ПЕРЕДМОВА

Випуск дайджесту присвячено досвіду провідних країн світу щодо проведення мікрофільмування, як основи створення страхових фондів, а також забезпеченню надійності зберігання інформаційних ресурсів.

У публікації «Северо-Восточный Центр консервации документов. Бостон, штат Массачусетс, США» розповідається що серед досягнень цифрової революції мікрофільмування спокійно зберігає свій статус і високо цінується - тобто широко практикується в стратегії переформатування документації для консервації. Неабиякою популярністю мікрофільм користується за свою практичность. На відміну від цифрових носіїв, мікрофільм є продуктом статичним, технологія якого перевірена роками та регулюється національними стандартами. Якщо мікрофільми створюються і зберігаються у відповідності з цими стандартами, такий носій має тривалість життя понад 500 років. Варто також відзначити, що, у зверненні з цифровими даними вимагається використання складних пошукових систем - у свою чергу мікроформа (наприклад, мікрофільм і мікрофіша) можуть бути прочитані безпосередньо неозброєним оком використовуючи тільки світло і збільшення.

Потенціал, закладений в мікроформах за загальним визнанням, не йде ні в яке порівняння з цифровими технологіями.

У публікації «Барьеры на пути утечек данных» розповідається про небачені раніше «інформаційні катастрофи», наприклад публікації сотень тисяч документів WikiLeaks, які дають уявлення про жахливі обсяги даних що можуть бути викрадені з використанням сучасних технологій і до яких наслідків це може призвести. Ще зовсім недавно подій порівнянного масштабу не могло бути в силу існуючих технічних обмежень на обсяги даних, які могли потрапити до рук зловмисників, - просто не було носіїв, що дозволяють вкрасти, наприклад, повний комплект документації на виріб під назвою «нейтронна бомба». Тепер необхідний обсяг даних вкладеться на декількох квадратних міліметрах флеш-пам'яті, і зберігаються вони в цифровій формі, як ніби спеціально створеної для спрощення крадіжок. У підсумку загроза крадіжки даних (data theft) і несанкціонований доступ до даних (data breach) увійшли сьогодні до числа критичних, а для протистояння їм пропонуються у тому числі засоби запобігання витоку даних (Data Leak Prevention, DLP).

У публікації «Подземному хранилищу в Луисвилле, штат Кентукки 10 лет» розповідається про сучасне підземне сховище інформаційних ресурсів в Луісвілле, штат Кентуккі, США.

СЕВЕРО-ВОСТОЧНЫЙ ЦЕНТР КОНСЕРВАЦИИ ДОКУМЕНТОВ

БОСТОН, ШТАТ МАССАЧУСЕТС, США

Источник: http://www.nedcc.org/resources/leaflets/6Reformatting/01MicrofilmAndMicrofiche.php. Автор: Стив Далтон (бывший директор полевой службы Северо-Восточного Центра консервации документов

Введение

Среди достижений цифровой революции микрофильмирование спокойно сохраняет свой статус и высоко ценится – то есть широко практикуется в стратегии переформатирования документации для консервации. Неугасающей популярностью микрофильм пользуется из-за своей практичности. В отличие от цифровых носителей, микрофильм является продуктом статичным, проверенная годами технология, которая регулируется национальными стандартами. Если микрофильмы создаются и хранятся в соответствии с этими стандартами, такой носитель имеет продолжительность жизни 500 с лишним лет. Стоит также отметить, что, в обращении с цифровыми данными требуется использование сложных поисковых систем – в свою очередь микроформа (например, микрофильм и микрофиша) могут быть непосредственно прочитаны невооруженным глазом используя только свет и увеличение.

Потенциал, заложенный в микроформах по общему признанию не идет ни в какое сравнение с цифровыми технологиями. Тем не менее, микроформа может способствовать расширению доступа к информации, которая иначе была бы недоступна, потому что исходный элемент находится на сайте или на цифровом носителе, который является уязвимым к повреждениям или может привести к потере информации при использовании. Кроме того, микроформа является относительно недорогой в производстве и воспроизведении.

Одним из ключевых показателей сохраняющейся актуальности микрофильмирования – это его постоянная поддержка на национальном уровне.

Национальный гуманитарный фонд

Национальный гуманитарный фонд (НГФ) продолжает поддерживать усилия по сохранению и микрофильмированию хрупких экземпляров книг и изданий.

В 1989 году Конгресс США одобрил инициативу НГФ по реализации двадцатилетней программы сохранения интеллектуального наследия содержащей около трех миллионов томов из хрупких коллекций по всей территории Соединенных Штатов. Джордж Фарр, директор отдела НГФ, доложил о сохранении и доступности материалов семидесяти двух библиотек

и библиотечных консорциумов, расположенных в сорока двух государствах, которые участвовали в проектах по сохранению и микрофильмированию фондов и до сих пор прилагают совместные усилия. По предположительным оценкам к завершению проекта будут замикрофильмированы 862 418 томов.

Основа микрофильма

На протяжении многих лет микроформа изготавливалась на различной основе, на которую наносится светочувствительный слой микрофильма, в том числе с использованием нитрат целлюлозы, ацетат целлюлозы и полиэстера.

Нитрат целлюлоза в основе микроформы как и другие производные нитрата целлюлозы, легко воспламеняются, подвержены выделению вредных газов при длительном времени хранения. К началу 1950-х годов промышленное производство пленки на основе нитрата целлюлозы прекратилось.

Ацетат целлюлоза в основе микроформы признана безопасной пленочной основой, негорючей, но со временем ухудшающей свои качества по срокам и гарантиям хранения. Этот процесс деградации ускоряется при неправильном хранении микрофильмов на основе ацетата. Несмотря на большое распространение микрофильмов на основе ацетата, ацетат пленка не подходит в качестве носителя для долгосрочного сохранения микроформ.

Полиэстер в настоящее время является единственной надежной базовой основой для микрофильмов, которая рекомендуется для длительного хранения. Этот материал стабильный и прочный, черно-белая полиэфирная пленка имеет срок службы 500 лет при надлежащих условиях хранения.

Типы микроформ

Микроформы изготавливают в различных форматах. Наиболее известными из них являются 16 мм или 35 мм рулонные микрофильмы и микрофиши, последние напоминают пластиковую карту на форматной пленке, микроизображения на которой расположены построчно или колонками. Рулонный микрофильм 16 мм или 35 мм формата, можно разрезать на короткие полосы для монтажа в джеккеты, апертурные карты или использовать для перевода в цифровую форму для информационных систем.

Три типа фильма распространены в коллекциях микроформ: серебряно-желатинового, диазотипного и везикулярного.

Серебряно-желатиновые (или галогенидосеребряные) микрофильмы

Такие микрофильмы основаны на знакомой нам технологии черно-белой фотографии и являются единственными, подходящими для долгосрочного хранения. Изображение получается путем светочувствительных соединений серебра в эмульсии пленки к свету. Оригинальный вид серебряно-желатинового микрофильма почти всегда негативный, но позитивные или негативные дубликаты могут быть скопированы с оригинала. Эмульсионная сторона такого микрофильма матовая, в то время как не эмульсионная сторона глянцевая. Современные

серебряно-желатиновые пленки являются долгосрочными при соответствующих условиях хранения и гарантированного их использования при изъятии из хранилищ.

Диазографическая пленка (диазопленка)

Это фотографическая светочувствительная пленка, на которой могут быть один или несколько светочувствительных слоев, которые содержат соли диазония в слое полимерного покрытия, при реагировании с красителем в светочувствительных слоях или в обрабатывающем растворе и получают четкие, плотные цвета. Формирование позитивного изображения происходит в результате образования красителя на неэкспонированных участках.

Воздействие ультрафиолетового излучения вызывает разрыв и потерю связей между молекулами солей. В процессе копирования диазотипная пленка экспонируется при контактной печати с оригиналом. Кислоты, используемые в покрытии для предотвращения реакции перетекания цветов нейтрализуются воздействием сильной щелочи (обычно аммиак). Дублирование изображений с оригинала выполняется напрямую. Цвет изображения зависит от состава солей диазония и составов, которые используются при обработке. Диазофильм изготовляется в различных цветах, включая черный. Он может иметь ацетат или полиэфирную основы, хотя полиэстер становится все более популярным из-за его стабильности и устойчивости к факторам окружающей среды. Сопротивление к выцветанию зависит от выбора соли и красителя, при этом черный требует комбинации красителей. Диазофильм является достаточно стабильным, но в конце концов изображение может исчезать даже в темноте.

Везикулярный микрофильм

Это прозрачная светочувствительная пленка состоящая из одного или нескольких светочувствительных слоев, которые содержат соли диазония в термопластичном материале. Тиражирование таких микроформ, не содержащих солей (галогенидов) серебра, происходит путем формирования негативного изображения в результате распада солей при нагревании и как следствие образования в экспонированном слое пузырьков газа, которые и формируют скрытое изображение, видимое после термической обработке. Его преимущества в том, что соли диазония производят азот при распаде под воздействием УФ-излучения. Микрофильм изготавливают путем контактной печати с оригиналом, и изображение проявляется при нагревании пленки. Нагрев мгновенно смягчает материал основы и вызывает расширение азота с образованием мелких пузырьков, которые остаются при охлаждении пленки. Обычно остаточный светочувствительный материал затем фиксируют экспонированием пленки к ультрафиолетовому излучению, в результате чего происходит полное затухание солей диазония. Падающий на пленку свет проходит через ее прозрачные участки, но рассеивается и отражается за счет пузырьков, в результате чего те области с пузырьками и проявляются видимыми. Размер изображения всегда обладают слегка приподнятыми областями. Везикулярная пленка может быть легко повреждена при механическом давлении, которое разрушает пузырьки. Еще одна уязвимость

везикулярного фильма состоит в возможной миграции пузырьков или их движении внутри термопластичного материала. При высоких температурах материал основы микрофильма смягчается и газ, содержащийся в пузырьках расширяется. Если пузырьки увеличиваются в размерах, они могут разорваться, оставляя пятна в слое прозрачной пленки, где изображение было ранее видимым. Сохранности везикулярного фильма может быть нанесен ущерб, при температурах ниже 167 ° F (75°C), Американский национальный институт стандартов (ANSI) считает такую температуру допустимой, поэтому затраты на производство такой пленки является оправданными.

Альтернативные виды микрофильмов

В последние годы в сообществе вырос интерес к цветным и полутоновым микроформам. Краткое обсуждение этих типов микроформ приведено ниже.

Цветные микрофильмы и микрофиши

Хотя есть много потенциальных применений для цветных микроформ, использование этих технологий не может точно гарантировать сохранение носителя, потому что продолжительность жизни большинства 35 мм цветных микрофильмов далека от черно-белых. Тем не менее, есть один положительный пример - цветная прозрачная пленка, Ilfochrome, которая считается весьма перспективной для хранения. В отличие от других цветных микрофильмов, которые отображают цветность во время обработки изображения, этот фильм имеет цветовой слой, встроеный непосредственно в ее эмульсию. Тестирование на стойкость фотографий института (Rochester, NY) предполагает, что продолжительность срока службы красителей превосходный – возможно от 300 до 500 лет – с условием что микрофильм не подвергался воздействию света. Исследования также показывают, что полиэфирная основа фильма может быть менее стойкой к разрушению, чем некоторые другие основы полиэфира. Тем не менее, продолжительность срока хранения может быть целых 200 лет и более. Тестирования светостойкости (важно оценить постоянство в использовании) до сих пор не проводилось.

