

СОХРАНЕНИЕ И ВОССТАНОВЛЕНИЕ ИНФОРМАЦИИ

Поскольку данные, хранимые компьютерными средствами подвержены потерям и повреждениям, вызываемым разными событиями, важно обеспечить средства восстановления данных. Приведение базы данных точно в то состояние, которое существовало перед отказом не всегда возможно, но процедуры восстановления базы данных могут привести ее в состояние, существовавшее незадолго до отказа.

В процессе эксплуатации информационных систем может происходить разрушение информации по причинам:

- физическое разрушение носителя информации или отдельных частей носителя с информацией;

- аппаратные сбои и разрушение информации;

- программное разрушение информации из-за ошибок в программах;

- воздействие вредоносных программ;

- ошибки оператора (персонала);

- преднамеренное разрушение с использованием различных средств.

Поэтому, обязательным элементом любых ИС являются процедуры сохранения и восстановления информации как защитная мера от разрушения (потери) данных.

Сохранение информации - это процедура получения резервной копии с целью ее последующего использования при ликвидации возможных разрушений информации. При сохранении информации используют

термины *копирование, дублирование, дампование, выгрузка*.

Копирование (сохранение) информации выполняется периодически по графику. Между точками снятия копий сохраняются все данные, которые использовались для внесения изменений в файлы (базы данных). Копирование проводится по схеме "отец-сын", что означает хранение двух копий для двух последовательных процедур копирования.

При файловой обработке между точками снятия копий сохраняют исходные файлы корректур. При работе с базами данных в режиме *онлайн* используют системный журнал и процедуру накопления изменений информации. Системный журнал - это файл, в который вносится информация (протоколируется) о ходе работы информационной системы, включая все изменения баз данных.

Восстановление информации - это процедура ликвидации разрушений данных с использованием сохраненной информации на некоторый момент времени (копии) и возможной корректуры с момента создания копии.

В интерактивных (онлайновых) системах предусматривается несколько уровней восстановления:

- **оперативное восстановление.** Оперативное восстановление используется, когда отдельные изменения в базах данных могут быть отменены при обнаружении ошибок в программах, аргументах поиска данных и т.д.

- **промежуточное восстановление.** Для целей промежуточного восстановления используется метод контрольной точки. *Контрольная точка* - это дампы оперативной памяти и/или областей баз данных, сохраняемый в *системном журнале* в процессе работы информационной системы в определенный момент времени для возможного последующего восстановления работоспособности системы и баз данных на этот момент времени. Контрольная точка создается через заданный интервал времени, через определенное количество изменений в базах данных, при выполнении определенных условий в системе.

- **длительное восстановление.** Используются копии баз данных для восстановления информации и массивы корректур (накопленных изменений).

При проектировании ИС и создании рабочей документации следует процедуры сохранения и восстановления информации выделять особо. Указанные процедуры входят также в состав функций по ведению баз данных.

Ведение базы данных - это комплекс мероприятий по поддержанию данных в актуальном и достоверном состоянии.

Восстановление базы данных — функция СУБД, которая в случае логических и физических сбоев приводит базу данных в актуальное и консистентное состояние.

Журнал транзакций. Восстановление через откат

Реализация в СУБД принципа сохранения промежуточных состояний, подтверждения или отката транзакции обеспечивается специальным механизмом, для поддержки которого создается некоторая системная структура, называемая **Журналом транзакций**. Журнал транзакций содержит дополнительную информацию об изменениях базы данных и предназначен для обеспечения надежного хранения данных в БД.

Целью журнализации изменений баз данных является обеспечение возможности восстановления согласованного состояния БД после любого рода сбоев (аппаратных и программных). Основой поддержания целостного состояния БД является механизм транзакций.

Транзакция – последовательность операций над базой данных, отслеживаемая системой управления БД от начала до завершения как единое целое.

Выделяют следующие **типы транзакций**:

1. плоские или классические (традиционные);
2. цепочечные;
3. вложенные.

Плоские или традиционные транзакции характеризуются следующими свойствами:

- **атомарности** выражается в том, что транзакция должна быть выполнена в целом или не выполнена вовсе;
- **согласованности**, которое гарантирует, что по мере выполнения транзакций данные переходят из одного согласованного состояния в другое – транзакция не разрушает взаимной согласованности данных;
- **изолированности** означает, что конкурирующие за доступ к базе данных транзакции физически обрабатываются последовательно, изолированно друг от друга, но для пользователей это выглядит так, как будто они выполняются параллельно;
- **долговечности** означает, что если транзакция завершена успешно, то те изменения данных, которые были ее произведены, не могут быть ее потеряны ни при каких обстоятельствах.

