

Ю. И. Мамаева, А. В. Мошковский

Институт бизнеса БГУ, Минск, Беларусь

Научный руководитель – А. О. Ярошевич, старший преподаватель

ПРОЕКТИРОВАНИЕ СИСТЕМЫ РЕЗЕРВНОГО КОПИРОВАНИЯ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

Работа посвящена разработке системы резервного копирования для защиты данных предприятия и обеспечения их доступности при сбоях. Рассмотрены виды резервного копирования, ключевые требования. Описаны основные компоненты системы, включая задачи резервирования, наборы данных, хранилища, политики и журнал операций. Система позволяет гибко настраивать хранение и управлять доступом, что снижает риск потери данных и ускоряет их восстановление, уменьшая затраты при инцидентах.

Ключевые слова: проектирование системы, резервное копирование, предприятие, системы резервного копирования

В условиях современной цифровой экономики данные являются одним из важнейших активов любого предприятия. Их утрата может привести к серьезным финансовым убыткам, потере клиентов и репутационному ущербу. Примеры таких ситуаций включают в себя не только случайное удаление или повреждение данных, но и кибератаки, природные катастрофы, аппаратные сбои. Статистика указывает на то, что организации, потерявшие данные, нередко сталкиваются с необходимостью сокращения штата, убытками и в некоторых случаях даже прекращением деятельности.

Следовательно, создание системы резервного копирования является не просто технологическим проектом, но критическим элементом стратегической устойчивости предприятия.

Цель данной работы – рассмотреть основные аспекты проектирования системы резервного копирования, способной защитить данные предприятия от потерь и обеспечить их доступность в случае чрезвычайных ситуаций.

Ключевые требования к системе резервного копирования включают в себя:

- надежность: система должна гарантировать высокую вероятность восстановления данных после сбоя;
- регулярность копирования: важно определить периодичность создания копий для минимизации потерь данных. Для оперативных данных копирование может выполняться ежедневно или даже ежедневно;
- безопасность: защита резервных копий от несанкционированного доступа, включая шифрование и аутентификацию пользователей, особенно важна при использовании облачных решений;
- быстрота восстановления: время, необходимое для восстановления данных, влияет на простои в работе компании и затраты, связанные с перерывами в обслуживании клиентов.

Для системы резервного копирования информации на предприятии можно выделить основные классы, описывающие процессы создания, хранения, управления и восстановления резервных копий. Вот несколько ключевых классов:

1. *BackupJob* (задача резервного копирования):

- Job_ID (int): уникальный идентификатор задачи;
- Source (string): путь к исходным данным;

- Destination (string): путь для хранения резервной копии;
- Schedule (datetime): расписание выполнения задачи;
- Status (enum): текущий статус задачи (запланировано, выполняется, выполнено, отменено);

- Frequency (string): частота выполнения (ежедневно, еженедельно и т. д.).

2. *DataSet (набор данных):*

- DataSet_ID (int): уникальный идентификатор набора данных;
- Name (string): название набора данных;
- Size (double): размер данных;
- Created_At (datetime): дата создания.

3. *BackupStorage (хранилище резервных копий):*

- Storage_ID (int): идентификатор хранилища;
- Location (string): местоположение (локально, облако и т. д.);
- MaxCapacity (double): максимальная вместимость хранилища;
- UsedCapacity (double): занятое место.

4. *BackupPolicy (политика резервного копирования):*

- Policy_ID (int): идентификатор политики;
- RetentionPeriod (int): период хранения данных;
- CompressionEnabled (boolean): включение сжатия;
- EncryptionEnabled (boolean): включение шифрования;
- Frequency (string): частота резервного копирования.

5. *RestoreJob (задача восстановления):*

- RestoreJob_ID (int): идентификатор задачи восстановления;
- BackupJob_ID (int): ссылка на задачу резервного копирования;
- Status (enum): статус выполнения задачи (выполняется, завершено, отменено);
- RestoreLocation (string): место восстановления данных.