Непрерывный спектр тонов микрофильма

Качественное черно-белое микрофильмирование дает высокую контрастность с превосходным разрешением текста. К сожалению, высокая контрастность микрофильмов обычно не охватывает широкий спектр серых тонов, таким образом теряется воспроизведение полутоновых фотографических изображений и иллюстраций. Для создания полутоновых микрофильмов могут быть использованы различные способы. Например, один поставщик использует пленку Kodak 2470 при прямом копировании на серебряно-желатиновый микрофильм и выдерживает фильм в течение длительного времени (время экспозиции может различаться), под галогенной лампой. Другой, использует пленку Fuji SuperHR20 с нормальной скоростью затвора и непрерывным спектром тонов достигается результ прежде всего за счет обработки в низкой контрастности, чем нормальная скорость обработки. В любом случае широкий диапазон серых тонов эффективно используется.

Стандарты для микрофильмов

Микроформы используются для долгосрочного сохранения информации и требуют тщательного производства и экспертизы в дополнение к хорошо контролируемым условиям хранения и обращения. Кураторы и менеджеры коллекций, которые используют микрофильмирование, должны установить нормы и правила для поставщиков, предоставляющих услуги по микрофильмированию, характеристики которых удовлетворяют требованиям потребителей к их использованию и сохранности. Стандарты Ассоциации по распространению информации (ANSI) и управлению образами (AIIM), а также спецификации, разработанные Группой научных библиотек (RLG) и Библиотекой Конгресса США, дают полезные рекомендации. Требования каждого учреждения могут отличаться, однако, и эти требования должны быть указаны и систематически контролироваться для защиты себя и коллекций фондов в интересах учреждения.

Каталог Стандартов AIIM может быть просмотрен в Интернете по адресу: www.aiim.org/industry/standards/97stdcat.htm.

Контроль качества

Для того, чтобы добиться соответствия требований, касающихся качества пленки производители микрофильмов должны тщательно проверять обработку первого поколения фильмов, в том числе: покадровый осмотр для обнаружения ошибки при съемке (например, проблем с фокусировкой передержания или недодержания изображений, и др.), видимых дефектов (например, отпечатков пальцев, царапин и т.д.), отсутствие страниц, и число соединений (клеевых швов) на каждом рулоне; показаний плотности, интерпретируется в соответствии с руководящими принципами стандартизации; определения наличия остаточного тиосульфата (см. ANSI / NAPM IT9.1-1996). Качество микрофильмирования должно обеспечивать допустимые показания плотности второго и третьего поколений копий микрофильма, для этого проверке на четкость и контрастность подвергают все копии. Результаты всех операций по контролю качества выполняются производителем и должны быть представлены на контроль качества в форме отчета.

Ответственность за контроль качества не должна лежать исключительно на производителе пленки. Микрофильмирующее учреждение должно также проводить свои собственные проверки с целью определения соответствия нормам стандартов. Практическое руководство можно найти в Справочнике по микрофильмированию Приложение 18 RLG (перечисленны в библиографии).

Среда для хранения данных

Температура и относительная влажность

В общем, требования к микроформам напоминают условия хранения к другим фотоматериалам. Круглогодичная относительная влажность ниже 50 % рекомендуется для всех типов пленки. Верхний предел 40 % рекомендуется для серебряно-желатиновых пленок в целях минимизации

вероятности появления микроскопического пятна окисления из серебра (иногда называемого "корь"). Температура не должна превышать 70 ° F (21 °C); более низкие параметры температуры являются предпочтительными. Оригиналы микрофильмов должны храниться при максимумах 65 ° F (18 °C), 35 % относительной влажности ± 5 %. ANSI / NAPM IT9.11-1993 и ANSI / PIMA IT9.2-1998, описывающим условия для архивного хранения пленки.

Для длительного хранения коллекций микрофильмов обеспечиваются жесткие рамки температурных показателей. Для сохранности оригинала и обеспечения сохранности информации на микрофильме перед их изъятием из хранилища, выносом за пределы складских помещений, просмотром и чтением необходим процесс акклиматизации к более высоким показателям температуры. Этот процесс необходим для постепенного повышения температуры после хранения микрофильмов. Быстрые перепады температуры при выносе микрофильма из холодного помещения в теплое может привести к появлению конденсации влаги на поверхности пленок или коробок для хранения (тары).

Кондиционирование помещений должно быть на основе хладагента. Вентилирующие системы могут приводить к попаданию мелких частиц пыли на поверхность микрофильма, которые потом приводят к появлению царапин на эмульсионном слое. Помещение для хранения должно быть обеспечено системой очистки воздуха, стабилизацией влажности и контролем содержания вредных веществ. Пленка особенно восприимчива к химическим и абразивным повреждениям и попадание в помещения для хранения испарений воды или химических растворов недопустимо. Как и при хранении бумажных артефактов, для долгосрочного хранения микрофильмов колебания всех показателей температурного и влажностного режимов должны контролироваться. Относительная влажность и температура для коллекций микрофильмов при долговременном хранении не должна изменяться более чем на ± 5 %, а ± 3 % является предпочтительными параметрами для хранения. Чем строже соблюдаются условия хранения и чаще контролируется относительная влажность, тем дольше срок службы микрофильмов.

Вредные факторы и загрязнения

Частицы пыли в воздухе являются загрязняющим фактором, они и есть очевидным источником царапин и повреждений на микрофильмах. Серебренно-желатиновые пленки особенно уязвимы для таких повреждений. Уборка в помещении для хранения микрофильмов, в том числе регулярные влажные уборки и очистка поверхностей пылесосом, играют важную роль в процессе хранения и использования микрофильмов.

Газообразные загрязнители воздуха, например, оксиды серы и азота, краски, аммиака, перекиси, озона и формальдегида, при воздействии на микрофильм могут приводить к повреждениям эмульсионного слоя пленки. Микрофильм не должен располагаться рядом с копировальными аппаратами – они могут быть источником озона. Кроме того, микроформы должны быть удалены из помещения для хранения при проведении его ремонта, окраске,

возникновении интенсивной циркуляция воздуха при открытии окон, и подлежат возврату в помещение по истечению трех месяцев. Деревянные стеллажи или шкафы не должны использоваться в помещениях для долгосрочного хранения.

Диазо, везикулярные и серебряно-желатиновые микрофильмы не должны быть размещены для хранения в одном и том же помещении и (в идеале) должны хранятся в таре, приспособленной для каждого вида пленки. Кроме того, старые микрофильмы везикулярного типа могут быть источником кислых продуктов распада. Такие экземпляры должны быть физически отделены от других типов микрофильмов и систематически заменяться на другие типы носителей.

Копирование

Даже в прекрасно контролируемых условиях длительного хранения необходимо иметь несколько копий микрофильма, что и обеспечивает гарантию от потерь и уничтожения архивного оригинала микрофильма. Большинство ценных коллекций с микрофильмами дублируются и имеют три поколения, что позволяет избежать потерь при колебаниях разных характеристик и факторов в условиях хранения.

Негативный оригинал микрофильма

Первое поколение микрофильма (он же негативный) должен быть серебрягно-желатиновый, производиться в соответствии с нормами, указанными в ANSI / AIIM MS23-1998. Это архивная копия, которую используют для получения дубликата негатива (см. ниже) для изготовления копий. Оригинал микрофильма следует хранить в месте, отделенном от других копий и в условиях, как можно ближе к идеальным. Есть ряд приспособленных хранилищ, которые можно арендовать для архивного хранения микрофильмов. Они должны гарантировать пользователю условия хранения по требованиям стандартов, изложенных в ANSI / NAPM IT9.11-1993. Единственное последующее использование негативного оригинала может проводиться для воспроизведения потерянного дубликата, при возникновении природных катаклизмов, форсмажоров.

Дубликат негативного микрофильма

Эта копия почти всегда серебяно-желатиновая. Дубликат негативного микрофильма используется для изготовления копий для коллекции. Он должен храниться в доступных условиях, так как является рабочей копией. В идеале, она должна быть физически отделена от других копий.

Контейнеры (тара) для хранения

Поскольку трудно обеспечить при существующих технологиях хранения полное удаление газообразных загрязнений (более старые микрофильмы могут выделять газы уксусной кислоты и поэтому помещения должны хорошо проветриваться). Негативы оригинала микрофильма должны хранится в хорошо контролируемых условиях, закрытые в металлические банки или инертные пластиковые контейнеры, обеспечивающие решение этого вопроса. В публикации KODAK D-31, хранение и сохранность микрофильмов (Компания Eastman Kodak, Рочестер, Нью-Йорк, 14650)

предлагается использование закрытых контейнеров. Эта стратегия не является панацеей и должны использоваться разумно. Тара должна отвечать требованиям к химическому составу. Необходимо периодически проверять микрофильм, чтобы убедиться в отсутствии ухудшения его характеристик. Руководящие указания по проверке серебристо-желатиновой пленки предлагаются в ANSI / AIIM MS45-1990. Если никакого ухудшения не наблюдается, пленка может быть возвращена в тару для хранения. Тара должна быть выбрана в соответствии с установленными руководящими принципами для архивного хранения и должна пройти все испытания фотографического качества, выполняемых институтом стойкости фотографий. NEDCC рекомендует бумажные корпуса тары высокого качества. MicroChamber ящики для хранения (производства по сохранению ресурсов International, Спрингфилд, штат Вирджиния) изготавливаются из доски пропитанной цеолитом, который нейтрализует газообразные загрязняющие вещества. Использование этих коробок значительно увеличивает срок службы микрофильмов в условиях загрязнения озоном, перекисью и другими соединениями, которые атакуют микрофильмы, она может также замедлить внешние повреждения от химикатов, влияющих на качество фильма.

Если относительная влажность среды хранения является стабильной и ниже 50 %, изоляция корпуса контейнера должна обеспечивать сохранность микрофильма. Клеевых соединений, где это возможно, следует избегать. Безопасные пластмассы, такие как сложный полиэфир, полиэтилен или полипропилен, но не поливинилхлорид (ПВХ) или винил – являются приемлемыми. Микрофиши должны размещаться в джекетах эмульсионной стороной от внутренней кромки корпуса для предотвращения истирания, что также добавляет защитных характеристик от клея на запечатанных краях. Рулонные микрофильмы должны храниться в индивидуальных коробках, с прикрепленными бирками.

Металлические шкафы с ящиками наиболее приспособлены для хранения микроформ, но инертные пластиковые контейнеры приемлемы для использования на библиотечных полках. Микрофиши должны находиться без потери устойчивости в ящиках. Разделительные направляющие должны быть изготовлены из материалов с нейтральным pH. Не допускается сжимание микрофильмов при открытии шкафов, а также при использовании разделения пространства в ящиках и нишах.

Как отмечалось выше, различные типы пленок должны храниться в различных контейнерах для предотвращения химического взаимодействия. Системы охлаждения и регулирования влажности должны применяться с учетом минимизации необходимости обработки шкафов для хранения, что способствует сохранению носителей информации. Износ и старение микрофильмов неизбежен при использовании коллекций, но скоростью старения и тяжестью степени ее последствий можно управлять.

Обработка пленки

Попадание на пленку отпечатков пальцев может повредить микрофильм, пользователи должны всегда одевать перчатки при работе с оригиналом. Все фильмы должны придерживаться при обработке или просмотре за края или концы. Во-избежание путаницы только один микрофильм изымается из корпуса тары. Карточка и бирка должны быть заполнены сразу после использования; а фильм немедленно возвращен в коробку (тару). Кроме того, перемотка микрофильма никогда не должна осуществляться при сильном натяжении на барабан или катушку, так как это может вызвать механические дефекты на пленке. Обучение персонала и пользователей в надлежащем обращении с микрофильмом необходимое условие для гарантии долговечности пленки.