Общими принципами восстановления являются следующие:

1. результаты зафиксированных транзакций должны быть сохранены в восстановленном состоянии базы данных;
2. результаты незафиксированных транзакций должны отсутствовать в восстановленном состоянии базы данных.

К ситуациям, при которых требуется восстановление базы данных, относятся:

- индивидуальный откат транзакции (аварийное завершение работы и т.д.);
- восстановление после внезапной потери содержимого оперативной памяти (аварийное выключение электропитания, неустранимый сбой процессора и т.д.);
- восстановление после поломки основного внешнего носителя базы данных.

Возможны два основных варианта ведения журнальной информации:

1. отдельный **локальный журнал**, который поддерживается для каждой транзакции и используется для индивидуальных откатов транзакций;
2. **общий журнал** изменений базы данных, используемый для восстановления состояния базы данных после мягких и жестких сбоев.

Структура журнала условно может быть представлена в виде последовательного файла, в котором фиксируется каждое изменение базы данных. Каждая запись в журнале транзакций помечается номером транзакции, к которой она относится, и значениями атрибутов, которые она меняет.

Откат транзакции (возможность для незаконченных транзакций) выполняется следующим образом:

- выбирается очередная запись из списка данной транзакции;
- выполняется противоположная по смыслу операция, восстанавливающая предыдущее состояние объекта базы данных;

- любая из обратных операций также заносится в журнал;
- при успешном завершении отката в журнал заносится запись о конце транзакции.

При восстановлении базы данных после мягкого сбоя в журнале отмечаются точки физической согласованности базы данных – моменты времени, в которые во внешней памяти содержатся согласованные результаты операций, завершившихся до соответствующего момента времени, и отсутствуют результаты операций, которые не завершились.

Основой восстановления базы данных после жесткого сбоя являются журнал и архивная копия БД. Восстановление начинается с обратного копирования БД из архивной копии. Затем для всех закончившихся транзакций по журналу в прямом направлении выполняются все операции, для транзакций, которые не закончились к моменту сбоя, выполняется откат.

В случае логического отказа или сигнала отката одной транзакции журнал изменений сканируется в обратном направлении, и все записи отменяемой транзакции извлекаются из журнала вплоть до отметки начала транзакции. Согласно извлеченной информации выполняются действия, отменяющие действия транзакции. Этот процесс называется откат (rollback).

В случае физического отказа, если ни журнал изменений, ни сама база данных не повреждены, то выполняется процесс прогонки (rollforward). Журнал сканируется в прямом направлении, начиная от предыдущей контрольной точки. Все записи извлекаются из журнала вплоть до конца журнала. Извлеченная из журнала информация вносится в блоки данных внешней памяти, у которых отметка номера изменений меньше, чем записанная в журнале. Если в процессе прогонки снова возникает сбой, то сканирование журнала вновь начнется сначала, но восстановление фактически продолжится с той точки, где оно прервалось.

В случае физического отказа, если журнал изменений доступен, но сама база данных повреждена, то должен быть выполнен процесс восстановления базы из резервной копии. После восстановления база будет находиться в состоянии на момент выполнения резервной копии. Для восстановления базы данных на момент отказа необходимо выполнить прогонку всех изменений, используя журнал изменений.

В случае физического отказа, если журнал изменений недоступен, но сама база данных не повреждена, восстановление возможно только на момент предыдущей контрольной точки.

В случае физического отказа, если повреждены как журнал изменений, так и сама база данных, то восстановление возможно только на момент выполнения резервной копии.

Восстановление поврежденной базы данных

Всегда существует вероятность того, что любое информационное хранилище будет повреждено и часть информации из него потеряна. Базы данных не являются исключением из этого правила. Обычно базу данных называют поврежденной, если при попытке извлечь или модифицировать содержащуюся в ней информацию возникают ошибки и/или извлекаемая информация оказывается утерянной, неполной или вообще неправильной. Порой повреждения базы данных скрыты и обнаруживаются только при проверке специальными средствами, но бывают и явные поломки базы данных, когда к базе невозможно подключиться, отлаженные программы-клиенты выдают нестандартные странные ошибки (в то время как никаких манипуляций над базой данных не производилось) или когда невозможно восстановить базу данных из резервной копии.

