только из-за этого заменить его было бы ошибкой.

Гораздо разумней не отказываться от микрофильмирования, а использовать его наряду с оцифровкой. Я выступаю за то, чтобы при планировании учитывать и микрофильмирование, а не делать ставку исключительно на оцифровку.

*Подобная ситуация существует и в других странах или только у нас?*

Конечно, нет. Противостояние электронных форм и аналоговых средств передачи информации существует во всем мире. В США, например, эйфория по поводу оцифровки достигла еще больших масштабов. Но в различных странах - например, в Швейцарии - существует и активное лоббирование микрофильмирования. В Швейцарии, как и у нас в Германии, существует программа страхового микрофильмирования с сохранением микрофильмов в специально созданном хранилище. Мы сотрудничаем со швейцарцами в этой области.

*Набирающий темпы процесс оцифровки Вас пугает?*

Знаете, я смотрю на эту проблему со здоровым профессиональным цинизмом: мы, архивисты, живем с постоянным сознанием того, что культурное наследие погибает. Мы и так можем сохранить его лишь частично. Это относится и к электронной информации. Для меня совершенно ясно, что многое из того, что мы сейчас имеем в электронном виде, через 15-20 лет не будет существовать в этой форме. Просто потому, что хранение будет стоить дорого или изменятся интересы или политические условия, потому что это нельзя будет больше использовать. Это нормальный процесс, и не следует его драматизировать. Однако не стоит обманывать себя, полагая, что цифровая информация будет храниться вечно.

Вопросы задавала Дагмар Гиберг, независимый публицист из Бонна.



## МЕРЫ И СПОСОБЫ СОХРАНЕНИЯ ИНФОРМАЦИИ

Источник: [http://e-biblio.ru/book/bib/01\\_informatika/infteh/book/docs/piece-118.htm](http://e-biblio.ru/book/bib/01_informatika/infteh/book/docs/piece-118.htm)

Любая социальная деятельность людей построена на создании, передаче, обработке и хранении информации. **Обеспечение сохранности информации** производится на основе применения специальных мер организации хранения и подготовки, восстановления и регенерации информации, специальных устройств резервирования. Качество обеспечения сохранности информации зависит от её целостности (точности, полноты) и готовности к постоянному использованию.

В первой половине прошлого века фотоматериалы зарекомендовали себя как надёжные носители информации, способные в специальных условиях долговременно её сохранять. Эта технология получила название микрофильмирование. Под **микрофильмированием** понимается совокупность процессов изготовления, хранения и использования носителей микроизображений информации. *Микроизображением* считается изображение, которое можно прочесть только при помощи оптических средств при увеличении до 40 крат (40х).

Фотографическая запись позволяет хранить микроизображения документов в виде микрофильмов и микрофишей, т.е. микроформ. Изображение обычной страницы документа формата А4 в микроформе может занимать площадь менее 1 см<sup>2</sup>. Микроформы служат защитной копией подлинника.

Первые микрофильмы появились в 1920-х – 1930-х годах. Фотографические носители постоянно совершенствовались. В то же время с 1930-х по 1990-х годы в нашей стране для микрофильмирования производились и использовались пленки на основе ацетатов целлюлозы.

В 1980-х годах западные фирмы (Kodak и др.) начали выпускать плёнки на полиэфирной (polyester) основе. Их долговечность в десять раз выше, чем у ацетатных, что объясняется их большой физической прочностью и химической стабильностью основы, а также большей компактностью. Именно их до сих пор рекомендуют для создания страховых и архивных фондов. **По мнению ряда специалистов, начиная с 1950-х годов и по настоящее время, микроформы остаются лучшим способом сохранения большинства документов для будущих поколений.**

В микрофильмировании используют микрофильмы рулонные, микрофильмы в отрезках, микрофиши, микрокарты и др.

Рулонная микрографическая пленка изготавливается шириной 16, 35 или 105 мм и длиной до 305 м. Форматная пленка – в виде отдельных листов определенных форматов. Основной международный стандартный размер микрофиши – 148x105 мм. Микрофиша имеет маркировку, позволяющую на

глаз установить её тему или род соответствующего документа, помещенного на ней.

Микроформа может представлять как полноразмерную копию, так и с уменьшением в масштабе от 1:9 до 1:30. По виду изображения микроформы являются негативными или позитивными.

Поиск нужного изображения производится пользователем с помощью читального аппарата (экран, соединённый с увеличителем). Этот процесс может управляться компьютером с выводом изображения на экран монитора.

Большинство ЭИР постоянно пополняется и длительно хранится на различных носителях. Важное значение для данных имеют методы их хранения и сохранения. Специалисты предлагают несколько методик обеспечения сохранности машиночитаемых данных вообще и в Интернете в частности. Среди них следующие:

- постоянная миграция материала к наиболее современным аппаратурно-программным средствам (т.е. непрерывная перезапись ресурса);
- сохранение исходного формата и средств раскрытия содержания материала;
- копирование (архивирование);
- защита от несанкционированного использования, замены, искажения и удаления;
- защита от компьютерных вирусов и неполадок в электрических и компьютерных сетях.

*Копирование* информации подразумевает создание рабочих, резервных и страховых архивов.

Под термином *«архив»* понимается совокупность электронных данных (в том числе программ), организованная на машиночитаемых носителях информации с целью обеспечения в случае необходимости их дальнейшего использования.

Архив – файл, содержащий один или несколько файлов в сжатой или несжатой форме и информацию, связанную с этими файлами (имя файла, дата и время последней редакции и т.п.). Архив – *страховочная копия*, используемая в случае утраты или порчи основной машиночитаемой информации, а также для длительного её хранения в месте, защищённом от вредных воздействий и несанкционированного доступа.

При этом *«архивация»* означает процесс создания на машинных носителях информации копий машиночитаемых ресурсов (данных, документов, программ) с помощью специальных программных средств. Компьютерными архивами информации, как правило, являются, электронные каталоги, базы и банки данных, а также коллекции любых видов информации.

Различают оперативные данные, условно-постоянную и другую информацию. Первые характеризуются значительной, по сравнению со вторыми, скоростью изменения своих параметров (объёма, содержания и др.). Они требуют более частого обновления копий, и, следовательно, имеют короткий период перезаписи и хранения (*шаг резервного копирования*).

Под **резервным копированием** понимают создание копий файлов с целью быстрого восстановления работоспособности системы в случае возникновения аварийной ситуации. Эти копии определенный срок хранятся на резервных носителях, которые периодически перезаписываются. Для обеспечения надёжности защиты данных некоторые специалисты рекомендуют иметь по три резервных копии последних редакций файлов.