6. *User (пользователь):*

- User_ID (int): идентификатор пользователя;
- Name (string): имя пользователя;
- Role (enum): роль пользователя (администратор, оператор);
- Permissions (list): список прав доступа.

7. *BackupLog (журнал резервного копирования):*

- Log_ID (int): идентификатор журнала;
- Job_ID (int): ссылка на задачу резервного копирования;
- DateTime (datetime): дата и время записи;
- Event (string): событие (создание, успешное завершение, ошибка).

Разработали диаграмму концептуальных классов в программном продукте Enterprise Architect (см. рисунок).

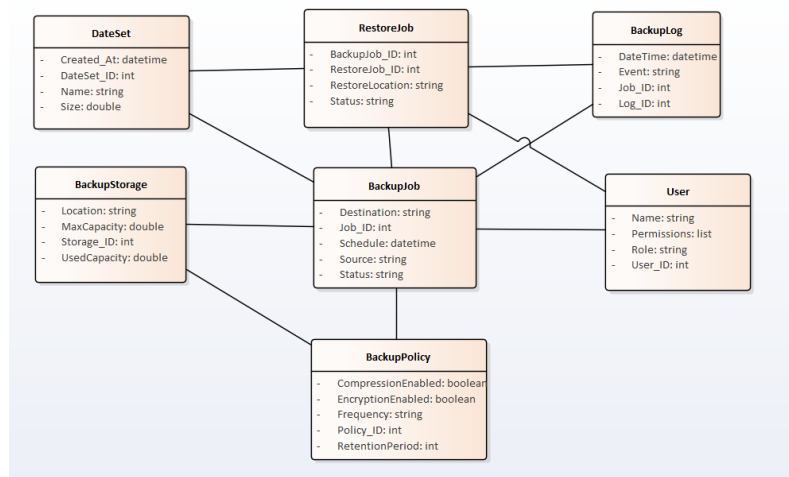


Диаграмма концептуальных классов

Пример работы системы.

Пользователь создает BackupJob, выбирая DataSet и задавая BackupPolicy для указания частоты копирования, а также выбирая BackupStage для сохранения данных. Система выполняет BackupJob, сохраняет данные в выбранном BackupStorage и записывает события в BackupLog. При необходимости пользователь может инициировать RestoreJob, указывая, какие DataSet восстановить из предыдущего BackupJob.

Система резервного копирования должна включать в себя расписание для автоматизации бэкапов, настройку политики хранения, контроль свободного пространства и функции восстановления с разными уровнями прав доступа.

Система резервного копирования информации.

Эта система предназначена для защиты данных предприятия, обеспечивая их регулярное резервное копирование и возможность восстановления в случае потери. Основные компоненты системы:

1. BackupJob (задача резервного копирования). Это основная единица работы системы – задание на резервное копирование. Задача содержит информацию о том, откуда копировать данные (источник), куда их сохранять (место назначения) и когда это делать (расписание). Каждой задаче также присваивается политика резервного копирования, которая определяет частоту копирования и уровень безопасности.

2. RestoreJob (задача восстановления). В случае потери данных можно создать задачу на восстановление. Она связана с конкретной задачей резервного копирования и указывает, какие данные и куда следует восстановить.

3. DataSet (набор данных). Это данные, которые включены в задачу резервного копирования. Каждый набор данных может быть связан с несколькими задачами и хранит информацию о дате создания и объеме.

4. BackupStorage (хранилище). Это место, где хранятся резервные копии. У хранилища есть максимальная емкость, и оно показывает, сколько места уже занято. Система позволяет задействовать разные хранилища для хранения данных.

5. BackupPolicy (политика резервного копирования). Политика определяет следующие параметры резервного копирования:

- частота: как часто происходит копирование;

- сжатие и шифрование: настройки для уменьшения объема данных и повышения безопасности;
 - период хранения: как долго данные хранятся до их автоматического удаления.
6. BackupLog (журнал). В журнале записываются все события, связанные с задачами резервного копирования и восстановления: успешные операции, ошибки и другие важные действия. Это помогает отслеживать, что происходит в системе.
7. User (пользователь). Пользователи – это сотрудники, у которых есть доступ к системе. Каждый пользователь имеет свои права и может управлять задачами резервного копирования и восстановления.