Основными причинами повреждения баз данных являются:

1. Аварийное завершение работы серверного компьютера, особенно внезапное отключение электропитания. Поэтому необходимо иметь на сервере источник бесперебойного питания.

При отключении питания на компьютере-сервере все процессы обработки данных резко прерываются. В результате информация в базе данных может исказиться или пропасть. После восстановления питания сервер просматривает данные, отслеживает незавершенные транзакции, не ассоциируемые ни с одним из клиентов, и «откатывает» все изменения, проведенные в рамках этих прерванных транзакций. Однако отключение питания не всегда сопровождается лишь такими незначительными потерями. Если сервер в момент отключения питания производил расширение базы данных, то велик риск получить «потерянные» страницы в файле базы данных (orphan pages), т.е. такие страницы, которые физически распределены и зарегистрированы на страницах учета

страниц, но запись данных на которые невозможна. Борьба с потерянными страницами в файле базы данных умеет только инструмент починки и модификации BackUtil или gfix (стандартная утилита FireBird). Потерянные страницы приводят только к излишнему расходу дискового пространства и как таковые не служат причиной потери или порчи данных. Но отключение питания может привести и к более серьезным повреждениям. После отключения питания и повторного включения может пропасть большое количество данных, в том числе и подтвержденных. Это происходит из-за того, что подтвержденные данные записываются не напрямую в файл базы данных на диске, а используют для этой цели файловый кэш операционной системы. То есть серверный процесс передает операционной системе команду на запись данных на диск, операционная система в свою очередь отправляет подтверждение на сервер, что данные сохранены на диске, а на самом деле данные находятся в файловом кэше. Операционная система не сбрасывает эти данные на диск, так как оценивает, что оперативной памяти еще много, и откладывает медленные операции записи на диск до тех пор, пока не закончится свободная оперативная память.

2. Дефекты и неисправности серверного компьютера, особенно дисков, дисковых контроллеров, оперативной памяти компьютера и кэш-памяти RAID-контроллеров.

3. Файловое копирование или другой файловый доступ к базе данных при запущенном сервере. Выполнение команды shutdown или отключение пользователей обычным порядком не является гарантией того, что сервер ничего не делает с базой; если sweep interval не установлен в 0, может выполняться sweep. Кроме того, после отключения последнего пользователя сервер выполняет уборку лишней информации. Обычно эта процедура занимает 1–2 мин, но, если перед этим выполнялось много операций delete или update, процесс может быть более длительным.

4. Истощение свободного дискового пространства во время работы с базой.

5. Для всех серверов Borland FireBird превышение допустимого количества транзакций без выполнения backup/restore.

Во избежание подобных ситуаций начиная с версии 1.0.12, предусмотрена работа программы «Планировщик резервного копирования данных» с расширенным набором функций архивации данных.

Программа предназначена для выполнения операций резервного копирования, восстановления, починки данных и копирования данных за выбранный период в автономном режиме. После старта она выполняет свои функции согласно заданному расписанию без привлечения к себе внимания со стороны пользователя. Лог работы программы ведется в журнале событий ОС Windows.

В отличие от программ, которые работают как сервисы Windows и могут запускаться до логина пользователя в ОС, «Планировщик резервного копирования данных» останется не запущенным пока пользователь не пройдет регистрацию в ОС. Поэтому для запуска программы необходимо произвести вход в Windows. Так как программа поставляется в дистрибутиве серверной части системы, то такой пользователем должен обладать правами администратора ОС.

Важно отметить, что:

1. Планировщик резервного копирования можно закрыть только через меню пиктограммы из системного трее

2. Если он выполняет какие-либо действия, то закрыть программу нельзя пока процесс не завершится.

3. Если в процессе выполнения архивирования, профилактики попытаться выключить компьютер, то программа не даст этого сделать.

Лог работы программы ведется в журнале событий ОС Windows.

Перед выполнением операций резервного копирования (BackUp) и восстановления базы данных (Restore), происходит анализ свободного места на диске. При этом:

1. Свободного места на диске, где находится БД АИСТ-М должно быть достаточно для хранения самой БД и ее копии, которая создается при восстановлении БД (Restore). Если БД состоит из нескольких файлов, то при оценке места на диске учитывается их общий размер.

2. Свободного места на диске, где находятся файлы архивной копии БД должно быть не меньше общего размера самой БД.

При отсутствии свободного места выполнении функций будет остановлено.