При работе на ПК необходимо периодически проводить дефрагментацию дисков. Программа, выполняющая эту функцию, входит в состав всех ОС типа Windows. Путь к ней через меню «Программы» – «Специальные» – «Служебные». Вероятность успешного восстановления информации выше, если она хранится в менее фрагментированном виде. Кроме того, регулярное использование программы дефрагментации позволяет минимизировать время обращения к жёсткому диску при работе.

Простым и надёжным способом сохранения и восстановления системы является *репликация* (клонирование) жёстких дисков. Специальная программа (например, Acronis TrueImage, PowerQuest ImagePro и др.) формирует единый сжатый файл, содержащий образ диска со всей имеющейся информацией. Этот файл можно записать на сменный носитель или в отдельный раздел того же жёсткого диска, обозначенный как другой дисковод. При этом достигается быстрое восстановление после сбоев, вирусных атак или проблем с оборудованием.

Резервное копирование делится на: **полное, инкрементальное и дифференциальное**. При *полном резервном копировании* создаётся копия всех данных, подлежащих резервному копированию. Недостаток процедуры – необходимость значительного времени на её осуществление и значительного числа и (или) объёма резервных носителей; достоинство – быстрое восстановление информации.

При *дифференциальном копировании* дублируются только файлы, созданные или измененные со времени проведения последнего полного копирования. Чем больше это время, тем дольше будет осуществляться дифференциальное копирование. В случае краха системы для восстановления данных приходится задействовать последние полную и дифференциальную копии.

При *инкрементальном копировании* дублируются только те файлы, которые были созданы или изменены после последнего полного, дифференциального или инкрементального копирования. Время выполнения такого копирования относительно мало, но в случае утраты информации её придётся восстанавливать, используя последнюю полную и все последующие инкрементальные копии – самая длительная процедура восстановления.

Наиболее приемлемая схема, минимизирующая время резервного копирования данных и их восстановления – еженедельное полное и ежедневное инкрементальное копирование.

**Архивное копирование** – процесс создания копий файлов, предназначенных для долговременного или бессрочного хранения. Носители, на которых они хранятся, называют *архивными*. Он предполагает более

строгое структурирование информации, высокую степень автоматизации процесса архивирования и восстановления данных, а также работу с большими объёмами информации.

Периодическое проведение архивного копирования позволяет иметь копии нескольких разных версий одних и тех же файлов. Как правило, архивируются данные, которые никем не модифицировались 90 или более дней. Особо важные файлы иногда помещаются в архив независимо от времени их последней модификации. Считается, что для обеспечения надёжности хранения следует иметь 2 – 3 архивных копии всех редакций файлов, подлежащих архивированию.

Архивное копирование тоже может быть полным, инкрементальным и дифференциальным. При организации процесса архивирования делаются полные копии, к которым, как правило, раз в месяц добавляются инкрементальные копии. Количество архивных носителей довольно быстро растёт.

Одним из родоначальников теории хранилищ был Билл Инмон. Современные системы хранения данных содержат архивируемую информацию на текущий момент, позволяют возвращаться на день, неделю, на 30, 90 и более дней назад, что соответствует периодам обновления данных в архивах.

Рассмотрим эти виды архивов подробнее.

*Рабочие архивы* служат для автоматической записи создаваемых постоянных или временных данных, в дальнейшем не используемых или переходящих в долговременные данные. Их рекомендуется создавать и актуализировать непосредственно по окончании ввода порции данных или смены. Рабочие архивы формируются на технологические материалы и БД, подготавливаемые, редактируемые и оперативные документы и создаются в отдельных каталогах на данном или другом компьютере, сервере и перезаписываемых внешних носителях данных.

В качестве рабочих копий для обслуживания пользователей, и распространения в качестве издательской продукции (дистрибутивные копии) используют позитивные микроформы.

*Страховые архивы* используют для повышения надёжности и долговременного хранения данных, представляющих особую ценность или имеющих статус ограниченного доступа. К ним относятся электронные каталоги, базы и банки данных, программные продукты, полнотекстовые и мультимедийные и административные (документооборот, бухгалтерия, кадры) данные.

В страховых (архивных) фондах хранят эталонные негативы первого поколения (мастер-негативы), используемые при микрофильмировании рукописей, архивных материалов и редких изданий. Специалисты предлагают создавать современные страховые архивы на оптических компакт-дисках.

Процесс архивации данных обычно занимает от 5 до 30 минут, что не является серьёзной потерей времени для пользователей, особенно с учётом

того, что время, необходимое даже для частичного восстановления утерянных данных, исчисляется часами, а порой и днями.

**Разархивирование** – процесс точного восстановления машиночитаемой информации, ранее сжатой и хранящейся в файле-архиве.

В организациях используют программно-технические средства записи (дозаписи, обновления, «горячей» замены), долговременного хранения и последующего считывания различных видов машиночитаемой информации на внешних носителях информации (магнитных лентах, ZIP, CD-ROM, CD-R, CD-RW, DVD-ROM, DVD-R, DVD-RW, сменных жёстких дисках и др.).

*ZIP-накопители* представляют сменные магнитные или магнитооптические диски размером с 3,5” дискету, имеющие высокую плотность записи (100 Мб – 2 Гб) и быстродействие до 7 Мб/с. Первые обеспечивают длительность хранения данных до 5 лет. Последние обладают повышенной надёжностью хранения данных и длительностью до 30 лет без перезаписи.

Традиционно используются накопители с технологией магнитной записи/считывания данных на магнитной ленте – *стримеры* (англ. «streamingtype»), позволяющие записывать на одну кассету от десятков Мб до 100 Г. Ленточные библиотеки или библиотеки на магнитных лентах предназначены для автоматизированного резервного копирования данных. Основным недостатком их является последовательный (медленный) доступ к данным и относительно невысокая надёжность носителя.

В последнее время для этих целей используют различные компакт-диски (CD, DVD). Они дешевле сменных магнитных и магнитооптических дисков, не требуют защиты от воздействия магнитных полей и обеспечивают практически мгновенное позиционирование считывающих головок в нужном месте диска, что позволяет гораздо быстрее считывать информацию, чем при использовании накопителей на магнитной ленте.

Ведутся разработки по созданию более ёмких, компактных и надёжных носителей информации (иные виды компакт-дисков, голографические накопители, флэш-память и др.). Основной проблемой широкого внедрения новых носителей является отсутствие уверенности у пользователей (да и у их создателей), что подобные устройства позволят долговременно хранить и сохранять записанные на них ЭИР. Пока ещё разработчики не могут заранее точно и однозначно назвать такие данные. В связи с этим появляются различные, порой противоречивые, сведения. Например, в их документах указывается срок жизни (и хранения данных) компакт-дисков от нескольких десятков до пятидесяти и даже ста лет.

Данные в архиве могут размещаться в сжатом или несжатом (первичном) состоянии.

