Беречь информацию, как зеницу ока

Хранение и обработка информации требуют комплексного подхода

Текст: Оксана Дяченко

Современный банковский бизнес невозможно представить без огромных массивов данных, которые необходимо получать, хранить, перерабатывать. Причем объемы этой информации ежегодно увеличиваются в среднем вдвое. Финансовая информация стоит огромных денег, неудивительно, что ее хранение и сопутствующая этому защита обходится банкам недешево.

Требования, в том числе регуляторов банковского рынка, к безопасности обработки данных и к обеспечению сохранности информационных систем и ресурсов постоянно ужесточаются. Финансовые организации вынуждены адекватно реагировать на данные ужесточения. Кроме того, в их собственных интересах обеспечивать надежное функционирование систем хранения и обработки информации.

СИСТЕМЫ ОБРАБОТКИ И ХРАНЕНИЯ ДАННЫХ

Быстрый рост объемов информационных ресурсов диктует необходимость принципиально новых подходов к хранению и обработке данных. Стоимость восстановления информации равна стоимости приобретения. Неудивительно, что вопрос сохранности бизнес-информации имеет большое значение в современном мире.

Эксперты утверждают, что из-за применения устаревших технологий происходит рассредоточение важных данных по вычислительным и информационным ресурсам. В такой ситуации организация несет неоправданные затраты на решение основных задач управления данными, среди которых выделяются следующие. Во-первых, обеспечение авторизованного доступа к данным и их защита от несанкционированного доступа. Во-вторых, управление резервным копированием и архивированием данных. В-третьих, расширение дисковой емкости. Наконец, восстановление данных после сбоев.

Системы хранения и обработки информации обеспечивают необходимую непрерывность бизнес-процессов и сохранность данных. Такие решения применимы в организациях с самым разным уровнем автоматизации и информатизации бизнес-процессов: от предприятий с начальной стадией автоматизации до организаций, использующих крупные ERP-системы.

На рынке в настоящее время предлагаются различные интегрированные решения. Среди них: виртуализация вычислительных ресурсов серверов предприятия, построение кластерных систем (локальных и территориально-распределенных), консолидация приложений (логическая, географическая, гомогенная, гетерогенная), использование blade-серверов для построения мини-ЦОД, консолидация данных. Кроме того, к интегрированным решениям относят создание систем хранения на основе технологий SAN и NAS, проектирование и реализацию резервных площадок центров обработки данных, репликацию данных на удаленные площадки, резервное копирование и восстановление информации, создание инженерной обеспечивающей инфраструктуры, мониторинг и управление вычислительными и инженерными системами.

ЧЕТЫРЕ ТИПА СИСТЕМ

Для организации сохранности информации применяются системы хранения данных (СХД), которые представляют собой комплексное программно-аппаратное решение.

В настоящее время существуют четыре основных типа систем хранения данных. Во-первых, DAS-системы – непосредственно подключаемые к вычислительной системе диски по каналу SAS в режиме «точка-точка». В данном решении в системе хранения данных использу-

ется SAS-экспандер, позволяющий подключать большое количество дисков по внешней четырехканальной магистрали.

Во-вторых, NAS-системы, которые знакомы большинству сотрудников, использующих в локальной сети своей организации файловый сервер. Файловый сервер – это NAS: устройство, подключенное в локальную сеть и предоставляющее доступ к своим дискам по одному из протоколов сетевых файловых систем. Такие устройства пользуются популярностью из-за относительно невысокой цены, несложной настройки и достаточно высокой надежности.

В-третьих, SAN-системы, позволяющие использовать блочные методы доступа и обеспечивающие хранение «нефайловой» информации (часто используются для баз данных). Некоторые приложения работают только с «локальными дисками» (т.е. с NAS) и не работают на SAN.

Наконец, серверы хранения данных – система, изначально ориентированная на отказоустойчивую работу с информацией. В таком сервере все компоненты являются отказоустойчивыми и, по сути, организуются в кластер. Фактически у пользователя есть два сервера, соединенных высокоскоростным каналом, позволяющим без остановки работы переходить с одной части на другую.

ЭКСПЕРТНОЕ МНЕНИЕ

Дмитрий СЛОБОДЕНЮК,
коммерческий директор Arinteg

Информационная безопасность для любой организации является приоритетной задачей, так как утечка критически важной для бизнеса информации может повредить не только финансовому состоянию и репутации предприятия, но и привести к потере им экономической или финансовой самостоятельности.