Программа реализует следующие функции:

Регулярное резервное копирование данных – позволяет создать архивную копию всей базы данных (Backup). При этом могут создаваться многофайловые архивы, что определяется настройкой программы.

Профилактика базы данных (Backup/Restore) – включает в себя выполнение сразу двух операций: резервного копирования данных (Backup) и восстановления данных (Restore). Профилактика выполняется как для получения резервной копии базы данных, так и для очистки базы данных от временных записей, что позволяет уменьшить размер БД. На этапе восстановления могут создаваться многофайловые БД, что определяется настройкой программы. При восстановлении все БД отключаются немедленно, а также происходит перезапуск сервера БД. Восстановление по этой причине возможно только на сервере БД. Следует отметить, что функция профилактики БД имеет приоритет выполнения перед функцией регулярного резервного копирования данных. В случае, когда в расписании для этих функций указаны одинаковые параметры запуска (например, совпадает день и время запуска), то будет выполнена только профилактика БД. Это обусловлено тем, что профилактика уже включает в себя операцию резервного копирования данных (Backup).

Перед выполнением восстановления БД (Restore) создается копия текущей БД, с расширением docpoint2.__b . Копия БД необходима для быстрого отката, при возникновении нештатных ситуаций. Для восстановления работоспособности системы достаточно переименовать файл(ы) копии БД. Например, копия БД docpoint2.__b переименовывается в docpoint2.gdb. При каждом запуске «Планировщика резервного копирования» проверяется, есть ли файл БД docpoint2.gdb. В случае если файл не найден (такое может произойти например в случае если во время выполнения профилактики БД произошло отключение сервера), то выдается текстовое сообщение о том что файл БД отсутствует и администратору системы предлагается восстановить базу из копии (автоматически переименовать docpoint2.__b в docpoint2.gdb)

Починка БД – при выполнении починки БД происходит также и проверка целостности БД. При починке БД происходит отключение всех подключенных на момент проверки пользователей и включение БД при завершении операции. При этом починка БД происходит в два этапа, сначала БД проверяется на наличие ошибок, после чего выдается запрос о том, были ли обнаружены ошибки в БД, и нужно ли выполнять исправление БД (дело в том, что в некоторых случаях рекомендуется сделать резервную копию файла, поскольку процесс восстановления будет вносить в БД изменения). В случае же если ошибки не найдены, то проверку нужно прекращать. Сама проверка должна производиться только в случае повреждения БД. Следует четко различать ошибки повреждения БД и, например, ошибки подключения к БД по причине отсутствия соединения. Обычно ошибки в БД могут возникать по причине нестандартного отключения электропитания.

Восстановление БД – восстановление БД из резервной копии происходит автоматически при выполнении функции «Профилактика БД», однако, эта операция может быть сделана по запросу пользователя. Для этого необходимо в меню «Операции» выбрать пункт меню «Восстановить БД». Резервная копия БД находится в каталоге определенном в настройках программы.

Удаление документов по указанную дату – используется для удаления «устаревших» документов и уменьшения размера БД. Пользователь может выбрать дату и время, на которую требуется удалить документы. Удаление документов происходит от самой ранней даты изменения документа найденной в БД, до даты выбранной пользователем. По умолчанию дата устанавливается из расчета, текущая дата минус один год. Периодически необходимо выполнять ревизию документов, для того чтобы те документы которые необходимо отставить, имели относительно свежую дату их изменения. Для этого, например, можно иметь некий переход в технологической схеме, прохождение через который менял бы дату изменения документа. Информация о количестве удаленных документов сохраняется в лог файле BackUtil.log.

Очистка BODY_LOG – удаление в каталоге BODY_LOG временных файлов не связанных ни с одним документом БД.

При откате (RollBack) транзакции, например, когда пользователь отказывается от сохранения изменений в документе, работая в ПЗ «Модуль обработки документов», в каталоге

каталога BODY_LOG формируются временные файлы. Удаление таких файлов, не связанных ни с одним из документов, выполняется автоматически при выполнении функций регулярного резервного копирования и профилактики БД. Однако очистка каталога может быть выполнена по запросу пользователя. Для этого следует выбрать в меню «Операции» пункт «Очистить BODY_LOG». Эта операция, а также период, за который будет произведена очистка, возможны при соответствующей настройке программы.

Физическое копирование БД - при выполнении этой операции происходит только копирование БД, без проведения процедуры backup/restore. Копирование производится в каталог для резервных копий БД.