Для упаковки файлов используются специальные программы-архиваторы, каждая из которых вместо одного или нескольких файлов создаёт один архивный файл в том или ином формате ассоциированным с соответствующим расширением. Одной из первых программ-упаковщиков был созданный фирмой Inc.SEA в 1985 году архиватор ARC. В 1989 году фирма PKWARE представила архиватор PKZIP и разархиватор PKUNZIP. В

1990 году появился, созданный Робертом Янгом (Robert Jung), архиватор ARJ. За ним архиватор RAR, созданный в середине 90-х годов XX века в России.

Ныне наиболее часто используются программы-архиваторы: ZIP, ARJ, RAR, WINZIP, WINRAR и другие, осуществляющие физическое сжатие длины записей. Данный приём с помощью специальных методов кодирования (статического или динамического) позволяет сократить объём данных на носителе от полутора до пяти раз. Простейший способ архивирования заключается в размещении копий важных данных и программ на том же носителе, например, магнитном диске в специально созданной директории. Он требует достаточного свободного пространства на диске и не защищает в случае выхода из строя этого диска или компьютера.

В архиваторах используются режимы динамического и статического сжатия. *Динамическое сжатие* характеризуется возможностью восстановления данных в исходную форму в процессе считывания их соответствующими устройствами компьютера. *Статически сжатые данные* могут быть считаны только после их полного восстановления (разархивации).

Архиваторы имеют удобный интерфейс пользователя, позволяют создавать многотомные и «самораспаковывающиеся» архивы (с расширением «.EXE»), производить иные операции. Для распаковки самораспаковывающегося архива достаточно запустить его как программу.

Строгих критериев, позволяющих считать один из названных архиватор лучше другого, не существует. Они имеют приблизительно одинаковые характеристики.

Основными характеристиками архиватора являются:

- степень сжатия файла (отношение размера исходного файла к размеру упакованного);
- скорость работы;
- сервис (набор функций архиватора).

Все сервисы программ-архиваторов исполняются с помощью специальных команд и ключей, описание большинства из которых появляется при запуске программы с ключом «h» или «?». Ключ обозначается с помощью «слежа» (/), например, «arg/?» или «pkzip/h». В последнее время большую популярность приобрел российский архиватор RAR, имеющий удобный интерфейс пользователя.

Простейшие и самые важные команды:

- архивировать (резервировать) – «a», что означает «addfilestoarchive» (ввести файлы в архив);
- разархивировать – «e», что означает «extractfilesfromarchive» (извлечь файлы из архива).

У пары архиваторов PKZIP и PKUNZIP перед этими и другими командами ставится знак минус (-). Например, для извлечения файлов из архива по имени «moiprog.zip», следует выполнить следующую команду «pkunzip -moiprog.zip», а для раскрытия архива из файла «programs.arj»

выполняют команду «arjeprograms.arj». Файлы могут добавляться в архив, извлекаться из него, тестироваться, заменяться или уничтожаться в нём, записываться на дискеты с напоминанием их замены при полном заполнении дискеты (так называемый многотомный архив). Для надёжного архивирования в ARJ используется режим тестирования при записи файлов в архив (-jt), при этом архивируемый файл сначала записывается во временный файл, а затем, после проверки, в архив.

В архиве может создаваться та иерархическая структура каталогов и подкаталогов, которая существовала на соответствующем носителе до архивирования. Соответственно, при извлечении из архива эта структура может быть сохранена, в ARJ, например, для этого используется команда «-p1».

С помощью команды «i» на экран монитора можно вывести список файлов, находящихся в архивном файле. Для работы с конкретным архивным файлом могут использоваться пароли. Создания саморазархивируемого модуля в ARJ осуществляется с помощью команды «-je», например, «arja -je (имя создаваемого архива)». С помощью специальной команды «m» можно производить выбор разных методов архивирования, например: без сжатия «0», с наибольшим сжатием «1», с меньшим сжатием, но большей скоростью «2» и «3» и, наконец, с минимальным сжатием, но наибольшей скоростью «4». Такая система применяется для ARJ. При этом команда будет выглядеть, например, следующим образом «arja -jm2 (имя создаваемого архива)».

Для частого выполнения однообразных команд можно создать командный файл, в который записать имя архиватора (разархиватора) и необходимые команды и ключи, например, «с:\arch\arja -r -m2 -jm1 -je1 (имя создаваемого архива)».

ЭИР всё более функционируют в Интернет и Интранет сетях, обеспечивающих совместный доступ пользователей к огромным массивам данных. Массивы данных в Интернете хранятся на подключённых к нему серверах. Хранить всю информацию только на одном сервере нецелесообразно, так как выход его из строя приводит к нарушению работы сети в целом.

Одним из способов оптимизации методов хранения является создание корпоративных хранилищ данных и организация нескольких (зеркальных) серверов, хранящих совершенно одинаковые программы и данные, что позволяет не только сохранять информацию, но и обеспечивать бесперебойную работу пользователей с интересующими их данными.

Другим вариантом является создание в сети распределённых баз данных, доступ к которым может быть обеспечен с любых компьютеров сети. Такой метод наиболее целесообразен в ЛВС, где компьютеры находятся на значительном удалении друг от друга, а также в глобальных сетях Интернет. Удобство его объясняется и теми факторами, что, во-первых, при обращении пользователя к необходимой ему информации не требуется соединяться с общим сервером, а можно обращаться непосредственно к тому компьютеру сети, на котором располагается информация, генерируемая его

работниками. Во-вторых, именно на таком ПК информация первична, наиболее часто обновляется (актуализируется) и достоверна.

В любом случае для хранения огромных массивов данных на одном сервере стало не хватать ёмкостей обычных накопителей на жёстких магнитных дисках (HDD). Решение проблемы было найдено в применении «батареи» жёстких и/или библиотеки оптических дисков.

Первые из них разработаны в 1987 году в США (Калифорнийский университет) и получили название **RAID** (англ. «Redundant Array of Inexpensive Disks»). Они представляют «этажерку» жёстких дисков (несколько физических дисков, объединенных в одно устройство), управляемое специализированным контроллером и обычно инициализированных для пользователя как один логический диск. Такое решение позволяет распределять основные и системные данные между несколькими носителями (дисками), в том числе дублировать данные – часть его резервируется для обеспечения восстановления данных в случае неисправности дискового массива.

Этот же термин может обозначать массив независимых дисков. В этом случае он может быть сформирован таким образом, чтобы, например, половина ёмкости отводилась под хранение данных, программ и т.п., а другая половина полностью копировала первую. При этом образуются два совершенно одинаковых массива составляющих *«зеркальные» диски*, так называемый *метод отражения* (англ. «mirroring»). Информация записывается на оба диска одновременно и, в аварийной ситуации с первым диском, она будет автоматически считана с другого. Другой способ получил названия *«метод дублирования»* (англ. «duplexing»). Он имеет более высокий уровень избыточности, но свободен от некоторых недостатков предыдущего – каждый диск подключается к собственному контроллеру.