Чтобы увеличить уровень надежности внутренних бизнес-процессов, нужно обеспечить защиту информации от уничтожения (как умышленного, так и случайного), кражи и внесения в нее несанкционированных изменений. Наиболее эффективное обеспечение информационной безопасности достигается за счет комплексного подхода, который включает в себя организационные и технические меры защиты. Основными принципами построения систем информационной безопасности являются: системность подхода, комплексность решений, непрерывность защиты, разумная достаточность средств защиты, минимум неудобств для пользователей, минимум накладных расходов на функционирование механизмов защиты.

Частью комплексного подхода обеспечения информационной безопасности может стать защищенный дата-центр. Такой подход считается эффективным, однако банк должен определить, создавать собственный центр обработки данных (ЦОД) или воспользоваться услугами на условиях аутсорсинга. В случае принятия банком решения об аутсорсинге услуг стороннего дата-центра необходимо тщательно подойти к выбору поставщика, чтобы минимизировать риски утечки конфиденциальной информации и обеспечить бесперебойную работу бизнеса.

Во-первых, аутсорсинговый дата-центр должен иметь достаточно высокую категорию отказоустойчивости – не ниже TIER-III.

По международной классификации ЦОД TIA-942 дата-центры делятся на четыре категории по степени отказоустойчивости:

- ЦОД первого и второго классов подходят компаниям малого и среднего бизнеса, так как по показателям надежности не обеспечивают бесперебойную работу бизнеса;
- ЦОД третьего и четвертого классов обеспечивают непрерывность бизнес-процессов и востребованы крупными финансовыми учреждениями, телекоммуникационными компаниями, территориально распределенными корпорациями.

Соответствие дата-центра международному стандарту по категории TIER-III гарантирует качество предоставляемых услуг, то есть это означает, что ЦОД обладает необходимыми ресурсами для обеспечения бесперебойной и безопасной работы:

- технологическая площадка – специализированные телекоммуникационные технические средства и оборудование для хранения и распределения информации, размещенные в специальном помещении, в котором созданы нормативные условия для безотказной работы оборудования, а также средства безопасности и контроля доступа;
- мониторинг – полноценный контроль над аппаратно-программным комплексом и информационными системами;
- резервное копирование – регулярное резервное копирование данных;
- обеспечение информационной безопасности – многоуровневая система защиты информации, быстрое реагирование на инциденты, контроль входящего трафика, DDOS-устойчивость, надежная антивирусная защита и т.д.;
- техническая поддержка – круглосуточная поддержка оборудования и программных средств для обеспечения бесперебойной работы дата-центра.

Во-вторых, требуется уделить особое внимание юридическому аспекту, так как перемещение вычислительных мощностей в ЦОД влечет за собой определенные риски для банка.

Договор с дата-центром должен учитывать все нюансы оказываемых услуг, наиболее важные из которых – вопросы конфиденциальности и соглашение об уровне обслуживания (SLA) с условиями, детально оговаривающими уровень услуг, поставляемых провайдером, и возможности управления их составом.

КОМПЛЕКСНЫЙ ПОДХОД

Для того чтобы обеспечивать надежное хранение и защиту данных, лучше всего, по мнению специалистов, применять комплексный подход, суть которого заключается в проведении ряда организационных мер (регламентов, процессов) и в наличии некоторых технических решений. На первый взгляд, способы защиты информации достаточно просты. Среди них выделяют: разграничение доступа, управление изменениями, дублирование информации в режиме онлайн, резервное копирование, территориальное разнесение копий информации.

Каждый из этих способов не может быть эффективен по отдельности. Наиболее результативным является применение всех вышеперечисленных мер в сочетании с четкой регламентацией действий персонала и автоматических операций с данными.

Информация, которая хранится в банке, должна быть в первую очередь упорядочена. Ее необходимо разделить по типам и направлениям бизнеса, определить ее критичность для организации, строго разграничить доступ к данным не только для сотрудников, но для администраторов. При этом рекомендуется выбрать способ и регламент защиты индивидуально для каждого вида информации.

«Все элементы инфраструктуры хранения и обработки информации должны быть надежны, производительны и дублированы, – говорит заместитель председателя правления банка «Союз» Владимир Смирнов. – Достаточно иметь одно слабое звено в системе, и она вся становится ненадежной и/или непроизводительной. Строго регламентируйте процесс внесения изменений в структуру данных, создание новых информационных ресурсов – опирайтесь на точное знание картины информационного пространства своей организации, чтобы эффективно его защищать».

Очень сложно защитить разрозненно хранящиеся части информации, кроме того, ими невозможно эффективно управлять. Поэтому следует консолидировать хранение данных на высокопроизводительных и надежных системах хранения, а не на локальных дисках серверных систем. «Гибкость в управлении данными даст вам лишний козырь в организации их защиты, кроме того, в конечном счете, так выйдет дешевле», – уверен Владимир Смирнов.