Оборудование

При выборе оборудования следует учитывать простоту в его использовании и техническом обслуживании. При просмотре микрофильма на читательном аппарате воздействие тепла не должно превышать параметры ANSI стандартов. Как упоминалось выше, повреждения везикулярной пленки может происходить при температурах ниже ANSI пределов, поэтому следует уделить этому особое внимание. Читальные аппараты для микрофильмов должны быть отключены, если пользователь не использует оборудование. Оборудование должно проверяться еженедельно для поддержки его в рабочем состоянии. Грязное оборудование снижает качество изображения. Сотрудник должен знать инструкцию по эксплуатации оборудования и выполнять возложенные на него обязанности по техническому обслуживанию оборудования. Попадание пыли на стекло объектива будет видно при увеличении. Пыль может также попадать на поверхность микроформы, где она может затемнить детали изображения и даже повредить пленку. Также должен быть создан и придерживаться регулярный график или расписание по очистке линз, зеркал и матовых поверхностей для просмотра экранов, но эта очистка должна производиться с особой осторожностью, так как эти поверхности могут быть легко повреждены что приведет к размытию изображения.

Планирование действий на случай возникновения непредвиденных ситуаций

Планирование действий на случай возникновения стихийных бедствий имеет решающее значение для коллекций микрофильмов. Микроформы сильно подвержены повреждению водой. Они должны быть защищены от наводнений или прорыва труб. Как только влага попадает на микрофильм, его необходимо освободить от защитного корпуса и не допускать высыхания в рулоне, так как это повлечет слипание витков в рулоне и приведет его в негодность. Мокрый микрофильм должен быть удален из коробки для хранения. Рулонная пленка должна быть распрямлена для сушки. Сушка на воздухе является приемлемой, но эффективней обратиться в местную лабораторию по обработке пленки, которая может предоставлять эту услугу в случае возникновения чрезвычайной ситуации. Микрофиши можно сушить в

помещении, эмульсионной стороной вверх разложив в один слой или прикрепив краем, который не имеет никакого изображения. Диазофильм склонен к проявлению пятен от воды, и царапин от жесткой ткани, поэтому удалять следы капель воды необходимо мягкой тканью.

Мокрый микрофильм не может подвергаться воздействию низких температур, сушке в скрученном состоянии в виде рулона, что может привести к слипанию слоев пленки или их расслоению в результате раскручивания. Если микрофильм не может быть сразу высушен на воздухе, то его необходимо погрузить в чистую холодную воду и отправить в лабораторию для безопасной обработки и сушки. Появление плесени должно быть предотвращено на всех типах пленки. Заплесневелая диазотипного и везикулярного вида пленка может очищаться слегка влажной мягкой тканью, а если плесень поражает серебряно-желатиновый слой необходимо обратиться за профессиональной помощью.

Выбор поставщика микрофильмов

Коммерческое микрофильмирование экономически эффективно для преобразования книг и документов в микрофильмы. Как указано выше, каждое учреждение по микрофильмированию должно разрабатывать стандарты для своих микрофильмов, и эти стандарты должны быть частью договора на оказание услуг. Заказчику необходимо посетить микрофильмирующее предприятие, чтобы убедиться в наличии экологического контроля, пожарной безопасности, содержании помещений и безопасности, удовлетворяющей требованиям сохранности оригиналов коллекций, которые будут микрофильмироваться. Это особенно важно для предотвращения повреждения оригиналов исходных материалов, которые будут возвращены в коллекцию после микрофильмирования.

Использование инструмента микрофильмирования является целесообразным. Многие носители информации (такие как книги, газеты, папирусы) микрофильмируют, потому что они стали слишком хрупкими, но информация, хранящаяся на них должна быть сохранена и доступна для обработки историками, исследователями и учеными. Если это так, или если необходимо сохранить важные материалы в их первоначальном виде, специальные услуги по микрофильмированию должны быть рассмотрены в первую очередь. Большинству коммерческих компаний по микрофильмированию хватает оборудования, времени и опыта для обработки хрупких материалов без ущерба для оригинала. Затраты же на более сложные случаи требуют специальных услуг и будут больше, но ценность артефактов или труднодоступность оригиналов (например, плотно переплетенных томов с узкими желобами, документы с угасающим текстом или ненадлежащего контраста) может быть предпосылкой к этим расходам. В таких случаях необходимо обращаться к профессионалам в области микрофильмирования.

Избранная библиография для менеджеров, работающих с микроформами:

1. American National Standard Practice for the Storage of Processed Safety Fotographic Film, Американский национальный стандарт по хранению проявленных огнебезопасных фотографических пленок. ANSI PH 1. 43-1985 (*)

(*) American National Standards Institute, Inc., 1430 Brodway, New York, NY 10018.

2. American National Standard for Imaging Media (Film) Silver Gelatin Type - Specifications for Stability. Американский национальный стандарт по носителям изображений (пленкам) галоидо-серебряного типа - спецификации устойчивости. ANSI IT 9. 1-1988.

3. American National Standard for Imaging Media - Photographic Processed Films, Plates, and Papers - Filing Enclosures end Storage Containers. Американский национальный стандарт по изображениям - проявленные фотографические пленки, пластинки и бумаги - защитные приспособления и контейнеры для их хранения. ANSI IT 9. 2-1989.

4. American National Standard for Imaging Media (Film) - Ammonia Proccesed Diazo Films - Specification for Stability. Американский национальный стандарт по носителям изображений (пленкам) - аммиачно проявленые диазо пленки - спецификации устойчивости. ANSI IT 9. 5-1988.

5. Association for Information and Image Management. Practice for Operational Procedures/Inspection and Quality Control of First Generation, Silver-Gelatin Microfilm of Documents. Практика обработки/проверки и контроля качества галоидо-серебряных микрофильмов первого поколения. ANSI/AIIM MS 23-1983. (**)

(**) Association for Information and Image Management, 1100 Wayne Avenue, Silver Spring, MD 20910).

6. Borck, Helga. "Preparing Material for Microfilming: A Bibliography (revised 1984) ." Подготовка материалов для микрофильмирования. Библиография. (проверка 1984 г.). Microform Review 14 (Fall 1985): 241-43.

7. Chase, Myron B. "Preservation Microfiche: A Matter of Standards." Сохранение микрофиш: проблема стандартизации. Library Resources and Technical Services 35(2) (April 1991): 186-190.

8. Child, Margaret S. "The Future of Cooprative Preservation Microfilming." Будущее совместного микрофильмирования с целью сохранения. Library Resourses and Technical Services 29(1) (Jan. -March 1985): 94-101.

9. Cox, Richard J. "Selecting Historical Records for Microfilming: Some Suggested Procedures for Repositories." Выбор исторических документов для микрофильмирования: некоторые методы, рекомендуемые для хранилищ. Library and Archival Security 9(2) (1989): 21-41.

10. Diaz, A. J. (ed). Microforms in Libraries: A Reader. Микроформы в библиотеках: прибор для чтения. Westport, CT: Microform Review, 1975.

11. Elkington, Nancy E. (ed). RLG Preservation Microfilming Handbook. Руководство по сохранению при микрофильмировании. Mountain View, CA: Reserarch Libraries Group, 1992.

12. Gwinn, Nancy E. (ed). Preservation Microfilming: A Guide for Librarians and Archivists. Микрофильмирование для сохранения: руководящие материалы для библиотекарей и архивистов. Chicago: American Library Association, 1987.

13. Johnson, A. K. A Guide for the Selection and Development of Local Goverment Records Storage Facilities. Руководство по выбору и улучшению хранилищ документов местных правительственных офисов. New York: NAGARA, 1989.

14. Library of Congress. Specifications for the Microfilming of Manuscripts. Спецификации по микрофильмированию рукописей. Washington D. C.: Library of Congress, 1980.

15. Preservation Microfilming: Planning & Production. Микрофильмирование для сохранения: планирование и производство. Papers from the RTSD Preservation Microfilming Institute, New Haven, Conn., April 21-23, 1988. Chicago: Association for Library Collection & Technical Services, ALA, 1989.

16. Recommended Practice for Operational Procedures/Inspection and Quality Control of Duplicate Microforms of Documents. Рекомендуемые способы обработки/проверки и контроля качества копий документов на микроформах. COM, ANSI/AIIM Ms 43-1988.

17. Recordak. Storage and Preservation of Microfilms. Хранение и сохранение микрофильмов. Kodak pamphlet no. P-108. Rochester, NY: Eastman Kodak Company, 1985.

18. Reily, James et al., "Stability of Black and White Photograhic Images, with Special Reference to Microfilm." Стабильность черно-белых фотографических изображений, со специальным рассмотрением микрофильмов. Abbey Newsletter 12(5) (July 1988): 83-87.

19. RLIN Preservation Masterlife. (CD-ROM) listing of microfilmed books and jornals. Перечень микрофильмированных книг и журналов. Compiled from the RLIN database and others. Available from Chadwick-Healey, Inc. for $ 750 a year; updated twice annually.

20. Spreitzer, Francis (ed). Microforms in Libraries: A Manual for Evalution and Management. Микроформы в библиотеках: руководство по их оценке и управлению. Chicago: American Library Association, 1985.

21. Spreitzer, Francis (ed). Selecting Microform Readers and Reader Printers. Выбор аппаратов для чтения микроформ и для их печати. Silver Spring, MD: AIIM, 1983.

БАРЬЕРЫ НА ПУТИ УТЕЧЕК ДАННЫХ

Источник: http://www.osp.ru/os

Хищения данных превращаются в одну из наиболее серьезных угроз для информационной безопасности — предотвращение краж данных и несанкционированного доступа к ним рассматривается уже в числе задач национального масштаба.

Леонид Черняк

Невиданные прежде «информационные катастрофы», вроде публикации сотен тысяч документов в WikiLeaks, дают представление о том, какие чудовищные объемы данных могут быть похищены с использованием современных технологий и к каким последствиям это может привести. Еще совсем недавно событий сравнимого масштаба не могло быть в силу существовавших технических ограничений на объемы данных, которые могли попасть в руки злоумышленников, – просто не было носителей, позволяющих украсть, например, полный комплект документации на изделие под названием "нейтронная бомба". Теперь необходимый объем данных уложится на нескольких квадратных миллиметрах флэш-памяти, да и хранятся они в цифровой форме, как будто специально созданной для упрощения краж. В итоге угроза кражи данных (data theft) и несанкционированный доступ к данным (data breach) вошли сегодня в число критичных, а для противостояния им предлагаются в том числе средства предотвращения утечки данных (Data Leak Prevention, DLP).

Добросовестным пользователям всегда не хватало устройства для компактной ручной транспортировки данных, и чего только не использовали: перфокарты и перфоленты, магнитные ленты, флоппи-диски. Емкость таких устройств росла, а недостатки, прежде всего нестабильность и недолговечность, сохранялись. Паллиативы в виде дисков типа ZIP оказались непрактичными, чуть получше показали себя CD-ROM, но и они скорее годятся для распространения данных и программ, а не для оперативной работы. И вот в 1998 году были изобретены, а через два года появились в продаже флэш-накопители, получившие повсеместное распространение от встроенных в бытовые устройства до серьезных твердотельных накопителей (Solid State Drive, SSD), и было бы странно, если бы это изобретение не взяли на вооружение не вполне законопослушные граждане.

До недавнего времени данные в основном воровали по сети — все 15 наиболее крупных краж в США за последние пять лет были осуществлены посредством атак с использованием SOL-инъекций, а сегодня в моду вошли носимые устройства. Известны два основных типа хищений с применением таких устройств: thumbsucking (от одного из английских названий флэш-накопителей ThumbDrive; thumb — "большой палец", thumb sucking –

привычка грудничков сосать палец) и Pod slurping (от iPod и slurping — "заглатывать").

Первый широко известный пример хищения данных с использованием флэш-памяти был зафиксирован в ядерной лаборатории в Лос-Аламосе. Там страдающая наркозависимостью служащая, занимающая самый нижний уровень в служебной иерархии, смогла вынести полный комплект чертежей атомной бомбы; впоследствии данные были обнаружены у нее дома. Более эффективно и профессионально с подобной целью может быть применен USB-диск со встроенной технологией U3, в котором все пространство делится на два раздела, после чего один, меньший по объему, раздел предоставляется операционной системе, а другой используется как обыкновенный флэш-диск. В первом разделе размещается небольшая программа Launchpad, запускаемая операционной системой автоматически, далее открывается список переносимых программ, которые можно запустить из второго раздела. Эти программы способны работать с файлами или реестром Windows, не оставляя следов на компьютере по завершении работы. Результаты работы могут сохраняться во втором разделе накопителя. Аналогичное изделие, специально адаптированное для хакеров, известно как SB Switchblade.