**CD библиотека** (DVD-библиотека) представляет внешний дисковый массив хранения информации. Её можно подключить к корпоративному серверу и, тем самым, увеличить объём дисковой памяти, доступной пользователям в режиме онлайн. К одному или нескольким серверам можно подключить несколько дисковых систем или массивов. Существует информационное хранилище, включающее 55 таких библиотек общей ёмкостью около 3,5 Тб.

Эти устройства называют *«роботизированными библиотеками»*, Juicebox или чейнджерами и используют в локальных, корпоративных и территориальных распределённых сетях. Они вмещают от нескольких до 100, 620 и более компакт-дисков, позволяют поддерживать до 50 виртуальных компакт-дисков для непосредственного электронного копирования на CD/DVD, а также с помощью встроенного жёсткого диска объёмом в несколько десятков Гб. Аналогично осуществляется и автоматическое архивирование массивов, определённых администратором сети, в том числе перенос редко используемых данных на DVD. Вся такая библиотека представляет единую структуру или том, а каждый диск – отдельный каталог в томе.

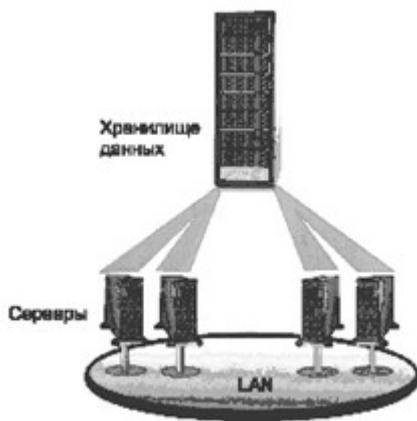


Рис. 12-1. Сеть хранения данных

Подобные технологии позволяют не только повысить устойчивость системы к различным сбоям, но и, моментально переключившись на другую часть массива, поддерживать постоянную работоспособность системы, что наиболее часто используется в работе серверов. Кроме того, в данном случае можно произвести замену вышедшего из строя накопителя на резервный без

отключения электропитания и перезагрузки системы – «горячая» замена. Названные возможности дисковых батарей и библиотек огромных массивов данных (хранилищ информации) в совокупности обеспечивают высокую надёжность хранения данных.

При использовании сетевых технологий для хранения информации применяют различные **информационные хранилища** – базы обобщённых данных, формируемые из множества различных внешних и внутренних источников. Для сохранности ЭИР применяют и *сети хранения данных* (StorageAreaNetwork, SAN). В корпоративных сетях широко используются специализированные **NAS-серверы** (NetworkAttachedStorage), осуществляющие совместимость, интеграцию и администрирование серверов общего назначения и хранение огромных массивов данных (Рис. 12-1).

Основная задача таких хранилищ заключается в обеспечении надёжного централизованного хранения ЭИР и необходимого ПО в соответствии с требованиями к их сохранности и защите.

В качестве информационных хранилищ используют *RAID* и *CD библиотеки* (в том числе DVD).

*Процесс проектирования системы хранения данных*, обеспечивающей резервное копирование, архивирование, структурированное хранение и восстановление данных в требуемые сроки должен опираться на пофайловый анализ подлежащих хранению данных, рекомендуемый проводить на основе следующей информации о файлах:

- даты создания, модификации, последнего обращения,
- расширение,
- расположение в каталогах файловой системы.

Процесс проектирования системы хранения сетевых данных рекомендуется начинать со сбора и анализа информации о хранящихся в сети данных. По всем серверам и рабочим станциям с критически важными данными необходимо выяснить:

- время работы и требования ко времени восстановления в случае сбоя;
- общий объём установленной дисковой памяти, в т.ч. занятый и свободный объёмы;

- данные о файлах (даты создания, модификации, последнего обращения к ним).

Нужно постараться упорядочить хранящиеся данные, поместив файлы, подлежащие резервному копированию, архивированию и другим видам хранения, в отдельные каталоги. Оценив реальную скорость копирования/восстановления информации, можно уточнить необходимое число накопителей в устройствах хранения данных.

При очень больших объемах информации, подлежащей резервному копированию, архивированию и структурированному хранению, становится неудобно осуществлять мониторинг и администрирование этих процессов непосредственно из ПО. В этом случае его интегрируют со средствами сетевого управления.



## **БОЛЬШИХ ДАННЫХ БОЛЬШЕ НЕ БУДЕТ. ЗАБУДЬТЕ!**

Источник: <http://www.pcweek.ru/ecm/blog/ecm/7863.php>

Автор: Андрей Колесов

В очередном своем отчете "Hype Cycle for Emerging Technologies 2015" (Цикл шумихи для развивающихся технологий) компания Gartner преподнесла сюрприз: в нем исчез хит ИТ-разговоров последних лет – Big Data. Не то, что бы эта шумиха по поводу этой темы прошла свой пик, она просто исчезла из перечня "обсуждаемых технологий".

Разговоры о том, не являются ли Большие Данные мыльным маркетинговым пузырем, шли с момента "запуска" этого термина в жизнь и лишь усиливались по мере усиления шума по поводу этой темы. Что, впрочем, характерно для любого "шумного" новшества на рынке. При этом правильный универсальный ответ на любые подобные сомнения, мне лично видится таким: в любом новом термине есть доля и реальных инноваций, и маркетинговой пропаганды. Нужно внимательно разобраться в сущности вопроса, чтобы отделить одно от другого, и выявить суть "сухого остатка". То, что Big Data исчезли из лексикона Gartner, на мой взгляд, является признанием того, что это был все же именно маркетинговый термин, который должен был своим необычным звучанием привлечь внимание общественности и повести ее за собой. При этом было хорошо заметно, что в значительной части ИТ-общественности, и даже в среде людей, которые вроде бы занимались продвижением Больших Данных в широкие массы, четкое понимание "что это такое и с чем его едят" наблюдалось далеко не всегда (см. например "Нужно ли законодательное регулирование в сфере больших данных" И в то же время, нужно признать и то, что за звучным

маркетинговым термином скрывается и новое содержание, которое будет все в больше и большей степени проникать в нашу реальную жизнь. Эта новая реальность заключает в том, что роль прогнозной аналитики на основе данных, формируемых в расширяющемся информационном пространстве, будет продолжать расти.

Figure 1. Hype Cycle for Emerging Technologies, 2015



Собственно, именно об этом сказали и специалисты Gartner, комментируя исчезновение Big Data из списка перспективных технологий: "Мир переходит от разговоров о Больших данных к реализации этих методов на практике".