Как работает система

1. Создание задачи резервного копирования. Пользователь настраивает задачу резервного копирования, указывая источник данных, место назначения и расписание. Также выбирается политика резервного копирования, которая определяет параметры копирования.
2. Выполнение копирования. В назначенное время система создает резервную копию данных и сохраняет ее в указанном хранилище. Запись о выполненной операции добавляется в журнал.
3. Восстановление данных. Если необходимо восстановить данные, пользователь создает задачу восстановления. Система находит нужную резервную копию и восстанавливает данные в указанный пользовательский ресурс.

Эта система позволяет предприятию защищать свои данные, сохраняя их на случай непредвиденных ситуаций. Благодаря журналу и политикам резервного копирования можно контролировать процесс и обеспечивать безопасность данных на высоком уровне.

Выводы и преимущества системы резервного копирования

Система резервного копирования предоставляет предприятию надежные механизмы защиты данных и быстрого их восстановления при любых непредвиденных обстоятельствах.

Основные преимущества данной системы:

- защита данных от потерь. Система обеспечивает регулярное копирование информации, что позволяет избежать потерь данных из-за сбоев оборудования, ошибок пользователей, вирусных атак или других угроз;
- быстрое восстановление данных. В случае утраты данных задача восстановления позволяет оперативно вернуть их из резервной копии, минимизируя простои и убытки для бизнеса;
- гибкость в настройке хранения. Система поддерживает использование различных хранилищ с разной емкостью, что позволяет оптимально распределять данные и использовать ресурсы в зависимости от потребностей компании;
- политики резервного копирования. Гибкие политики позволяют настраивать частоту копирования, сжатие, шифрование и срок хранения данных. Это дает возможность контролировать безопасность и экономить ресурсы, например, снижая объем данных через сжатие;
- журнал событий для контроля и аудита. Журнал ведет записи обо всех операциях резервного копирования и восстановления, включая успешные и неуспешные задачи. Это помогает анализировать и улучшать процесс, а также позволяет отслеживать любые аномалии или ошибки.

Использование такой системы делает управление данными более надежным и эффек-

тивным, обеспечивая предприятию уверенность в том, что критически важная информация надежно защищена. Это улучшает непрерывность бизнес-процессов, снижает риски и повышает общую устойчивость предприятия к различным угрозам.

Таким образом, резервное копирование является одним из ключевых элементов информационной безопасности на предприятии. Наличие эффективной системы резервного копирования позволяет снизить риски потерь данных и обеспечить надежное восстановление информации. Для оптимальной работы системы важно правильно выбрать метод резервирования, периодичность копирования и обеспечить защиту резервных копий. В условиях возрастающих угроз информационной безопасности эффективное проектирование системы резервного копирования становится важнейшим фактором устойчивости и конкурентоспособности организации.

Список использованных источников

Бурков, А. В. Проектирование информационных систем в Microsoft SQL Server 2008 и Visual Studio 2008 : краткий курс / А. В. Бурков. – М. : ИНТУИТ, 2016. – 226 с.

Грекул, В. И. Проектирование информационных систем : краткий курс / В. И. Грекул. – М. : ИНТУИТ, 2016. – 400 с.

Захаров, Н. А. Проектирование систем автоматизации : курс лекций / Н. А. Захаров, М. З. Салихов ; под. ред. М. З. Салихова. – М. : Изд. дом МИСиС, 2011. – 96 с.

Кумейко, С. В. Применение копирования в учете / С. В. Кумейко, В. А. Тихомиров, А. И. Краинский. – Ленинград : Союзмашучет, 1938. – 128 с.

Мирхасанов, Р. Ф. Пропедевтика: схематический графический анализ и вольное копирование : учеб. пособие / Р. Ф. Мирхасанов. – М. : Директ-Медиа, 2022. – 184 с.