Метод хищения Pod slurping можно признать разновидностью thumbsucking; отличие в носителе, им может быть iPod или аналогичный медиаплеер. Еще известны способы хищения данных через порт Bluetooth — Bluesnarfing.

Угрозы изнутри

Угрозы национальной безопасности становятся все разнообразнее, и это начинают уже понимать современно мыслящие спецслужбы, например Секретная служба США, которая в отличие от своего российского аналога, Федеральной службы охраны РФ, помимо своей непосредственной функции выпускает общедоступные отчеты, где представляет существующие и новые угрозы национальной безопасности. Отчет за 2010 год, Data Breach Iinvestigations Report, посвящен всестороннему анализу статистики хищений данных и аккумулирует данные о компьютерных атаках, публикуемые в странах Северной Америки и Западной Европы, Китае, Египте и Японии. Остальные страны, в том числе и Россия, не предоставляют таких официальных данных. Половина хищений фиксируется в США, где около 70% потерь данных приходится на три сектора экономики: финансовый (33%), гостиничный (23%) и торговлю (15%). Документ начинается с констатации факта наметившихся изменений в статистике компьютерных преступлений – хотя внешние хакерские атаки и проникновения все еще остаются основным способом хищений (на них приходится 70%, а на внутренние – 48%, сумма не равна 100%, поскольку часто злоумышленники действуют совместно), показательна динамика последнего года: внешние сократились на 9%, а внутренние увеличились на 26%.

Тенденция к перераспределению от внешних к внутренним угрозам естественным образом определяет направление в развитии средств

обеспечения безопасности, отсюда повышенное внимание к DLP. Упомянутый выше отчет констатирует: главный вклад в рост внутренних хищений вносят намеренное асоциальное поведение сотрудников компаний и организаций и превышение ими служебных полномочий. Системы DLP можно назвать защитными экранами наизнанку, в отличие от межсетевых экранов.

Так уж сложилось, что термины «защита информации» и «информационная безопасность» предполагают наличие внешних угроз, но реальная жизнь демонстрирует, что не меньший вред предприятию могут нанести свои собственные "плохие парни", а практика социальной инженерии это успешно подтверждает. Опасность, исходящая изнутри, получила официальное название "утечка информации", что нашло отражение в стандарте ISO/IEC 17799-2005, созданном на основе британского стандарта, а его содержание перенесено в отечественный аналог ГОСТ/Р ИСО МЭК 17799-2005. Первые разработки DLP известны с начала десятилетия, а широкое распространение эти системы получили примерно с 2006 года, и с тех же пор обращение к DLP вызывает множество вопросов, поскольку за тремя буквами скрывается не конкретная совокупность технологий, а размытая область человеческой деятельности, включающая технологии, методологию, нормативные документы и многое другое, связанное с недопущением неавторизованного использования и распространения конфиденциальной информации. Не случайно помимо принятого названия DLP, существуют и альтернативные, отражающие определенную специфику: Information Leak Prevention (ILP), Content Monitoring and Filtering (CMF), Information Protection and Control (IPC) и Extrusion Prevention System (EPS). Особо интересно последнее, где слово extrusion использовано как антипод intrusion ("проникновение").

Система DLP должна обнаруживать критически важные данные в базах данных, файловых серверах, настольных и мобильных компьютерах; информировать о попытках пересылки этих данных или записи на накопитель, и в ней должны быть зафиксированы правила, по которым осуществляется блокировка данных, и другие превентивные меры.

Недавно возникшая проблема больших данных (Big Data Problem) может рассматриваться как еще одна из важнейших причин роста интереса к DLP. Отчет организации Computing Technology Industry Association, озаглавленный Trends in Information Security, свидетельствует, что в 2008 году свыше 60% утечек данных было так или иначе связано с человеческими ошибками, пятью годами раньше этот показатель составлял всего 8%, и если не предпринимать специальных мер, в том числе таких, как внедрение систем DLP, то по мере роста объемов данных он будет только возрастать. Аналогии с инцидентами в других отраслях свидетельствуют о том, что реальная безопасность без автоматизации недостижима, человеческий фактор – причина большинства техногенных катастроф.

Внедрение решений класса DLP должно способствовать получению ответа на три главных вопроса: где и в каких данных содержится

конфиденциальная информация? Как и кем эти данные используются, кто имеет к ним доступ? Что нужно предпринимать, дабы избежать потерь? В идеале средства DLP должны обеспечивать: глубинный анализ контента; автоматическую защиту данных во всех возможных местах нахождения, то есть на пользовательских компьютерах (их называют конечными точками, end-point), в сетях и в системах хранения данных; анализ инцидентов и корректирующую работу с пользователями.

Антропология DLP

В общем случае под DLP понимают комплекс технологий для автоматизации процессов идентификации и защиты критически важных данных, состоящий из трех взаимодополняющих компонентов: Management (управление), Identification (идентификация) и Protection (защита).

Управление. Руководящие принципы любой системы DLP определяют то, какие данные следует рассматривать как критически важные, какие действия разрешены по отношению к этим данным и как такие данные следует защищать. Это чрезвычайно сложная задача. Допустим, нужно защитить номер кредитной карты 1234 2345 3456 4567, однако эта последовательность цифр может быть чем угодно: артикулом изделия, номером телефона и т. п. Для того чтобы выделить ее именно как номер карты, необходимо каким-то образом задать контекст. Кроме того, в руководящих правилах должно быть задано, что следует делать компоненту Protection в том случае, если обнаружены защищаемые данные, нужно ли их перед пересылкой зашифровать или следует уведомить о попытке нарушения полномочий. Возможности Management ограничены представлением защищаемых данных, например их форматом или кодировкой: код номера кредитной карты в упакованном файле может сильно отличаться от кода того же номера в электронной таблице. Чем больше форматов распознает система DLP, тем она эффективнее, тем больше шансов обнаружить существенно важные данные, и, как следствие, поставщики DLP-решений утверждают всеядность своих технологий, что во многих случаях неверно — всегда найдутся исключения, которые необходимо учитывать. Это одна из причин для постепенного и итерационного внедрения DLP на предприятии.

Идентификация. В этом компоненте используются принципы, сформулированные в компоненте Management, — здесь выполняется некоторый тест и принимается решение о принадлежности данного фрагмента к критическим данным. Поскольку принципы формулируются с допущениями, то результат теста не может быть верным на 100%: в любом случае можно пропустить нужное или заблокировать ненужное.

Защита. После того как компонент Identification обнаружил данные, нуждающиеся в защите, компонент Protection выполняет ее обычно с использованием одного из двух возможных способов — либо зашифровывает, либо блокирует. Если налицо неразрешенная попытка списывания на диск по USB, то, скорее всего, она будет прервана, а если данные передаются по почте, но в открытом виде, хотя их положено шифровать, то они будут зашифрованы. Блокирование обычно не создает

больших проблем, хотя и приводит к увеличению числа обращений в службу поддержки. Чаще всего оказывается, что люди не делают чего-то злостного, а лишь не вполне точно следуют служебным инструкциям. Что же касается криптографии, то ее более широкое распространение может потребовать дополнительных организационных мер.

Аналитики Gartner и Forrester среди компаний, специализирующихся на DLP, отмечают: RSA (в составе EMC), Websence, Symantec, Fidelis security, McAfee, CA, Vericept, Code Green, Trend Micro иVerdasys. Отечественный рынок таких продуктов и близких к ним отличается доминированием трех локальных производителей: Jet Infosystems, SecireIT и InfoWatch. По приблизительным оценкам, этим компаниям принадлежит примерно по четверти всего объема рынка, а оставшаяся часть занята иностранными компаниями. Очевидно, что по мере повышения его зрелости доля зарубежных компаний будет возрастать.

Работа с системами DLP на предприятиях заметно отличается от использования других технологий защиты информации — мнение по этому вопросу консультанты PricewaterhouseCoopers выразили в отчете «Data Loss Prevention: Keeping sensitive data out of the wrong hands» (DLP: не отдавайте важные данные не в те руки). Компаниями уже освоен выпуск продуктов, способных блокировать или предотвратить вывод значимых данных за пределы организации, однако пока все эти продукты еще не достигли зрелости — остается риск того, что заблокируются критические для функционирования предприятия данные. По этой причине должен быть разработан детальный план мероприятий по внедрению DLP, включающий оценку плюсов и минусов, последствий ошибок пропуска реальной угрозы или признания опасной безобидной вещи. Системы DLP нельзя отнести к категории «внедрил и забыл» — необходимо постоянно оценивать текущие результаты и совершенствовать руководящие принципы (политики). Разумно построенная система DLP должна позволить:

- усовершенствовать схемы назначения уровня секретности для данных, точнее определить их тип и местонахождение;
- получить точные представления о жизненном цикле данных, выделить их потоки, обнаружить пробелы в анализе, уточнить их расположение, ассоциированные с ними средства контроля и то, как эти средства контроля используются;
- сконцентрировать контроль на существенно важных данных, соответствующим образом организовать работу персонала, имеющего дело с этими данными, распределить между исполнителями функции и ответственность;
- не только защитить данные, но и обнаружить разрывы в бизнес-процессах.

Классификация систем DLP

Для систем DLP принята двухзвенная классификация по их размещению: в сетях (Network DLP, рис. 1) или в конечных пунктах назначения данных (Endpoint DLP, рис. 2). Кроме того, средства DLP можно

классифицировать по возможным состояниям данных, на работу с которыми они ориентированы: данные в состоянии покоя (data at rest), в процессе перемещения (data in motion) и в процессе использования (data in use). Каждому из таких состояний адресуется свой собственный набор технологий, например подходы, лежащие в основе Network DLP, проще, более традиционны и дешевле, но менее эффективны.

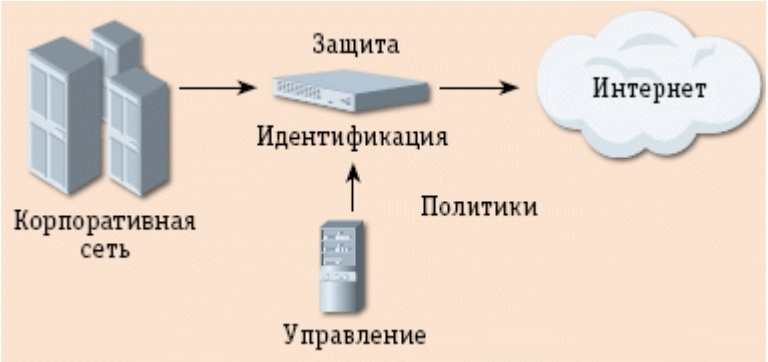

Рис. 1. Три компонента DLP в сетевом варианте

Данные в состоянии покоя. Для идентификации и регистрации тех мест, где хранится существенно важная информация, система DLP должна уметь обнаруживать на серверах, в сетях хранения и на рабочих местах файлы в форматах текстовых документов и электронных таблиц, а найдя их, должна уметь открыть файл, сканировать на предмет поиска интересующей ее информации. Для выполнения такой функции система DLP применяет агенты

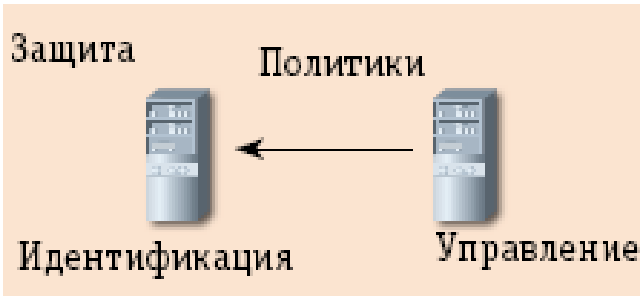

Рис. 2. Три компонента end-point DLP

того или иного типа, обследующие все возможные места нахождения данных. Сбор такой информации является существенным шагом в работе предприятия, он позволяет найти пункты размещения данных, пути их миграции и соотнести их с регламентирующими правилами. Наиболее простые решения этого типа распространяются только на системы хранения — это storage-centric DLP.