По сути Big Data был изначально некоторым зонтичным термином, за которым скрывался целый набор разных целевых задач и методов их решения. Специалисты подчеркивали, что речь идет о новом этапе развития "аналитики", а необычный термин был выбран именно для того, что подчеркнуть, что тема вышла на некоторый новый качественный уровень.

Теперь же, когда общество уже в существенной мере прониклось идеями Больших данных, для возвращения в реальность Gartner предлагает разделить этот общий термин на несколько практических направлений, используя для этого более "содержательные" названия:

- Advanced Analytics and Data Science
- Business Intelligence and Analytics
- Enterprise Information Management
- In-Memory Computing Technology
- Information Infrastructure

Мы долго привыкали к термину Big Data. Интересно: как быстро мы его забудем?



## SKYPE FOR BUSINESS — НОВЫЙ УРОВЕНЬ ПОДДЕРЖКИ ДЕЛОВЫХ КОММУНИКАЦИЙ ОТ MICROSOFT

Источник: <http://www.pcweek.ru/its/article/detail.php?ID=177856>

Поддержка групповой работы и корпоративных коммуникаций – именно это направление применения ИТ является одним из наиболее актуальных для современных предприятий, и неудивительно, что его актуальность постоянно возрастает. Деловой мир уже давно стал глобальным и распределенным, но важно добавить, что при этом он становится все более неформальным и оперативным. Предприятиям и организациям уже недостаточно механизмов поддержки внутреннего взаимодействия сотрудников – им необходимо поддерживать постоянную внешнюю связь с клиентами, поставщиками, партнерами. Это нужно не только гигантским международным компаниям, но и небольшим стартапам: не только по тому, что их проекты часто изначально нацелены на глобальный рынок, но и в силу необходимости поддержки сугубо внутреннего взаимодействия: хотя такая команда может состоять всего из трех человек, физически они могут находиться в разных точках планеты. И сегодня нужны не просто средства общения, а гибкие инструменты, которые выходят за рамки привычных представлений о фиксированных бизнес-процессах и способны обеспечить режим живого взаимодействия людей, разделенных тысячами километров.

Именно для решения подобных задач современных деловых коммуникаций компания Microsoft предлагает организациям (от самых небольших до гигантских) выпущенный нынешней весной продукт Skype for Business (SfB). Отметим сразу – это не новый продукт в семействе ПО корпорации, а серьезное обновление ранее существовавшего решения Microsoft Lync Server и прямой результат интеграции последнего с популярнейшим коммуникационным пользовательским сервисом Skype. Подчеркнем и то, что SfB не позиционируется в качестве замены других широко используемых на рынке средств, таких как SharePoint и Exchange. Предназначенный для своего класса задач, он может эффективно дополнить возможности этих продуктов, в том числе в варианте самой тесной интеграции. Нужно также сказать, что SfB – не единственный в своем роде продукт (это направление в последние годы называют унифицированными коммуникациями), на рынке есть предложения и от других поставщиков. Тем более имеет смысл пояснить, зачем SfB нужен и малым, и большим заказчикам и почему именно он.

### **Нужно ли объяснять, что такое Skype?**

Еще несколько лет назад, чтобы разъяснить заказчику, что такое Lync Server, нужно было организовать специальную презентацию или предоставить специально подготовленные материалы. Сегодня рассказать

о назначении и функционале SfB можно апеллируя к хорошо всем знакомому коммуникационному сервису Skype – в той или иной мере его используют в повседневной жизни миллионы компьютерных пользователей. Его назначение – коммуникации в реальном времени с использованием двух основных функций: голосовой связи (по традиции ее продолжают называть «телефонной»), дополненной возможностями видеосвязи и многосторонних телеконференций, и обмена текстовыми мгновенными сообщениями. Но в отличие от традиционной телефонии, реализованной на принципе физической коммутации прямых каналов связи (при каждом сеансе связи с помощью серии соединений создается как бы прямой физический провод между абонентами), в данном случае формируется виртуальное соединение с помощью пакетных Интернет-технологий (то, что называется IP-телефония, или в более общем варианте – VoIP, Voice over IP).

Возможность реализации такой идеи для голосовой связи на теоретическом уровне была осознана еще в начале 90-х (собственно, на этой же идее пакетной передачи информации была тогда уже реализована электронная почта), но в то время пропускная способность Интернета и технические возможности клиентских устройств (преобразование звука и видео в цифровой вид и обратно) не позволяли реализовать ее. Первые практические примеры использования IP-телефонии относятся к концу прошлого века, а настоящим ее прорывом в широкие народные массы стало появление в 2003 г. первой версии известного теперь всем Skype.

Прогресс в области информационно-коммуникационных технологий уже давно привел к тому, что при том же высоком качестве стоимость связи Skype в десятки и даже в сотни раз меньше, чем у традиционной коммутационной телефонии, даже в ее цифровой реализации. При этом она позволяет реализовать также качественно новый функционал, например видеобщение и телеконференции. Важно отметить и принципиально более высокий уровень защиты коммуникаций – весь обмен информацией выполняется в зашифрованном виде (то, что в середине XX века было реализовано в виде ВЧ-связи, доступной только на высшем уровне управления страной). Таким образом, передаваемые сведения являются недоступными для любой третьей стороны, в том числе и для самого провайдера сервиса.

Следующее ключевое достоинство Skype – это возможность использования для связи практически любого современного абонентского устройства (это может быть мобильный телефон, смартфон, планшет, ноутбук, настольный ПК), имеющего подключение к мобильной сети или проводным телефонным каналам связи. Именно эта универсальность (человек, связываясь с нужным ему абонентом, не задумывается о том, какие именно каналы связи будут использоваться, с какого устройства будет звонить он сам и с помощью какого устройства примет звонок его собеседник) дала название зародившемуся во второй половине предыдущего десятилетия корпоративному ИТ-направлению – унифицированные коммуникации (unified communications, UC). В общем случае абоненты

в процессе звонка и общения могут вообще не догадываться, что они используют этот коммуникационный сервис.

Skype совершил настоящую революцию в телефонии, резко расширив ее возможности и географию применения, сделав ее доступной и массовой. Все уже давно привыкли, что онлайн-связь между компьютерами, подключенными к Интернету в любых точках Земли, можно установить совершенно бесплатно без ограничения времени ее использования. А при звонках с телефонов и на телефон стоимость услуг иногда на порядок меньше, чем при применении обычной или мобильной телефонии (причем не только в зарубежном роуминге, но и при локальной связи). Общению людей не мешают государственные границы и уровень «дружественности» разных стран; абоненты могут быть уверены, что их информация «останется между ними», не будет доступна третьим лицам.

