

Как не потерять данные

Опасность утраты данных и модель угроз

Утрата данных приводит к полной или частичной остановке бизнес-процессов компании. Допустим, потеряны данные ERP-системы и резервной копии нет. При отсутствии данных по клиентам и бухгалтерских расчетов организация вынуждена простаивать. А простой — это, как известно, потерянные деньги.

Обеспечить сохранность данных и сократить простой бизнес-процесса позволяет резервное копирование, которое представляет собой комплекс мер против распространенных угроз утраты данных.

Модель угроз данным организации

1. Человеческий фактор: случайные или намеренные действия людей по удалению данных.
2. Отказ оборудования: выход из строя материнских плат, дисков, блоков питания и т. д.
3. Ошибки приложений: вызваны сбоями электропитания, отказом оборудования или вирусной активностью.
4. Форс-мажор: разрушение здания с серверами вследствие обстоятельств непреодолимой силы, таких как землетрясения, цунами, теракт и т. д.

Комплекс мер по восстановлению данных

Прежде чем принимать какие-либо действия против угроз потери данных, нужно составить **план резервного копирования**, который предусматривает:

- описать данные, которые нужно резервировать;

- периодичность резервирования;
- объем резервируемых данных, исходя из времени копирования;
- место, где будут складироваться копии;
- пропускную способность каналов передачи данных.

Наш опыт показывает: чем тщательнее продуман план резервного копирования, тем более результативные меры можно принять против угроз потери данных и построить эффективную систему резервного копирования.

Мера 1: выбор ПО

Программное обеспечение комплексного решения по резервному копированию состоит из клиентской и серверной частей. Серверное ПО устанавливается на сервер, где производится основная настройка системы. Управляется система резервного копирования через консоль администрирования с сервера либо со специально выделенной рабочей станции администратора. Выбор решения для серверной части зависит от используемой в компании операционной системы.

Клиентская часть состоит из агентов, работающих с резервируемыми данными. Выбор агентов определяют составляющие плана резервного копирования и операционная система, на которую устанавливается агент. В зависимости от настроек агентов можно обеспечивать резервирование следующих типов данных:

- приложения, такие как базы данных SQL или почтовые базы Exchange, Lotus, SharePoint;
- файловые ресурсы и диски;
- операционная система.

В зависимости от типа копируемых объектов производятся настройки для их восстановления, в связи с этим мы рекомендуем сделать соответствующую запись в регламенте восстановления данных.



Мера 2: выбор «железа»

Выбор оборудования определяется объемом копирования, требованиями к доступности хранилища и его производительностью. Оптимальным решением является система хранения данных (СХД), работающая по протоколу Fibre Channel или iSCSI. СХД позволяет дублировать дисковую систему, дисковые контроллеры, блок питания и сетевой адаптер — все это помогает построить высокопроизводительную отказоустойчивую систему.

Мера 3: документация резервного копирования

Внедрение системы может считаться законченным только при условии написания регламентов резервного копирования:

- «Регламент резервного копирования» — пошаговое руководство для настройки системы. Здесь также указываются цели резервного копирования: противодействие угрозам утраты данных, восстановление данных, хранение разных версий объектов;
- «Регламент восстановления» — описывает варианты восстановления в каждом из случаев угроз (см. «Модель угроз»). Он позволяет ИТ-персоналу сократить время восстановления данных благодаря четкой схеме действий.

Мера 4: тестирование системы

Как показывает опыт, ИТ-специалисты компаний часто упускают важный шаг — тестирование созданной системы резервного копирования. Попробуйте симулировать сбой системы — и вы узнаете много нового и дополните регламенты полезными сведениями. ●●●