Данные в процессе перемещения. Для работы с данными такого типа применяются встроенные технологии или специализированные устройства для перехвата и анализа сетевого трафика. Система DLP обязана осуществлять пассивный мониторинг трафика, распознавать данные в пакетах, при необходимости собирать содержимое пакетов, реконструировать файлы и ставить окончательный диагноз: разрешена или не разрешена передача данного файла. Ядром этого процесса является процедура глубокого анализа или инспектирования пакетов DPI (Deep Pocket Inspection) — хорошо известная технология защитных экранов, сочетающая функциональность обнаружения IDS (Intrusion Detection System) и предотвращения вторжений IPS (Intrusion Prevention System). Она позволяет проверять пересылаемые данные; выявлять их типы и приложения, работающие с ними; осуществлять загрузку сети тем или иным сервисом; выявлять злонамеренный трафик и аномалии в протоколах. Для анализа данные должны быть расшифрованы либо самой системой DLP, либо препроцессором. Системы DLP данного типа реализуются программными средствами либо с помощью специализированных машин (DLP appliance), которые производят компании McAfee, Code Green, Palisade Systems и Blue Coat Systems.

Данные в процессе использования. Это, возможно, самая сложная и ответственная часть DLP, отвечающая за контроль действий пользователей над данными, выполняемых на рабочих станциях и чреватых утечками: попытки копирования на носимые устройства, распечатки, перемещения данных между приложениями и т. п. Принципиальное отличие end-point DLP состоит в глубинном анализе контента на основе принятых правил. Для этого типа анализа используются различного типа алгоритмы, основанные на частичном или полном совпадении документов, на «отпечатках пальцев» данных, статистике или на комбинации нескольких методов. Для реализации любого из алгоритмов могут быть использованы десятки разных программных агентов, способных работать на разных уровнях: непосредственно на уровне контента, на уровне файловой системы, на уровне сети и на уровне интерфейса пользователя с системой.

Подходы к созданию систем DLP

Какой из подходов предпочтительнее, сетевой или по месту нахождения данных? По ответу на этот вопрос специалисты делятся на два лагеря: сторонники решений network-based и data-in-motion, приверженцы data-at-rest и end-point DLP. Сильным аргументом первых является то, что фильтрация сетевого трафика позволяет уловить до 80% всех утечек, причем без особых сложностей, в таком случае нет необходимости в сложных правилах, а достаточно лишь установить фильтры в нужных местах. Но они же признают, что выбор не является альтернативным, скорее вопрос в том, с чего начинать, сначала с data in motion, а потом data at rest. Приверженцы второго подхода считают, что преимущество data-at-rest DLP в глубоком искоренении возможностей для утечек и хищения данных. Эти технологии не всегда требуют для себя использования специализированного оборудования.

Обычно внедрение систем DLP в организациях начинается с защиты сетей, как наиболее очевидного канала для утечки. Следующим шагом чаще всего бывает создание статичных систем защиты хранимых данных (storage-centric DLP). До недавнего времени такого рода системы network и storage-centric DLP исключали значительную часть инцидентов, связанных с потерей данных. Далее можно перейти к end-point DLP, и постепенно в связи с изменением структуры угроз безопасности данных роль этих систем возрастает. Наиболее современные системы DLP сочетают в себе оба типа программного обеспечения: end-point и network-based, позволяя создавать общую функциональность и вырабатывать общую корпоративную политику обеспечения безопасности.

На фоне разных технических аспектов DLP нельзя упускать один весьма существенный — психологический. Когда сотрудники узнают о внедрении DLP, количество попыток хищения уменьшается на порядок.

Полнота и точность

Продукт Websense Data Security Suite сочетает в себе технологию детектирования информации с архитектурой, интегрирующей средства DLP и обеспечения безопасности в Web, а также защиты электронной почты. Предложенная компанией технология информационных отпечатков основана на извлечении текста и других данных из сообщений и файлов с последующим расчетом кодовой последовательности, характеризующей защищаемую информацию. Отпечатки вычисляются на конфиденциальном документе, а затем на передаваемых сообщениях: система DLP сравнивает полученные отпечатки и принимает решение о фильтрации. Вместо полнотекстовой индексации используется циклическое хеширование, что позволяет работать с не текстовыми данными (например, документами САПР) и автоматически отличать заполненный бланк от пустого. Кроме того, отпечатки не позволяют злоумышленникам восстановить исходный текст и устойчивы ко всем основным типам модификации.

Отпечатки – это только часть методической базы PreciseID и кроме неструктурных отпечатков документов имеются отпечатки для текстовых полей РСУБД, используемые, например, для защиты фактически хранимых персональных данных. В компании разработана процедура создания классификаторов на базе естественных языков, и сейчас их около 1000. В решении определяются имена на 12 языках, включая русский, а регулярный анализ строк дополняется алгоритмической логикой; например, чтобы отличить номер пластиковой карты от случайного набора цифр вычисляются контрольные разряды.

По данным аналитиков, каждая ошибка первого рода (ложная тревога) стоит организации порядка 10 руб., а цена ошибок второго рода (пропуск конфиденциальных данных за пределы компании) может достигать значений со многими нулями, поэтому точности в решениях от Websense уделяется первостепенное внимание. В спорных случаях применяется процессор естественных языков (Natural Language Processing), реализующий

контекстно-статистический анализ слов и выражений, подавляя ложные срабатывания, свойственные традиционным методам. По данным исследования, проведенного Percept Technology Labs, технология цифровых отпечатков обеспечивает около 1 % ошибок первого и второго рода.

— ***Петр Савич*** *(psavich@websense.com) — старший инженер по продажам компании Websense в Восточной Европе.*

Платформа защиты информации

Платформа «Дозор-Джет» представляет собой масштабируемое решение для создания архива данных и анализа его содержимого, позволяющее управлять остальными компонентами системы защиты, производить фильтрацию обрабатываемых данных в соответствии с заданной политикой и осуществлять поиск. Архитектура системы позволяет осуществлять контроль за утечками как для простых (гигабайты данных в месяц), так и для масштабных конфигураций (десятки и сотни терабайтов данных в архиве). Компонент анализа сетевых потоков способен обрабатывать трафик размером более 2 Гбит/с на одном сервере, а масштабируемая архитектура позволяет интегрировать решения от различных производителей (антивирусные средства, системы хранения, документооборота, OCR-системы, системы управления).

Система извлечения данных и метаданных, входящая в состав комплекса «Дозор-Джет», помогает извлекать текстовые данные, характеризующие свойства документов, даже при их случайном или намеренном искажении, например при подсоединении в конец мультимедиафайла. «Дозор-Джет» позволяет использовать для фильтрации и поиска списки слов и выражений, словари и наборы идентификаторов, данные о типе файла, данные о транспортной сессии. Кроме того, система дает возможность применять цифровые отпечатки — набор алгоритмов, позволяющих определить порядок использования защищенных документов (как текстовых и бинарных, так и изображений). Для контроля данных возможно также использование средств поиска стандартных идентификаторов, таких как номера телефонов, ИНН, ОКПО, ОКАТО, номера в финансовых документах, имена и фамилии, номера паспортов, кредитных карт и т. д. При этом система проверяет найденные значения с помощью контрольных сумм, а также других признаков, позволяющих обойтись без ложных срабатываний.

При развертывании системы обычно осуществляется аудит, в процессе которого вырабатываются ключевые точки контроля и политика компании, направленная на снижение рисков. Как правило, кроме введения в действие тех или иных правил обработки и проверки данных, необходимо провести соответствующую работу по изменению регламентов обращения с информацией, а иногда и регламентов основной производственной деятельности компании.

Отношения и обязательства между поставщиком и заказчиком регулируются сервисным договором, и, как правило, гарантии на системы контроля утечки в нем не предоставляются.

— ***Дмитрий Михеев*** *(ovpr-comments@jet.msk.su) — эксперт центра информационной безопасности компании "Инфосистемы Джет" (Москва).*

Централизованная фильтрация

В состав DLP-решения от Symantec входит централизованная консоль управления (настройка политик, формирование отчетности, расследование и закрытие инцидентов), модуль защиты рабочих станций (контроль действия пользователей, блокировка попыток выноса конфиденциальных данных, сканирование файловой системы всех рабочих станций на предмет хранения там конфиденциальных документов), модуль контроля сетевого трафика (мониторинг сетевых взаимодействий внутри корпоративной сети и на границе периметра), модуль сканирования хранилищ (поиск и автоматическое перемещение конфиденциальных данных).

Общую схему работы технологии цифровых отпечатков можно описать следующим образом: из документа, с которого снимается цифровой отпечаток, выделяется текстовое содержание, которое разбивается на фрагменты, и для каждого из них создается «отпечаток» — математическая сумма содержимого. В итоге весь документ представляется набором «отпечатков», который сравнивается с набором для вновь пересылаемого -- если имеется пересечение, то DLP-система это диагностирует. Однако практические реализации данного механизма могут существенно отличаться как по точности срабатывания, так и по потребляемым ресурсам. Как известно, комбинирование нескольких технологий идентификации содержимого повышает эффективность работы, что справедливо и для Symantec DLP, где поддерживаются как простейшие методы (ключевые слова, регулярные выражения, идентификаторы данных), так и технологии цифровых отпечатков с текстовых данных и с таблиц.

Ни одна DLP-система не гарантирует нулевой вероятности утечки, однако внедрение таких технологий позволяет снизить бизнес-риски. Исходя из опыта наших заказчиков как в России, так и за рубежом можно сказать, что количество утечек данных после внедрения таких систем в среднем падает на 80-90% за первые несколько недель или месяцев.

— ***Олег Головенко*** *(Oleg_Golovenko@symantec.com) — технический консультант компании Symantec в России и СНГ (Москва).*

Интегральные DLP

DLP-решения Zgate, Zlock и Zserver Suite компании SecurIT имеют традиционную архитектуру, включающую в себя перехватчики, анализатор, архив, журнал событий и систему управления. Zgate перехватывает и анализирует сетевой трафик (HTTP, HTTPS, SMTP, FTP, ICQ, Skype и т. д.), Zlock контролирует печать и запись данных на внешние накопители, Zserver Suite защищает данные в серверных хранилищах и на резервных носителях

при хранении, обработке и транспортировке. Все эти решения имеют ряд отличительных особенностей. Во-первых, имеется большое количество контролируемых каналов, среди которых только интернет-пейджеров насчитывается около полутора десятков. Во-вторых, в решениях применяется гибридный анализ перехваченных данных с использованием цифровых отпечатков, лингвистики, регулярных выражений, OCR и собственной технологии SmartID. В-третьих, в Zlock и Zgate поддерживается возможность блокировки утечек, а не только информирование по факту инцидента.

Как и у большинства производителей, в решениях SecurIT в основе технологии «цифровых отпечатков» лежит алгоритм преобразования исходного текста в специальный вид, например в последовательности из трех слов. При анализе информации такие последовательности документа сравниваются со специально созданной базой «цифровых отпечатков» конфиденциальных данных. Наряду с этим в Zgate используется технология определения и исправления ошибок, а также замаскированного текста. В общем потоке информации конфиденциальные данные выявляются с помощью фильтра, а попавшие в него данные могут блокироваться для передачи, архивирования, записи и т. д. Количество ошибок в DLP-системе зависит от настроек, массива защищаемых данных и сценария утечки -- по результатам собственных испытаний и анализа статистики использования SecurIT DLP средняя погрешность составляет примерно 2 %.