Отметим еще один важный момент: Skype не заменяет, а существенно дополняет функционал и возможности других привычных средств поддержки коллективного взаимодействия, таких как облачные хранилища данных и электронная почта (например, OneDrive).

### **Если есть Skype, то зачем же нужен Skype for Business?**

Самый простой ответ таков: затем же, зачем нужны предприятиям SharePoint и Exchange при наличии OneDrive и почтового ящика Outlook...

Публичные общедоступные сервисы, ориентированные на частных пользователей, не очень соответствуют (а зачастую и вовсе не соответствуют) задачам и требованиям компаний. Предприятиям нужны частные (приватные) решения, которые полностью находятся под их собственным контролем и управлением и не зависят от внешнего провайдера. Им нужны средства, которые будут решать именно их задачи с учетом конкретных условий и требований, с нужным им уровнем доступности, производительности, масштабируемости и безопасности. Заказчикам необходимо интегрировать данный сервис в общую корпоративную систему, обеспечить его взаимодействие с различными бизнес-приложениями и инфраструктурными компонентами. Очень часто компаниям требуется расширение функционала сервиса через его доработку на программном уровне.

Таким образом, корпоративным заказчикам нужен надежный, многофункциональный продукт масштаба предприятия, на базе которого они могли бы формировать собственное коммуникационное пространство и которое включало бы не только внутренний контур организации, но и при необходимости выходило за его пределы, охватывая внешних контрагентов (клиентов, партнеров, поставщиков и пр.). Именно таким продуктом является Skype for Business.

Следует понимать, что при всей схожести по классу решаемых задач и пользовательскому интерфейсу с публичным сервисом Skype продукт SfB — это другое решение, изначально ориентированное на корпоративное применение. По сути, SfB — это слияние в одном продукте двух ранее

развивавшихся параллельно и в значительной степени независимо друг от друга линий коммуникационных технологий — Lync Server и Skype.

Возможно, это не случайное совпадение: первый продукт Microsoft под названием Communication Server для решения задач корпоративного синхронного взаимодействия появился, как и Skype, в 2003 г. Потом под этим же именем были выпущены еще две версии (2005 и 2007, каждая с серьезными промежуточными обновлениями), а четвертая версия в 2010 г. появилась уже как Lync Server (от слов link и sync). Этот продукт затем был существенно обновлен в 2013-м.

Таким образом, нынешний Skype for Business Server 2015 — это фактически уже шестая версия продукта. То есть в данном случае речь идет о проверенной временем технологии, причем занимающей лидирующие позиции на рынке корпоративных унифицированных коммуникаций, пользующейся популярностью и доверием корпоративных клиентов. Смена же названия отражает важную реперную точку в развитии данной коммуникационной технологии: интеграцию существовавших ранее независимо и параллельно друг с другом двух ее направлений — потребительского и корпоративного.

Фактически SfB объединяет в себе хорошо известный функционал и дизайн Skype с корпоративными возможностями Lync, а также возможности расширения базового функционала продукта и его интеграции с другими бизнес-приложениями. От Lync новая версия SfB, в частности, получила средства проведения онлайн-конференций, усиленную безопасность, легкость интеграции в корпоративную среду, инструменты администрирования и настройки в соответствии с корпоративными политиками. Компания может сама выбрать, с каким вариантом пользовательского интерфейса будут работать ее сотрудники — в стиле Skype или в традиционном Lync. При этом пользователи могут общаться в среде этого решения не только с людьми, включенными в корпоративную адресную книгу, но также и с абонентами публичного сервиса (разумеется, если это допускается внутренними правилами компании).

### **Расширенные сервисы для организации конференций и собраний**

Одно из направлений развития Skype for Business — организация и проведение многостороннего одновременного общения людей в виде виртуальных собраний. Реализация этих возможностей идет в том числе в виде создания онлайн-сервисов Office 365. Так, летом этого года Microsoft объявила о доступности технической предварительной версии ряда таких сервисов для корпоративных клиентов Office 365:

- **Skype Meeting Broadcast**, доступный пользователям по всему миру, позволяет транслировать собрания Skype for Business в Интернете для аудитории до 10000 человек, которые смогут присоединиться к встрече через браузер с любого устройства. Функционал сервиса упрощает организацию больших виртуальных собраний, его предварительная версия поддерживает интеграцию с Bing Pulse для проведения опросов в режиме реального

времени и с Yammer для предоставления возможности участникам общаться во время трансляции;

- **PSTN Conferencing** (доступен пока только в США) предоставляет возможность приглашать людей для участия в собрании Skype for Business в Office 365, используя стационарный или мобильный телефон. Таким образом, сервис позволяет людям присоединиться к онлайн-встречам даже в местах, где отсутствует доступ к Интернету;

- **Cloud PBX with PSTN Calling** (также пока доступен только в США) обеспечивает людям возможность осуществлять в клиенте Skype for Business звонки на традиционные телефоны и управлять этими звонками — удерживать или возобновлять их, а также переключаться между ними. Эта функция построена на базе усовершенствованной корпоративной голосовой технологии, доступной в Lync Server и Skype for Business Server. К концу года Microsoft обещает сделать сервис Cloud PBX доступным для клиентов по всему миру с возможностями настройки использования существующих телефонных линий для входящих и исходящих звонков.

Все эти сервисы выйдут на рынок в окончательном общедоступном варианте до конца нынешнего года. Ближе к этому сроку Microsoft сообщит детали о ценах и порядке лицензирования решения.

Кроме того, Microsoft продолжает расширять сотрудничество с ведущими телекоммуникационными компаниями. Так, уже в этом году целый ряд ее стратегических партнеров (AT&T, BT, Colt, Equinix, Level 3 Communications, Orange Business Services, TATA Communications, Telstra, Verizon и Vodafone) обеспечит в своих сервисах и устройствах прямое подключение Skype for Business для клиентов Office 365 посредством облачного средства Azure ExpressRoute для Office 365, которое позволяет клиентам создавать частные соединения между своими офисами и дата-центрами Microsoft, предлагая при этом более предсказуемую производительность сети, возможность лучше управлять доступностью сети и необходимую надежность с предоставлением выделенного соединения и дополнительной защитой конфиденциальных данных.

Отметим, что если в момент своего рождения двенадцать лет назад Communication Server воспринимался на рынке как младший брат в семействе офисных серверов Microsoft (SharePoint и Exchange), то в последние годы он занял равные позиции в этой «богатырской тройке». Все эти три серверных решения, пересекаясь между собой в минимальной степени по функционалу, сейчас фактически представляют собой интегрированную корпоративную платформу групповой работы и коммуникаций. Особенно частым вариантом совместного использования является вариант Exchange и Skype for Business. Для заказчиков Skype for Business доступен как в виде отдельного продукта по лицензионной модели, так и в составе подписки на Office 365 совместно с другими серверными решениями.