Возврат состояния до последней операции – при выполнении этой операции происходит переименовывание копии базы оставшейся после последнего выполнения операции «Профилактика БД». Важно запомнить, что при выполнении этой операции текущий вариант базы будет перезаписан более старой ее копией, без возможности возврата к нему.

Если на сервере установлено несколько БД АИСТ-М, то перед выполнением операции будет выдано окно со списком всех баз зарегистрированных в системе. И только после выбора конкретной базы будет выполнена выбранная операция

Как происходит восстановление уже поврежденной БД в случае внезапного отключения электропитания? Для понимания этого сравним БД с файловой системой FAT. Для того чтобы восстановить конкретный файл в файловой системе, выполняются 2 действия:

1. Проверка файловой системы на целостность (логическую), например утилитой scandisk.
2. Проверка остался ли этот файл без изменений (например, специальной программой, работающей с файлом).

Аналогичные действия необходимо произвести над неисправной БД.

1. Проверить целостность БД. База данных, как и файловая система, построена на страницах, которые выделяются в одном пространстве по мере необходимости.
2. Выполнить одну за другой функции «Выполнить резервное копирование» (Backup) и «Выполнить восстановление БД» (Restore).

Эти операции позволят выяснить, удачно ли прошло логическое восстановление БД. Если в ходе этих операций не возникло никаких ошибок, то база данных логически цела, и может использоваться для работы. Исключением может быть «потеря» нескольких документов, по причине того, что они в момент выключения находились в памяти операционной системы и не были сохранены (или были сохранены частично) на диске. Если базу восстановить не удастся, то при наличии резервной копии (если она создается регулярно) есть возможность просто восстановить данные на момент последнего резервного копирования, при этом вся работа, происшедшая после создания резервной копии будет утеряна, но будут восстановлены в полном объеме данных за весь период до резервного копирования.

Для восстановления БД в случае ее поломки (повреждения), не связанной с отключением электропитания, существует другой алгоритм.

Важно запомнить, что ввиду особой сложности этой процедуры, ее может выполнять только вручную администратор системы. При этом восстановление выполняется только для одной конкретной БД. Восстановление требует остановки работы подразделения, т.к. во время операции производится остановка сервиса СУБД.

1. Перед выполнением операции будет выполнен запуск скрипта, если он прописан (по умолчанию отсутствует).
2. Если в системе зарегистрировано более одной БД, то пользователю выдается список зарегистрированных БД, из которого он должен выбрать, какую из БД он будет восстанавливать.
3. Выбор пользователем файла - архивной копии. По умолчанию путь к хранению архивной копии будет указан тот, куда производится автоматическое архивирование БД.
4. Запрос на сохранение копии текущей БД, перед восстановлением путем копирования файла. Копирование может и не производиться. При выборе варианта с сохранением будет запрошен путь, куда сохранять копию БД.
5. Проверяется состояние службы «AutoServiceDocPoint», если она запущена, то выполняется ее остановка. Если сервис был запущен, то состояние сохраняется, для последующего запуска службы, после выполнения операции.

6. Проверяется состояние службы «ControlServerService», если она запущена, то выполняется ее остановка. Если сервис был запущен, то состояние сохраняется, для последующего запуска службы, после выполнения операции.

7. Останавливается сервис управления СУБД (FireBird).

8. Выполняется изменение расширения для файлов БД с `gdb` на `_b`. С целью иметь копию БД в ее первоначальном виде (в случае неудачного восстановления БД), а также с целью недоступности БД по «привычному» пути. Т.е. при попытке после старта сервиса СУБД выполнить подключение к БД, пользователь получит сообщение о том, что БД не найдена. Если в процессе переименования возникли ошибки, то сервис управления СУБД (FireBird) будет запущен.

9. Выполняется старт службы СУБД (FireBird) и выполняется пауза, указанная в параметре «Задержка (в миллисекундах) между остановкой/запуском сервисов». По умолчанию, после установки системы пауза равна 2000 (2 секунды). Пауза предназначена для времени инициализации запущенного сервиса.

10. Выполняется восстановление БД. Восстановление производится не в файл с расширением `gdb`, а в файл с расширением `_db`. С той целью, чтобы пользователи не могли подключаться к БД во время восстановления. Размер страницы БД берется из параметра «Размер страницы БД при восстановлении» настроек, по умолчанию этот параметр равен 4096.