Основную уверенность в надежности решения заказчику должна дать хорошая подготовительная работа — необходимо правильно оценить риски и описать сценарии использования информации и только потом выбрать конкретную техническую DLP-реализацию. Не стоит забывать и об административной работе, которая может снизить количество утечек.

*— **Александр Ковалев** (kovalev@securit.ru) — директор по маркетингу компании SecurIT (Москва).*

Последнее слово за заказчиком

В арсенале компании InfoWatch имеются практически все наиболее эффективные способы идентификации конфиденциальной информации, и все они объединены в алгоритм "Гибридный анализ". Его средствами анализируется каждый передаваемый фрагмент данных (копируемый файл, отсылаемое сообщение, "пост" в системах мгновенного обмена сообщениями или на форуме, печатаемый документ и т. д.) на предмет выявления информации, которую компания-пользователь считает конфиденциальной.

Применяемый в решениях InfoWatch метод цифровых отпечатков (Digital Fingerprints) позволяет с вероятностью более 95% найти значимую цитату в проверяемом документе путем сравнения со «слепком» в другом документе. Метод применяется в основном при защите статических данных (клиентских баз, документных хранилищ, корпоративных библиотек) — можно снять «отпечаток» с каждого защищаемого элемента и заставить систему автоматически запрещать перемещение информации, содержащей большие значимые цитаты. Именно значимые, так как, уменьшая размер

цитат, можно скатиться до одиночных слов и полностью остановить документооборот в компании. Алгоритм гарантирует стопроцентное детектирование значимых цитат, но некоторые цитаты могут оказаться неконфиденциальными, что и дает некоторый процент ложных срабатываний. Однако алгоритм неприменим в случаях, когда пользователь не имеет образца конфиденциальной информации, с которого можно было бы снять «слепок».

Статистические методы плохо работают на быстро изменяющейся информации или с неизвестными данными, например с входящими документами: процесс снятия отпечатка с большой базы может занимать несколько часов, поэтому защищаться будет не актуальная, а прошлая база. Входящие документы могут использовать не принятую в компании систему грифования документов, и конфиденциальный документ, пришедший из другой компании, не будет воспринят как таковой. Здесь на помощь приходит лингвистика, позволяющая проанализировать текст на предмет наличия в нем специальных терминов и сочетаний, а также их контекста (например, ни один торговец не назовет прямым текстом героин героином, а будет называть его «товар» и т. д.). В результате можно с точностью 85-90 % определить категорию сообщения (финансы, производство, коммерция, личная переписка и т. д.) и его класс (общедоступное, ДСП, секретное и т. д.). По производительности и точности срабатывания статистические и лингвистические методы в DLP соотносятся приблизительно так же, как сигнатурные и эвристические методы в антивирусах. Первые, работающие с заранее известными «угрозами», дают близкую к 100 % вероятность защиты и высокую производительность. Вторые умеют работать с неизвестными угрозами, расширяя функционал первых, но при этом понижается производительность и растет число ложных срабатываний. Самый большой процент ложных срабатываний (около 25 %) отмечается на неструктурированных данных для необученной системы, построенной на правилах категоризации, которые были встроены по умолчанию. После обучения в течение нескольких часов количество ложных срабатываний падает до 5-7 %, а если есть возможность снять отпечатки с образцов документов, то и до 1-2 %.

Как и для любых других систем защиты информации, финансовой ответственности за пропуск важных данных компания-производитель не несет, поскольку причина может заключаться, например, в том, что заказчик не предоставил исполнителю все категории конфиденциальной информации. Однако у InfoWatch имеется опыт более сотни внедрений, и вопрос о гарантиях и ответственности еще не возникал, но если утечка была вызвана ошибкой алгоритма, то, безусловно, компания-разработчик сделает все возможное, чтобы его исправить.

В DLP, в отличие от антивирусов, пока нет независимых тестов на точность срабатывания (например, Virus Bulletin), да и вряд ли они возможны – документы у каждой компании свои и представляют собой внутренний, а не внешний, как вирусы, объект. Иногда бывает, что заказчик, избалованный

предыдущим опытом организации защиты инфраструктуры, посчитает, что после внедрения DLP-системы все произойдет само собой, однако никто, кроме него, не знает о его данных и процессах их перемещения, поэтому улучшить эффективность системы защиты данных от утечек может только сам пользователь. В отрыве от всей системы защиты данных, без встраивания в бизнес-процессы, сами по себе DLP-системы вряд ли эффективны.

— ***Рустэм Хайретдинов*** *(rustem.khairetdinov@gmail.com) — заместитель генерального директора компании InfoWatch (Москва).*

Простота и скорость

Характерная особенность решения для DLP компании McAfee — это простота архитектуры, что, однако, не означает бедность функциональных возможностей. В McAffee Network DLPManager есть уникальные функции, например фиксация и индексация событий независимо от срабатывания правил, позволяющая обрабатывать события и восстанавливать картины произошедшего в случае, когда были допущены ошибки в настройках. Кроме этого предусмотрено несколько способов идентификации конфиденциальных документов: анализ ключевых слов и выражений; встроенный язык регулярных выражений, позволяющий описывать критерии конфиденциальности; тегирование по типу документа; анализ местонахождения и приложений, которые обрабатывают документ; цифровые отпечатки.

Говоря о гарантиях при работе с решением DLP от McAffee, следует отметить, что ни одна компания в мире не имеет в своем лицензионном соглашении пунктов об ответственности за ошибки системы DLP. Следует учесть, что одной системы мало — для надежности решения требуется совокупность организационно-технических мер. Надо повышать осведомленность сотрудников в вопросах информационной безопасности, применять технические специализированные средства мониторинга, контроля и противодействия утечкам конфиденциальных данных. Только комплексный подход даст заказчику уверенность в надежной защите конфиденциальной информации на предприятии.

—Алексей Чередниченко *(Alexey_Cherednichenko@McAfee.com) – руководитель направления продаж для секторов "Нефть и газ" и "Телеком McAfee".*

Разумный баланс

Компания Trend Micro предлагает ряд решений, включающих в себя функции защиты от утечек данных, и полный набор таких функций содержится в продукте Trend Micro DLP for Endpoint. Это решение позволяет контролировать конечный узел одновременно по нескольким фронтам: USB-накопители, запись на CD/DVD-диски, различные сетевые протоколы и др. Одним из последних обновлений данного решения стало включение функциональности обнаружения вредоносных программ хищения данных.

Для идентификации конфиденциальной информации Trend Micro DLP for Endpoint использует шаблоны четырех типов, простейшим из которых является тип файла. Кроме этого используются ключевые слова и образцы, однако самой уникальной функцией является запатентованный компанией алгоритм создания «отпечатков» содержимого, способный идентифицировать неструктурированные данные на любом из возможных направлений их потери. Алгоритм использует статистическую модель документа для его идентификации слепком, имеющим размер менее 120 байт. Такой размер позволяет определять большое количество документов в конечной точке без подключения к центральному серверу. В отличие от метода контрольной суммы, данный способ невосприимчив к изменениям в документе и не создает больших баз данных контрольных сумм для одного документа. Ключом к работе алгоритма отпечатков (Data DNA) является идентификация значимых маркеров в документе на основании частоты и распространения.

Для идентификации конфиденциальной информации могут быть с помощью шаблонов сгруппированы четыре типа цифровых ресурсов. Для неструктурированных данных идеальным является применение алгоритма Data DNA, а для структурированных лучше подойдет сочетание пароля и регулярных выражений (образцов). Поиск структуры любого набора данных может быть достаточно сложным, но благодаря классификации данных и учету семантики данных можно изолировать маркеры в данных, которые могут быть расположены в качестве цифровых ресурсов.

Trend Micro, как и любой другой поставщик DLP-решений, не дает гарантий эффективности системы предотвращения утечек — каждому пользователю рекомендуется провести тестирование решения в конкретной среде и с реальными данными, чтобы доказать его действенность. Однако 100%-ного решения проблемы потери данных нет, и большинство организаций смотрят на нее с той точки зрения, что «сначала нужно закрыть самые крупные дыры». Обычно это USB-накопители, сообщения корпоративной электронной почты, общедоступная информация в Сети, и во многих организациях данные методы коммуникации являются частью бизнес-процесса. Всегда можно найти баланс между свободным потоком информации и безопасностью, причем кроме технологий на уровень защиты от потерь данных очень влияет человеческий фактор и условия процесса.

*— **Раймунд Генес** (russia@trendmicro.com) — технический директор компании Trend Micro*

В 2005 году нынешний руководитель аналитической компании Deloitte Research Уильям Эггер ввел понятие Government 2.0, а в 2010 году состоялась конференция Gov 2.0 Expo, посвященная применению технологий Web 2.0 к задачам электронного правительства.

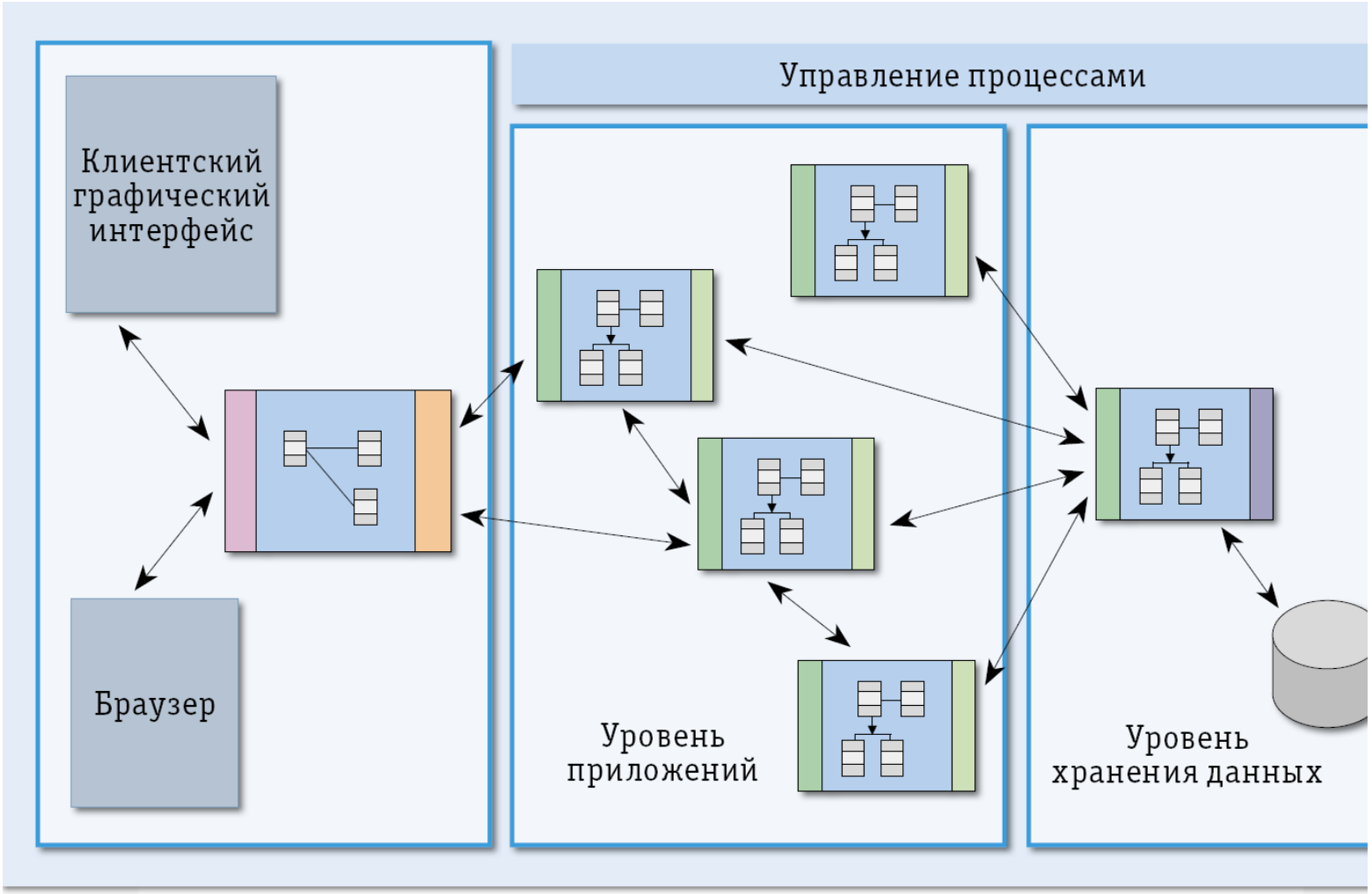

Рис. 1. Архитектура системы электронного правительства

Из выступлений на конференции можно сделать вывод: Government 2.0 должно представлять собой платформу, повышающую продуктивность правительства и позволяющую постоянно развивать набор предоставляемых населению сервисов. Как иронично сказал организатор конференции Тим О'Рэйли, "система Government 2.0 должна не только помогать политикам быть избранными, но еще и стимулировать их лучше выполнять свою работу". С технической точки зрения эта система должна обладать рядом качеств.