## Почему именно Microsoft Skype for Business

Как мы уже говорили, Skype for Business представляет собой решение класса «корпоративные унифицированные коммуникации» — динамично развивающегося ИТ-направления. Еще несколько лет назад аналитики отмечали, что своеобразие этого ИТ-сегмента рынка заключается в том, что он сформировался в результате слияния течений из двух разных, ранее практически не пересекавшихся ИТ-областей — коммуникационно-сетевой и программной. Причем само появление софтверной «струи» фактически было связано с выходом на этот рынок корпорации Microsoft со своим Communication Server 2003. Поначалу эксперты довольно скептически оценивали шансы этого продукта на успех в борьбе с традиционными лидерами этого направления. Однако, согласно ИС-исследованиями Gartner, уже версия 2007 данного продукта позволила Microsoft занять первую позицию в тройке лидеров, а в последующие годы уверенно удерживать это лидерство.

Анализируя причины такого успеха Microsoft, аналитики отмечали в качестве преимущества ее продукта именно программно-виртуальный подход к решению коммуникационных задач (то, что в последние годы относят к категории программно-конфигурируемых решений) и независимость от используемой аппаратной части, в то время как продукты конкурентов в сильной степени ориентированы на применение собственных технических средств. При этом сильной стороной Microsoft традиционно является высокий уровень интеграции всех компонентов его софтверной платформы, особенно в рамках ее клиентско-серверного офисного семейства. Курс на сближение с пользующимся огромной популярностью во всем мире сервисом Skype, возможность использования в SfB хорошо уже знакомого интерфейса, должны сократить затраты предприятий на обучение и техническую поддержку сотрудников при внедрении и эксплуатации решения.

Уже с выпуском предшественников SfB в 2007 и 2010 гг. технологии унифицированных коммуникаций Microsoft на практике показали свою высокую производительность, масштабируемость и надежность: продукт обеспечивал поддержку до нескольких тысяч активных пользователей на один сервер, а в крупных международных распределенных компаниях были реализованы проекты с числом пользователей в сотни тысяч. В последние годы росла популярность Lync Server и в России, причем среди его заказчиков есть и коммерческие компании, и государственные организации.

Важным плюсом SfB является возможность его реализации в двух вариантах — в виде традиционного программного продукта, а также в виде онлайн-сервиса от самой корпорации Microsoft, что в том числе позволяет заказчикам использовать модель гибридных облаков. Более того, свои облачные сервисы SfB могут создавать и независимые провайдеры (примеры такой практики уже имеются и в мире, и в нашей стране).

Как обычно, Microsoft предлагает возможность и независимым разработчикам строить бизнес на основе ее технологий: с помощью соответствующего SDK можно создавать собственные клиентские приложения, использующие функционал сервера SfB, разработчики могут выполнять интеграцию своего ПО с системой как на клиентском, так и на серверном уровне, а на основе открытого API можно использовать функции SfB в веб-приложениях. В ближайшее время такие же возможности появятся и для мобильных приложений.



## О РЕШЕНИИ КЛАССА “БЕЗОПАСНОСТЬ КАК СЕРВИС” (SECaaS)

Источник: <http://www.pcweek.ru/its/article/detail.php?ID=179595>

*В преддверии намеченного на 24 ноября форума Russian Information Services Summit 2015 редакция PC Week/RE обратилась к ключевым спикерам конференции с предложением поделиться своим мнением относительно современного уровня распространения сервисного подхода, внутренних и внешних корпоративных инфраструктурных и прикладных ИТ-сервисов в России, проанализировать основные движители и препятствия в области практического применения аутсорсинга, облаков и других видов сервисов в ИТ и основанных на ИТ прикладных задачах и рассказать о том, какую тему докладчик собирается осветить в своем выступлении на RISS'2015. Вот что нам сообщил **Юрий Бражников**, генеральный директор по России и СНГ компании *5nine Software Inc.**

Сервисный подход в эксплуатации корпоративной ИТ-инфраструктуры в России достаточно распространён. Множество крупных компаний выделили свои ИТ-подразделения в отдельные компании и работают с ними на основе сервисных контрактов наравне с другими участниками рынка. Аутсорсинг, наверное, более распространён в промышленности, в меньшей степени в финансах, по понятным причинам. Решаемые задачи и степень интеграции с ИТ-инфраструктурой и корпоративными информационными системами зависят от конкретного предприятия. Решение вопросов информационной безопасности пока у нас не всегда соответствуют требованиям и вызовам современного состояния инфраструктуры, особенно, частных и публичных облаков. Новые угрозы, появившиеся с широким внедрением технологий виртуализации, пока широко не осознаны и решаются по аналогии с физическими средами, что концептуально не верно. Виртуализация принесла не только много преимуществ, но и новых угроз, которые должны быть предотвращены путем внедрения современных

технологий информационной безопасности. Например, при помощи защиты виртуальной инфраструктуры на уровне гипервизора, а не классической концепции endpoint security.

Есть несколько трендов, существенно влияющих на внедрение сервисного подхода к реализации ИТ стратегии предприятия. Во-первых, это существенное развитие технологий виртуализации и удалённого доступа. Виртуальные среды могут обеспечить большую часть потребностей современного предприятия, даже с решением задач поддержки высоконагруженных серверов, больших данных и отказоустойчивых конфигураций. Широкое распространение ШПД и VPN и падающие конкурентные цены тоже способствуют переносу нагрузок в ЦОД сервис-провайдера. Усложнение финансового положения предприятий заставляет просчитывать варианты переноса части задач на аутсорсинг.

Возможность использования сторонних ЦОДов во многом определяется законодательством о персональных данных, их сборе и обработке на территории РФ.

При переносе задач из корпоративного ЦОДа в облако сервис-провайдера важнейшей задачей является обеспечение безопасности данных и приложений. Часто это основной фактор отказа от использования коммерчески привлекательных предложений по аутсорсингу бизнес-процессов. Решение, о котором я собираюсь рассказать на конференции, помогает значительно повысить безопасность инфраструктуры предприятия, перенесённой в сторонний ЦОД, и получить доступ к управлению настройками изоляции и обеспечения защиты от угроз на уровне приложений. С другой стороны, это решение поможет сервис-провайдерам предоставлять новый вид услуг — «безопасность как сервис» (SECaaS). Это крайне актуальная сейчас тема.



## **ОПТИМИЗАЦИЯ РАБОТЫ С ДОКУМЕНТАМИ: КАК СНИЗИТЬ РАСХОДЫ НА ТРЕТЬ**

Источник: <http://www.pcweek.ru/its/article/detail.php?ID=178573>

Широкое распространение СЭД в корпоративных структурах не избавило их от необходимости в организации работы с бумажными документами. Последние остаются важной частью многих бизнес-процессов, а их печать, сканирование, обработка – существенной статьёй расходов. Управлять такими расходами эффективно – непростая задача, для решения которой имеет смысл воспользоваться услугами сторонней специализированной компании.