10.1. При необходимости (в зависимости от выбора пользователя), производится копирование БД. Файл копируется из `_b` по указанному пути в `gdb`.

10.2. Перед восстановлением выполняется контроль свободного места на диске. Проверка производится следующим образом если свободного места на диске плюс место, занимаемое ранее переименованным файлом БД (с расширением `_b`) больше, чем архивная копия этой БД +10%, то места достаточно для выполнения операции. Информация о расчете свободного места при любом исходе заносится в протокол. В случае нехватки места на диске операция завершается аварийно (запись об этом событии попадает в протокол) и происходит обратное п.5 переименование файла БД с расширением `gdb`.

10.3. Выполняется восстановление БД в файл с расширением `_db` через Firebird API, вся информация о ходе выполнения восстановления попадает в файл протокола. Для совместимости поддерживается восстановление многофайловых архивов. Архивы БД, берутся по месту, указанному в настройках хранения архивных копий, для дополнительно зарегистрированных БД из подкаталогов DB1, DB2 и т.д.

10.4. Восстановление, в отличие от предыдущих версий данного программного продукта, производится в один файл (многофайловость не поддерживается), а поэтому производится дополнительный контроль присутствия вторичных файлов БД (с расширениями `gd1m` `gd2` и т.д. и `_1`, `_2` и т.д.), если такие файлы найдены, то они являются мусором и удаляются, о чем информация заносится в протокол.

10.5. Если восстановление завершено успешно, то файл, куда производилось восстановление БД (`_db`) изменяет свое расширение на `gdb`. Иначе происходит переименование обратное п.5. из файла с расширением `_b` в файл с расширением `gdb` (откат к предыдущей версии).

11. Если до операции сервис AutoServiceDocPoint не был запущен, то производится его запуск.

12. Если до операции сервис «ControlServerService» не был запущен, то производится его запуск.

13. После выполнения операции будет выполнен запуск соответствующего скрипта «ПОСЛЕ восстановления БД», если он прописан (по умолчанию отсутствует).

Важным элементом сохранения информации являются профилактические действия, которые следует производить для предотвращения поломок баз данных, – это постоянное создание резервных копий. Это самый надежный способ от повреждений базы данных. Только резервное копирование дает полную гарантию сохранности данных. Но в результате резервного копирования может получиться и невозможная копия, поэтому восстановление базы из копии никогда не должно выполняться путем записи поверх оригинала и резервное копирование должно следовать определенным правилам. Во-первых, резервное копирование должно быть как можно более

частым, во-вторых, оно должно быть последовательным, и, в-третьих, резервные копии нужно проверять на возможность восстановления.

Частое резервное копирование означает, что нужно достаточно часто делать резервную копию, например один раз в сутки. Чем меньше промежуток данных между резервным копированием базы данных, тем меньше данных потеряется в результате сбоя.

Последовательность резервного копирования означает, что резервные копии должны накапливаться и храниться как минимум неделю. Если есть возможность, то нужно записывать резервные копии на специальные устройства типа стримера, если нет – то скопировать их на другой компьютер. История резервных копий позволит отследить скрытые повреждения и справиться с ошибкой системы.

Необходимо проверять, можно ли восстановить без ошибок полученную резервную копию. Проверить это можно только одним способом – через тестовый процесс восстановления (restore). Надо отметить, что процесс восстановления занимает примерно в 3 раза больше времени, чем резервное копирование, и для больших баз проверку на восстановление ежедневно делать затруднительно, так как это может прервать работу пользователей на несколько часов.

В том случае, если сервер должен функционировать при значительной нагрузке можно воспользоваться механизмом SHADOW для снятия «моментальных» снимков с базы данных и дальнейших операций по резервному копированию уже с моментальной копией.

При создании резервной копии и затем при восстановлении базы данных из этой копии происходит пересоздание всех данных в базе данных. Этот процесс (backup/restore) способствует исправлению большинства нефатальных ошибок в базе данных, связанных с повреждениями жесткого диска, выявляет проблемы с целостностью данных в базе, очищает базу данных от старых версий и фрагментов записей, незавершенных транзакций, значительно уменьшает размер базы данных. Если база данных рабочая, то рекомендуется производить эту процедуру еженедельно.

Если по каким-то причинам невозможно часто производить процесс backup/restore (особенно restore), то можно воспользоваться инструментом для проверки и восстановления баз данных gfix, который позволяет провести проверку и восстановление многих ошибок без использования процедуры backup/restore.