- **Способность к преобразованию.** Это предполагает наличие внутри правительства собственных инновационных механизмов, прозрачность функционирования, сотрудничество между всеми участниками процесса управления и участие в нем граждан. Об этих чертах Government 2.0 говорил и Барак Обама в свой речи "Прозрачность и открытое правительство" (Transparency and Open Government).
- **Многоуровневая модель взаимодействия.** Реально уровней взаимодействия может быть больше, но в наиболее обобщенном виде можно говорить о трех – между работниками одного ведомства, между разными ведомствами и между ведомствами и гражданами.
- **Поддержка социальных сетевых медийных сервисов.**
- **Подчиненность решаемым задачам и итерационный характер процессов.** Задачи решаются в повторяющемся цикле: постановка, решение, оценка результата, внесение корректив вплоть до получения решения нужного качества.

Закон Эшби

Закон необходимого разнообразия, сформулированный Уильямом Россом Эшби, входит в число эмпирических, образно отражающих замеченные свойства природной или техногенной среды. Пик славы английского психиатра Эшби пришелся на 60-е годы XX века – он вошел в историю науки как один из первых исследователей в области кибернетики и теории сложных систем. Закон его имени звучит следующим образом: "При создании сложной системы необходимо, чтобы такая система имела большее разнообразие, чем разнообразие решаемой проблемы, или была способна создать такое разнообразие. Иначе говоря, система должна обладать возможностью изменять свое состояние в ответ на возможное возмущение. Разнообразие возмущений требует соответствующего ему разнообразия возможных состояний. В противном случае такая система не сможет отвечать задачам управления, выдвигаемым внешней средой, и будет малоэффективной. Отсутствие или недостаточность разнообразия могут свидетельствовать о нарушении целостности подсистем, составляющих данную систему".

Хотя закон Эшби имеет простую вербальную формулировку, из него следуют серьезные выводы в самых разных областях человеческой деятельности, в том числе и в социальной сфере. Например, опираясь на него, несложно показать бесперспективность простых "вертикальных" систем управления обществом и появление отклонений от вертикали как следствие

недостаточности разнообразия в системе власти. Закон Эшби явным образом ограничивает возможности автоматических систем управления в технике и автоматизированных систем управления в бизнесе. Потенциал применения этих систем ограничен свойственной им сложностью. Проще говоря, сложность системы управления не может быть ниже сложности системы, которой она управляет, простая система не может быть использована для управления сложным объектом. Игнорирование закона Эшби является причиной многих социальных и техногенных катастроф.

Еще в 1962 году академик Виктор Глушков выдвинул идею «Общегосударственной автоматизированной системы учета и обработки информации» (ОГАС) – ее создатели верили или делали вид, что верили, в возможности механизма плановой экономики, то есть пытались представить экономическую систему страны намного более простой, чем она была на самом деле. Они считали, что могут создать систему управления, сопоставимую по сложности с экономической системой огромной страны, где неписанные правила и понятия имели отнюдь не меньшее значение, чем прокламированные нормы. Разумеется, никакие компьютерные технологии того времени не могли быть поставлены в соответствие с реальным экономическим механизмом. По степени идеализации реальной жизни конкуренцию ОГАС могла составить система «Киберсин» (1971 год), разработанная Старфордом Биром и ставшая одной из причин переворота, устроенного в Чили военными под руководством Аугусто Пиночета.

Облачное будущее

Вместе с облаками все ИТ переходят в новую фазу своего существования, область действия грядущих изменений распространяется на персональную деятельность, на работу корпораций и на государство в целом. Этому переходу способствуют основные преимущества облаков: повсеместность и открытость доступа из любой точки; надежность и готовность, превышающие возможности любой отдельно взятой системы; возможность выбора различных облачных платформ; сохранение приватности данных и безопасность; экономические преимущества и уверенность в дальнейшем развитии. Раскрытие этих преимуществ зависит не только от прогресса в технологиях, но и от ряда психологических моментов. Немалое значение имеет инертность мышления, стоит напомнить, как было сложно тем, кто вырос на мэйнфреймах, перейти на клиент-серверные архитектуры, а сегодня точно так же будет сложно отказаться от собственных компьютеров в пользу облачных ресурсов. Основная надежда на смену поколений профессионалов – преимущества облаков проявятся в полной мере, когда лидерами станут представители поколения, воспитанного на использовании Web-ресурсов.

Распространению облаков препятствует целый ряд факторов. Те, кто пошли по облачному пути, отмечают, что дело не в технологиях, а в смене культурной парадигмы. Нужно сделать насилие над собой, чтобы допустить возможность выхода данных и приложений за корпоративные стены. Переход к

облакам с неизбежностью затронет структуру занятости в ИТ, уйдет в прошлое рутинная работа с настройкой ПО, разнообразная деятельность по администрированию, работа с оборудованием серверов и систем хранения. В целом можно сказать, что ИТ станет в большей степени занятием для белых воротничков, чем для голубых. Еще одна проблема — интернационализация; облачные услуги легко пересекают границы, уже сейчас страны Евросоюза обеспокоены конкурентными преимуществами заокеанских поставщиков, но именно эта угроза несущественна для частных правительственных облаков.

Несмотря на неизбежные сложности, уже сейчас можно говорить о сложившихся путях миграции в облака и общих выводах, сделанных теми, кто пошел по ним. И один из выводов состоит в том, что не следует менять местами цель и средство – облака, как бы они ни были важны, остаются средством или инструментом, а не конечной стратегической целью.

План Cloud First

План с характерным названием Cloud First по созданию современного электронного правительства, представленный Вивеком Кундрой в декабре 2010 года, привлек к себе колоссальное внимание. Весь план разбит на шесть разделов, и собственно облакам посвящен первый, состоящий из шести пунктов.

1. Консолидация центров обработки данных. В 1998 году деятельность федеральных органов власти США поддерживало 432 ЦОД, к 2010 году их число увеличилось до 2094, а согласно входящей в план Cloud First инициативе по консолидации центров обработки данных Federal Data Center Consolidation Initiative, к 2015 году их число должно быть сокращено до 800. Эту задачу будет решать специально созданная команда Data Center Consolidation Task Force. Реализация FDCCI позволит сократить затраты энергии, площади, стоимость аппаратного и программного обеспечения, эксплуатационные расходы.
2. В ближайшие полтора года намечено создать внутриправительственную торговую площадку, с помощью которой наладить обмен высвобождающимися мощностями, площадями и оборудованием.
3. Сдвиг технической политики в сторону Cloud First. Существующие государственные информационные системы уступают частным; например, системы поддержки видео по заказу могут обеспечивать многократное увеличение мощности (от 50 до 4000 виртуальных машин) за три дня, а государственные системы, которые должны иметь способность адаптироваться к пиковым нагрузкам, такими возможностями не обладают. Программа Cloud First должна обеспечить преимущество по трем позициям: экономичность – оплата за услуги по мере их использования сокращает начальные инвестиции и позволяет контролировать затраты в процессе эксплуатации; гибкость – изменение потребных программных и аппаратных ресурсов может осуществляться по мере необходимости; скорость – сокращаются до минимума затраты времени на развертывание и сертификацию. Основная нагрузка по

разработке Cloud First ложится на Национальный институт стандартов и технологий (NIST). Предполагается очень высокий темп внедрения, значимые результаты должны быть получены в течение 12 – 18 месяцев.

4. Контракты с основными производителями позволят в течение 12 месяцев начать предоставление инфраструктурных сервисов основным федеральным ведомствам (облачные системы хранения, виртуальные машины). В полном объеме эта программа потребует 18 месяцев.

5. Контракты с основными SaaS-провайдерами должны обеспечить работу электронной почты, а позже должны быть внедрены другие сервисы.

6. Система сервисов должна быть построена так, чтобы их можно было без дублирования распределять между различными подразделениями и ведомствами.

Следующей по важности проблемой Кундра считает отсутствие необходимого управления программными разработками, поэтому вторая часть плана (пункты 7 – 12) содержит меры, направленные на преодоление этой слабости: подготовка специалистов по управлению разработкой ПО; мероприятия, ставящие целью создание консолидированных команд разработчиков; обмен опытом и кадрами между отдельными коллективами для создания в конечном итоге сообщества высокопрофессиональных программистов, работающих на государство.

Состоящая из четырех пунктов третья часть (пункты 13 – 17) посвящена совершенствованию процесса закупки оборудования и ПО, а оставшиеся носят административный и организационный характер.

Частные облака государственного масштаба

За исключением облаков, создаваемых Пентагоном, в США осуществляются программы по развертыванию частных облаков шести крупнейших ведомств: Администрация общих служб (General Services Administration, GSA), Национальное агентство по аэронавтике (National Aeronautics and Space Administration, NASA), Министерство внутренних дел (Department of the Interior), Министерство здравоохранения (Department of Health and Human Services), Бюро переписи (Census Bureau) и Белый дом (White House).

GSA заключила договор с провайдером Terremark Worldwide на поддержку двух порталов: USA.gov и испаноязычного GobiernoUSA.gov, на которые ежегодно приходят более 140 млн обращений. Практика показала, что это решение способно справляться с пиковыми нагрузками. Использование гибридной модели (сочетание частного и публичного облака) было сознательным, целью было показать другим ведомствам реальную возможность выхода из собственных четырех стен. Дальнейшее развитие этого облака предполагает создание сервисов IaaS.

NASA запустило свою платформу NEBULA с несколькими целями. Во-первых, для реализации программы по облечению доступа к данным, во-вторых, для предоставления сервисов SaaS, IaaS, PaaS. Платформа Nebula

позволяет создать сверхмощное хранилище данных на базе кластерной файловой системы Lustre. Ресурсы Nebula используются внутри NASA и обеспечивают кооперацию с учеными, работающими вне этой организации.

Национальный бизнес-центр National Business Center (NBC) Министерства внутреннии дел является провайдером услуг для федеральных агентств и учреждений; центр специализируется на облачном ПО для финансовых услуг и управления государственными закупками. Облачный центр программ поддержки Program Support Center в составе Министерства здравоохранения обслуживает более 60 организаций, входящих в состав министерства. Бюро переписи населения выбрало комбинированную схему – для поддержки партнерских организаций (более 100 тыс.) используется схема SaaS от Salesforce.com, а данные хранятся в собственном частном облаке. Администрация президента применяет Google Moderator для координации собственной деятельности.