Для лучшего обеспечения сохранности информации специалисты советуют дублировать и распределять ее. Для особенно критичных данных применяется дублирование между территориально разнесенными ЦОДами, для менее критичных – достаточно асинхронной репликации, считает Владимир Смирнов. Распределив хранилища информации по различным ЦОДам, можно избежать необходимости перехода на резервные системы хранения для значительной части информационных ресурсов в момент выхода из строя одного из центров. «Важно отметить, что недопустимо консолидировать данные без их дублирования – делать это нужно обязательно комплексно», – подчеркивает эксперт банка «Союз».

Вице-президент банка БКФ Михаил Геворков также подчеркивает важность дублирования информации в целях минимизации последствий выхода оборудования из строя. Современная техника позволят обеспечить бесперебойность работы и сохранение данных. И вопрос здесь только в цене: сколько денег банк готов потратить на ИТ, чтобы избежать потери важной информации.

Существенный момент в процессе хранения данных – резервное копирование. Только периодическое копирование информации на отчуждаемые носители, которые хранятся отдельно от ЦОД, может гарантировать сохранность данных. Если персонал допустит ошибку, в результате которой данные будут искажены, они будут также искажены на всех резервных системах. И только резервная копия будет хранить верную информацию.

Данное копирование потому и называется резервным, что избыточные копии файлов и каталогов сохраняются на сменный носитель просто «на всякий случай». Резервное копирование следует проводить ежедневно – при этом копируются все новые или измененные файлы, так что они наверняка будут доступны для восстановления.

«Резервное копирование» – это целая наука, говорят специалисты, практически отдельная отрасль информационного бизнеса. Это понятие включает в себя методологию, специализированные аппаратные и программные средства.

Для резервного копирования информации применяются, в первую очередь, ленточные накопители, реже – магнитооптические диски, перезаписываемые CD или сетевые массивы жестких дисков. Простейшие программы резервного копирования встроены в любую операционную систему.

Эксперты утверждают, что следование изложенным выше рекомендациям позволяет банкам исключать возможность потери бизнес-данных.

НАСУЩНЫЕ ПРОБЛЕМЫ

Проблемы, которые наиболее часто возникают при организации хранения и защиты данных, можно разделить на несколько групп. Во-первых, вопросы, связанные с финансированием тех или иных ИТ-проектов. Затраты на инфраструктуру хранения данных должны быть ясны и понятны бизнесу. Обосновать все издержки будет проще, если представить на рассмотрение комплексное видение всего проекта, считают ИТ-специалисты. Наличие у банка плана непрерывности бизнеса серьезно облегчает финансирование ИТ-проектов.

Вторая группа проблем связана с необходимостью структурировать информацию и бизнес-данные. «Зачастую исторические наслоения информации различной степени актуальности, критичности и направленности хранятся в одной большой «куче», – говорит Владимир Смирнов. – Существенно упростить решение этой проблемы мож-

АКЦЕНТ

Из-за применения устаревших технологий происходит рассредоточение важных данных по вычислительным и информационным ресурсам. В такой ситуации организация несет неоправданные затраты на решение основных задач управления данными, среди которых выделяются следующие. Во-первых, обеспечение авторизованного доступа к данным и их защита от несанкционированного доступа. Во-вторых, управление резервным копированием и архивированием данных.

но, заинтересовав пользователей в самостоятельной реорганизации информации и разборке завалов. Например, вместо того чтобы увеличивать ресурсы старого файлового хранилища, можно подготовить новое, которое будет производительнее старого. Подготовить структуру хранения файлов, предложить пользователям самостоятельно перенести свои данные в новую структуру (но уже не «в общую кучу»). Обычно такая затея существенно снижает уровень беспорядка».

Третья группа проблем возникает из-за устойчивого нежелания сотрудников документировать свои действия, работать по инструкциям и т.д. Лишь только внедрив четкие правила управления изменениями и разграничив доступ к системам, можно добиться того, что сотрудники станут заинтересованными в появлении регламентов и инструкций. «Они не только станут их исполнять, но даже предложат способы их улучшения», – уверен Владимир Смирнов.

БЛИЖАЙШИЕ ПЕРСПЕКТИВЫ

Каждый банк – это провайдер финансовой информации, и перспектива технологий ее защиты для банков является приоритетной. Поэтому следует ожидать определенных положительных изменений в этой сфере как в ближайшей, так и в дальнейшей перспективе.