Услуги по эффективной организации работы с документами предоставляет, в частности, японская компания KYOCERA Document Solutions. Предлагаемое ею универсальное решение «Система управления документооборотом» (Managed Document Services; MDS), включающее услуги по оптимизации ИТ-инфраструктуры для работы с документами, а также специализированное ПО для ИТ-отдела и пользователей с разными задачами и правами доступа к документам, позволяет сократить связанные с документооборотом расходы в среднем на 30–35%. Об этом свидетельствует опыт уже реализованных проектов внедрения MDS, в том числе в российских компаниях – ювелирной компании АДАМАС, страховой группе МСК, ДИТ г. Москвы и др.

### **На пути к оптимизации**

Полноценное внедрение решения MDS предполагает пять этапов: предварительный анализ в компании инфраструктуры печати, проработка индивидуального проекта ее оптимизации, внедрение специализированного ПО, мониторинг эффективности новой системы поддержки документооборота и, наконец, ее оптимизация в режиме реального времени в соответствии с динамикой изменения потребностей бизнес-пользователей.

Каждый такой проект индивидуален, поскольку выполняется с учетом конкретных задач и интересов заказчика. При этом оптимизация парка устройств (принтеров, МФУ) не предполагает их обязательную замену, даже если в компании представлены модели разных вендоров. Перейти на устройства KYOCERA, существенно выигрывающие по стоимости отпечатка у аналогичных моделей других вендоров, можно позднее по мере возникновения насущной необходимости в этом.

### **Программные компоненты MDS и их назначение**

Важная составная часть MDS-решения – программные компоненты, предназначенные как для оценки состояния и мониторинга функционирования инфраструктуры поддержки документооборота, так и для упрощения различного рода пользовательских задач.

Так, для анализа и инвентаризации действующего парка оборудования применяется ПО KYOanalyser, которое позволяет получить моментальный срез текущего состояния парка офисной техники, включая информацию о количестве отпечатков, полученных на каждом отдельном устройстве, а при повторном сканировании парка – объем печати за прошедший период.

Программа Net Admin обеспечивает круглосуточный непрерывный мониторинг парка устройств (до 5000 единиц), упрощая сбор информации о них и формирование ежемесячных отчетов по объемам печати и произошедшим инцидентам.

Компонент KYOroute Server, который устанавливается на принт-сервере, оптимизирует распределение нагрузки между печатающими устройствами, направляя задания на наиболее подходящие из них, а также передает на сервер статистику по выполненным заданиям. Оптимизация нагрузки осуществляется на основе принятых политик печати в отношении

отдельных пользователей и конкретных документов по заданным критериям или в зависимости от исходных характеристик обрабатываемого документа.

Ряд программных модулей предназначен для управления устройствами KYOCERA. Так, приложение KYOCERA Net Viewer обеспечивает удаленный доступ к каждой единице оборудования, подключенного к единой сети, реализуя постоянный мониторинг устройств с отображением их текущего состояния. Приложение способно работать в рамках локальной корпоративной сети, без выхода в Интернет. Поддерживаемый парк – до 100 устройств.

Драйвер KX Driver обеспечивает единый пользовательский интерфейс для устройств, поддерживающих языки управления PCL XL, PCL 5e, PostScript, что сводит к минимуму обращения пользователей за помощью, а персональная панель PanelPlus позволяет настроить панель управления каждого устройства KYOCERA под индивидуальные требования пользователя.

В составе набора специализированного ПО также предусмотрены утилиты, ориентированные на определенные профессиональные сферы. Для учебных заведений будет полезна утилита Teaching Assistant – она предназначена для сканирования и автоматизированной обработки бланков с учебными тестами с выдачей оценочных результатов по каждому учащемуся. Применение данного инструмента позволяет многократно сократить время, обычно затрачиваемое на просмотр бланков и подведение итогов тестирования.

Автомобильные дилеры с помощью программного модуля KyоEasyPrint могут автоматизировать печать комплектов документов, требующих нетривиальной предпечатной обработки.

С помощью программного компонента Mobile Print отправить файл на печать или задание на сканирование документа можно непосредственно с планшета или мобильного телефона. Утилита поддерживает iOS- и Android-устройства, а также широкий набор форматов документов (PDF, TXT, JPEG, TIFF, XPS и др.).

Безопасную печать документов (один из важнейших аспектов использования ИТ в бизнесе) позволяет реализовать модуль Print&Follow SE. В этом случае один из сетевых принтеров выполняет функции сервера хранения отправленных на печать заданий, а получить распечатку документа пользователь может на любом подключенном к сети устройстве, пройдя процедуру авторизации. На обеспечение безопасной печати нацелен и другой специализированный компонент – Net Manager, предполагающий авторизацию пользователей на устройствах с помощью карточки или ПИН-кода и предоставляющий широкий спектр возможностей для мониторинга печати.

Ряд задач по управлению инфраструктурой печати и сканирования документов можно отнести к разряду универсальных для любых заказчиков. Для этих задач также предусмотрены соответствующие программные инструменты.

## **О сервисном контракте**

Одним из важных моментов при принятии решения о передаче задачи оптимизации процессов работы с документами на аутсорсинг является и сам сервисный контракт, его наполнение. MDS-контракт с компанией KYOCERA хорошо проработан и включает в себя, в частности, круглосуточную поддержку заказчика, выделение персонального сервис-менеджера, возможность предоставления в пользование заказчику оборудования KYOCERA, замену расходных материалов и целый ряд других услуг, включая регулярную отчетность перед заказчиком по объемам выполненных работ. Последний аспект особенно важен, поскольку повышает степень доверия заказчика к исполнителю, дает возможность заказчику четко понимать, на что именно он расходует свои средства.

Подробная информация на сайте: [www.kyocera-mds.ru](http://www.kyocera-mds.ru)

# ЗМІСТ

Передмова.....	1
К вопросу об организации защиты информации при длительном хранении документации с использованием интегрированных (гибридных) технологий.....	2
Система маркировки электронных носителей в страховом фонде документации.....	6
Технология микрофильмирования для долговременного хранения электронных документов.....	11
Создание электронных архивов – актуальная задача сегодняшнего дня.....	13
Оцифровка – не гарантия вечной сохранности.....	17
Меры и способы сохранения информации.....	20
Больших Данных больше не будет. Забудьте!.....	29
Skype for Business — новый уровень поддержки деловых коммуникаций от Microsoft.....	31
О решении класса “безопасность как сервис” (SECaaS).....	37
Оптимизация работы с документами: как снизить расходы на треть...	38