IBM CloudBurst — облако из коробки

Руководствуясь известным правилом: "За покупку у IBM не уволят", чиновники, руководящие созданием облаков для государственных нужд, из Китая, Вьетнама и ряда других стран отдают предпочтение продукту IBM CloudBurst, который предназначен специально для создания крупномасшабных частных облаков. Для осуществления подобных крупных проектов нужен соответствующий по своим возможностям партнер, который должен не только обладать передовыми технологиями, но и быть способным к оказанию сервисной и финансовой поддержки. По совокупности качеств выбор в пользу IBM достаточно аргументирован, тем более что интегрированное решение IBM CloudBurst, его еще называют "облаком из коробки", включает в себя все необходимое для создания облаков: вычислительные системы, ресурсы хранения, сетевое оборудование, средства виртуализации и программное обеспечение для управления сервисами.

Первая версия CloudBurst (burst – "ливень") была выпущена летом 2009 года. Система собирается из управляющих серверов System x 3650 M2 и серверов-лезвий HS22 Nehalem, образующих облако виртуальных машин. Программное обеспечение включает встроенный гипервизор VMware ESXi 3.5, а также Tivoli Provisioning Manager V7.1, Monitoring V6.2.1 и Systems Director 6.1.1. Для виртуализации десктопов могут быть использованы продукты VMware, Citrix Systems, Desktone, Quest или Wyse.

В два этапа – осенью и в начале зимы 2010 года – IBM представила обновленную версию CloudBurst v2.1, расширенную по отношению к предыдущей версии процессорами Power7. В ней использованы модернизированные серверы HS22V на чипсете Intel 5520, допускающем установку четырехъядерных Xeon 5500 и шестиядерных Xeon 5600. Еще они отличаются увеличенным до 144 или 288 Гбайт размером памяти. В базовом варианте HS22V, которым комплектуется стек CloudBurst v2.1, устанавливается память 72 Гбайт, что позволяет в сочетании с новым гипервизором VMware

ESX Server 4.1 запускать на одном сервере до 30 виртуальных машин. CloudBurst v2.1 выпускается в трех версиях: малая, средняя и большая, которые монтируются в стандартную стойку, имеют один управляющий сервер 3550 M3, но различаются числом лезвий. Младшая модель CloudBurst v2.1 комплектуется системой хранения System Storage DS3400, а две старшие – модулями System Storage EXP3000, и в результате они могут поддерживать 100, 460 и 960 виртуальных машин.

С декабря 2010 года в состав CloudBurst v2.1 входят серверы IBM Power 750 Express на процессоре Power7 – Unix-серверы, предназначенные для баз данных среднего и крупного масштаба. В них, как и положено этому классу компьютеров, используется технология виртуализации PowerVM для платформ IBM AIX и Linux, позволяющая динамично настраивать ресурсы системы в зависимости от нагрузки на каждый из разделов, а также Active Memory Expansion – новая технология Power7, благодаря которой эффективный максимальный объем памяти может значительно превышать объем имеющейся физической. Инновационный механизм упаковки содержимого памяти позволяет в некоторых случаях увеличить ее объем вдвое, что позволяет повысить эффективность каждого раздела или создавать больше логических разделов при том же физическом объеме памяти. У IBM Power 750 имеется еще целый ряд перспективных новаций: Intelligent Threads, Intelligent Cache, Intelligent Energy и Light Path Diagnostics. Причины выбора Power 750 Express высотой 4U, а не серверов-лезвий PS700, PS701 или PS702 Express остаются загадкой – выбор лезвий на Power7 выглядел бы вполне логично, ведь они могли бы обеспечить вдвое большую плотность виртуальных машин, чем серверы HS22V; возможно, разгадка будет дана в CloudBurst v3.

Облака на Востоке

Проект создания "Цифровой Японии" (Digital Japan Creation Project) был разработан национальным Министерством внутренних дел в 2009 году. Данный проект еще называют ICT Hatoyama Plan по имени руководителя этого ведомства Кунио Хатоямы. Рассчитанный на 10 лет, проект отличается масштабностью и предполагает создание 300-400 тыс. дополнительных рабочих мест в области информационных и коммуникационных технологий и удвоение объема соответствующего сегмента рынка за этот период. В первую очередь предполагается более полно использовать существующий потенциал цифровой индустрии и создавать новые производства. В дополнение к этому ставится целью более широкое использование беспроводных технологий, например взаимодействие между движущимися автомобилями для снижения аварийности. Для этого потребуется рационализировать использование радиочастотного диапазона, который в новых условиях рассматривается как один из важнейших национальных ресурсов. Возможности, предоставляемые всеми этими технологиями, позволят изменить организацию общественной жизни, в том числе решить проблему цифрового неравенства, трансформировать сферы потребления, образования и здравоохранения.

Показательно, что в таких многопрофильных корпорациях, как Hitachi, более приоритетными становятся технологии работы с данными, чем традиционные электро- и машиностроительные.

Центральное место в плане Хатояма отводится правительственному облаку Kasumigaseki, названному по имени квартала в Токио, где расположены министерства и ведомства, но не стоит упускать из виду, что речь идет о Японии и название более символично. Kasumigaseki состоит из kasumi, означающего "туман", и seki, означающего "ворота или проход", и переводится как "туманный проход". Создание этого "частного" по принятой классификации облака настолько значительная проблема, что ее рассматривают как инициативу национального масштаба, разделяя на две задачи: во-первых, обеспечение высочайшего уровня сервисов во взаимодействии между населением и правительством, а во-вторых, создание национальной базы знаний.

Kasumigaseki Cloud (рис. 2) будет разрабатываться очередями и внедряться начиная с 2015 года. Облако должно стать консолидированной аппаратно-программной платформой, позволяющей рациональным образом распределять функции между 1800 министерствами, ведомствами и другими государственными учреждениями. С технической точки зрения облако должно способствовать сокращению затрат, энергии и штата ИТ-персонала. Конечная цель для правительства – сокращение системной сложности, минимизация числа обращаемых документов, исключение дублирования и т. д., а для граждан – упрощение процедур взаимодействия с госорганами. Национальный цифровой архив (National Digital Archive) должен быть снабжен средствами доступа к хранилищу государственных документов, книг, научных публикаций, культурных артефактов, географической/геологической информации, статистических данных.

Облако должно быть построено исключительно японскими телекоммуникационными компаниями и быть частным по своей природе. Учитывается тот факт, что по местным законам хранение персональных данных на серверах, расположенных вне страны, запрещено, правительство даже не рассматривает потенциальную возможность переноса данных и приложений в глобальные облака.

В Китае пока нет общенациональных облачных проектов, а среди локальных наиболее интересен проект под названием "Облачный компьютерный центр Желтой реки" (Yellow River Delta Cloud Computing Center), создаваемый в городе Дунъин провинции Шаньдун, будущем гигантском мегаполисе, основанном в 1983 году как база для развития дельты Хуанхэ и нефтяного месторождения Шэнли. Проект предполагает создание "умного города" (Smarter City), где компьютерные технологии не только поддерживают функционирование гражданского общества, но и являются инфраструктурной основой для всего экономического развития.

Рис. 2. Туманный проход

Дунъин должен стать "городом цифровых инноваций". Здесь облако, построенное IBM, должно способствовать преобразованию всего производственного комплекса от традиционного промышленного экономического образца в комплекс, построенный на принципах *сервисной экономики* (services-based economy).

Сначала Yellow River Delta Cloud Computing Center станет платформой для разработки ПО для автоматизации нефтедобычи и всей цепочки поставок нефтепродуктов, на второй фазе будут созданы "умный аэропорт", "умные дороги", на третей фазе облачные услуги распространятся на здравоохранение и коммунальные службы. Меньший по масштабам проект реализуется в городе Уси, что значит "нет олова", – так был переименован город Юси после того, как были выработаны находившиеся здесь оловянные рудники. Взамен них в Уси создается "софтверный парк", тоже построенный IBM, он должен предоставлять вычислительные ресурсы по заказу молодым компаниям.

В Таиланде правительственное информационное агентство Government Information Technology Service реализует не столь грандиозную, как в Японии, облачную задачу и для начала перевело в облако электронную почту, а теперь внедряет модель SaaS, с тем чтобы консолидировать ресурсы и сократить затраты. Во Вьетнаме для разработки национальной облачной стратегии привлечена лаборатория IBM Cloud Labs. Здешнее правительство видит в облаке путь для перевода страны на экономику, базирующуюся на услугах services-lead economy.

Облако по-английски

Проект британского облака G-Cloud является одной из важнейших частей более крупного стратегического проекта Government ICT Strategy, который должен объединить около 400 министерств, ведомств и других организаций. Первая фаза проекта была запущена в эксплуатацию в минувшем году, а промежуточный финиш намечен на 2013-2014 годы. Проект позволит сократить на 3,2 млрд фунтов ежегодный ИТ-бюджет правительства, составляющий 16 млрд. Основной исполнитель проекта – бристольская лаборатория HP Labs, известная своими исследованиями в области utility computing. Функции, возложенные на G-Cloud, вполне традиционны для систем этого класса, а вот форма их демонстрации действительно необычна. В ноябре был торжественно открыт "театр" HP G-Cloud Theatre, где пользователь может потрогать руками все, чем богата система G-Cloud. Одна из главных задач, решаемых таким образом, – избавление от предрассудков по отношению к облакам, прежде всего от сомнения в их безопасности.

ПОДЗЕМНОМУ ХРАНИЛИЩУ В ЛУИСВИЛЛЕ, ШТАТ КЕНТУККИ 10 ЛЕТ

Источник: http://www.undergroundvaults.com/news/happy-10-year-anniversary-to-underground-vaults-storage-in-louisville-kentucky/

Десять лет назад, всемирно признаная компания UVS занимающаяся хранением микрофильмов, документов и других ценностей расширила свою деятельность со Среднего Запада в Луисвилл, штат Кентукки. Подземное хранилище было оборудовано в одном из самых безопасных мест штата Кентукки в бывшей шахте по добыче известняка с объемом более 4000000 квадратных футов. Свою деятельность компания UVS начала с управления записями и хранилища для долгосрочных клиентов. В начале хранилище занимало площадь всего лишь 5500 квадратных метров. Занимаясь исключительно обслуживанием клиентов и обеспечением безопасного хранения, выделенные площади были быстро заполнены и потребовалось дополнительное пространство. Сегодня, десять лет спустя, компания UVS занимает около 100 000 квадратных метров подземного хранилища в Луисвилле, в котором имеется холодильная камера для хранения при низких температурах. При хранении материалов используются штрих-коды и соответствующие сканеры. Каждая коробка плёнки и каждое место хранения помечены уникальным штрих-кодом. Для поиска используются автономные сканеры для считывания штрих-кодов снимаемых с полок и возвращаемых на место материалов.

Практика подземного хранения вещей восходит к записям ранних цивилизаций. На самом деле, большая часть информации, которую мы обнаружили об этих ранних культурах сохранилось на протяжении веков потому, что была похоронена под землей.

В подземельях Египетские фараоны осуществляли уход за священным религиозным текстами, диктаторы хранили украденные во время Второй мировой войны артефакты, люди сохраняли свои самые ценные активы. Поэтому, когда основатели подземелья начали искать безопасное место для хранения записей актов гражданского состояния, эти истории вызвали идею создания подземного хранилища. В результате сложившихся обстоятельств, в Европе после Второй мировой войны было восстановлено похищенное имущество, которое Гитлер спрятал в бункерах и соляных шахтах Германии. Артефакты в хранилищах были найдены в идеальном состоянии.

Для обсуждения идеи по обеспечению хранения записей компании в соляной шахте Кэрри, на глубине 650 футов под землей, собрались шесть человек. Результатом этих обсуждений ознаменовано рождение подземного хранилища. И не потребовалось дополнительных затрат, чтобы убедить первых клиентов в преимуществах по защите ценностей которые предоставляются в соляной шахте. Сегодня, UVS надежно хранит важные материалы для правительства и физических лиц, музеев и частных коллекционеров, фотопленки крупных киностудий и микрофильмы, услугами хранилища пользуются магнаты Уолл-стрит и основные бутики улицы.

ЗМІСТ