Усложнение ИТ-систем, всеобщая виртуализация, «облачные» вычисления – все эти современные тренды окажут свое воздействие на системы защиты хранения данных. Решения по защите должны стать более гибкими, масштабируемыми, управляемыми для того, чтобы сочетать в себе высокую производительность и успешно противостоять современным угрозам.

Эксперты уверены, что новые задачи возникают при изменении самой парадигмы хранения данных – при переходе к технологии database in memory, когда все данные находятся в оперативной памяти и их защита осуществляется кластеризацией ресурсов, дублированием. Это требует серьезного пересмотра стратегий защиты. Вполне вероятно, что возникнет технология хранения зашифрованных данных с принципиально новыми методами индексации и поиска.

Учитывая современные тенденции развития ИТ-технологий в мире, таких как SOA, Cloud computing, технологии защиты информации будут развиваться в нескольких направлениях, считает Владимир Смирнов. Во-первых, будут совершенствоваться средства географически распределенного хранения данных с обеспечением избыточности и самовосстановления. Во-вторых, будет осуществляться организация централизованно управляемых инфраструктур хранения (сквозное управление всеми средствами ресурсов хранения и резервного копирования организации), а также виртуализация ресурсов хранения. В-третьих, произойдет увеличение емкости и производительности средств резервного копирования и хранения информации (в том числе за счет твердотельных устройств).

По мнению Михаила Геворкова, большая часть банков, особенно относящихся к третьей-четвертой сотне, постепенно перейдут на аутсорсинг центров обработки данных и переложат на плечи аутсорсеров проблемы защиты. В настоящее время рынок таких предложений еще не сформировался, да и спрос на подобные услуги весьма скромен.

АУТСОРСИНГ ЦОД: «ЗА» И «ПРОТИВ»

Зачастую многие банковские организации даже не рассматривают возможность аутсорсинга ЦОД, опасаясь за сохранность и конфиденциальность корпоративных данных. И это при том, что в профессиональных дата-центрах много внимания уделяется именно вопросам защиты информации, и уровень ее защищенности здесь, безусловно, выше того, который компании могут обеспечить самостоятельно. Современный дата-центр высокой по мировым стандартам категории надежности TIER III+ предполагает наличие мощной кабельной инфраструктуры, систем резервирования электропитания и кондиционирования, средств обеспечения физической и информационной безопасности дата-центра, круглосуточную техподдержку силами квалифицированных и опытных ИТ-специалистов. Кроме того, в таком дата-центре осуществляются круглосуточный мониторинг всех элементов ИТ-инфраструктуры, автоматическое резервное копирование данных, неограниченный доступ в Интернет, а также заключение с заказчиком соглашения об уровне услуг (SLA), которое предусматривает штрафы за его несоблюдение.

Подключение дата-центра к сетям электроснабжения, аренда помещений, сложная инженерная инфраструктура, содержание штата квалифицированного персонала – все это с каждым годом обходится дороже, поскольку технологии производства ИТ-оборудования постоянно эволюционируют.

Конечно, говоря об аутсорсинге услуг ЦОД, нужно четко представлять себе и возможные риски. Они, безусловно, есть и особенно высоки на стадии выбора поставщика услуг. Кроме того, результат аутсорсингового проекта в значительной степени зависит от содержания заключенного договора. Тем не менее рынок услуг ИТ-аутсорсинга постоянно растет, ужесточается конкурентная среда, повышаются качество услуг и гарантии их качества. Кроме того, для многих аутсорсинг услуг ЦОД – это экономически оправданная альтернатива не только содержанию ИТ-инфраструктуры, но и строительству собственного центра обработки данных.

Безусловно, крупнейшие финансово-кредитные учреждения имеют собственные ЦОДы. Например, центры обработки данных Сбербанка, ММВБ, РТС, Хоум Кредит Банка входят в десятку крупнейших в России.

Отдельно следует упомянуть о строительстве нового центра удвоенной мощности, которое ведет Сбербанк в Москве. По словам заместителя председателя правления Сбербанка Станислава Кузнецова, полный ввод высокотехнологичного комплекса инженерно-технических систем – «Мега ЦОД» – планируется в конце октября текущего года. Станислав Кузнецов отметил, что этот объект не имеет аналогов в России, его цель – консолидация IT-ресурсов Сбербанка. Общая площадь «Мега ЦОД» составляет 16 тыс квадратных метров, площадь под оборудование займет 5 тыс квадратных метров. Стоимость комплекса оценивается в 140-150 млн долларов, оборудования – в 650 млн долларов. Заметим, что данный проект не только не имеет аналогов в России, но и по окончании строительства будет одним из самых крупных дата-центров в Европе.