Глава 23. Служба электронной почты

Электронная почта является важнейшей службой для бизнеса любой компании. Она должна быть надежной, так как сбои в ее работе неприемлемы. Часто она является единственным инструментом общения для генерального директора, и его мнение о надежности электронной почты может существенно повлиять на репутацию и бюджет системных администраторов. Около 45% информации, важной для бизнеса, хранится в сообщениях электронной почты. Это также важнейший способ связи с клиентами и партнерами. Поэтому, при проектировании системы электронной почты, нужно уделять особое внимание ее надежности и расширяемости.

Для создания успешной системы электронной почты нужно предусмотреть основу для построения надежной службы, включая простую, понятную и хорошо документированную архитектуру. Важно использовать открытые протоколы и стандарты, чтобы обеспечить совместимость с другими системами. Также необходима интеграция с системой управления пространством имен для организации корпоративных почтовых адресов.

В процессе проектирования нужно учитывать безопасность, так как система электронной почты может стать целью злоумышленников. Важно также обеспечить конфиденциальность данных и соответствие нормативным требованиям.

Компания должна разработать и внедрить политику неприкосновенности электронной почты, которая должна быть доведена до каждого сотрудника. Эта политика определяет, кто и при каких условиях может читать электронную почту. Также необходимо предусмотреть, что электронные письма могут просматриваться администраторами при необходимости диагностики. Электронная почта, проходящая через другие сети, не должна считаться частной, а конфиденциальная информация не должна передаваться через незащищенные сети. В некоторых компаниях автоматизируется процесс проверки почты на наличие ключевых слов и конфиденциальной информации.

**23.1. Основы**  
Для создания надежной и масштабируемой службы электронной почты необходимо начинать с прочной основы. Системный администратор должен прежде всего обеспечить стабильную основу, прежде чем добавлять новые функции или увеличивать объемы трафика. Архитектура системы должна быть простой, понятной и хорошо документированной. Важным аспектом является использование открытых протоколов и стандартов, что позволит системе взаимодействовать с другими приложениями и системами. Одним из ключевых элементов является система управления пространством имен для организации корпоративных почтовых адресов. Также при проектировании электронной почты нужно учитывать безопасность, так как она может стать целью для злоумышленников. Вопросы неприкосновенности и хранения электронной почты также должны быть согласованы с корпоративной политикой и нормативными требованиями.

**23.1.1. Политика неприкосновенности**  
В каждой компании должна быть четко установленная политика неприкосновенности электронной почты, которая разъясняет, кто и при каких условиях может просматривать электронную почту. Политика должна указывать, что почта, проходящая через другие сети, не является частной, и конфиденциальную информацию нельзя передавать через незашифрованные каналы. В некоторых компаниях электронная почта автоматически проверяется на наличие определенных ключевых слов, а также проверяются вложения на содержание конфиденциальной информации. Важно, чтобы каждый пользователь был ознакомлен с политикой и подтвердил это.

**23.1.2. Пространства имен**  
Пространства имен для адресов электронной почты играют важную роль как для внешних пользователей (клиентов и деловых партнеров), так и для внутренних сотрудников. Использование одного адреса для внешней и внутренней почты помогает избежать путаницы. Например, стандартный формат имени и фамилии (John.Smith@foo.com) часто используется, однако в некоторых случаях это может привести к конфликтам, если в компании есть несколько сотрудников с одинаковыми именами. В таких ситуациях может использоваться автоматический ответ для помощи отправителю в определении правильного адресата.

**23.1.3. Надежность**  
Электронная почта является жизненно важной службой, от которой люди ожидают бесперебойной работы, так же как и от других базовых систем, например, телефонной связи или освещения. Люди не осознают, как сильно они зависят от электронной почты, пока не происходит сбой. Когда система электронной почты выходит из строя, это приводит к множеству звонков в службу поддержки, особенно в критические моменты, когда кому-то необходимо срочно отправить важные документы. Сбой электронной почты имеет эмоциональные последствия для как пользователей, так и системных администраторов. Это не та служба, в которой можно экспериментировать; любые изменения в системе должны проводиться только после тщательного тестирования. Самое важное, что отказ электронной почты влечет за собой серьезные финансовые издержки: потеря электронной почты может вызвать панику в бизнесе, нарушение контрактных обязательств, потерю клиентов и времени, поскольку пользователи переходят на менее эффективные способы связи.

**23.1.4. Простота**  
Система электронной почты должна быть как можно более простой. Сложные системы снижают надежность и усложняют поддержку. Для повышения надежности важно ограничить количество машин, которые обеспечивают службу электронной почты, и не включать рабочие станции в процесс доставки почты. Рабочие станции под UNIX можно настроить как серверы почты, но этого не следует делать, поскольку у них часто отсутствуют необходимые функции для обеспечения надежности, такие как резервное копирование и бесперебойное питание.

Система электронной почты состоит из пяти основных аспектов: транспортировка почты (MTA), доставка почты (MDA), доступ к почте (POP3, IMAP4), обработка списков и фильтрация (спам и вирусы). Для небольших компаний все эти функции обычно могут быть размещены на одной машине. В более крупных компаниях их распределяют по разным системам. Простота архитектуры заключается в том, чтобы не усложнять настройку и обеспечить централизованную систему для отправки почты, избегая отправки почты с рабочих станций напрямую.

В крупных компаниях важно использовать однотипные системы и настроить почтовых клиентов для работы через централизованную систему передачи почты. Протокол SMTP должен быть отключен на машинах, не входящих в систему. Такая конфигурация позволяет системным администраторам точно отслеживать, куда отправляется вся почта для каждой учетной записи. Важно избегать ситуаций, когда почта отправляется в несколько мест, что может привести к ее потере, так как получатель может не знать о ее поступлении.

**23.1.5. Блокировка спама и вирусов**  
Спам (нежелательная коммерческая почта) и вредоносные программы, такие как вирусы, являются серьезной проблемой для системы электронной почты. Более 50% всей почты, приходящей на серверы, может быть спамом. Также с конца 1990-х годов электронная почта стала основным способом распространения вирусов и других вредоносных программ. Блокировка спама и вирусов может быть выполнена как на клиенте, так и на сервере. Однако предпочтительнее блокировать их на сервере, так как это упрощает обновления и гарантирует защиту без необходимости настройки множества почтовых клиентов. Некоторые пользователи могут отключать защитные программы на своих клиентах, что снижает эффективность защиты.

Программы для борьбы с спамом и вирусами не являются идеальными. Они могут обнаруживать известные угрозы, но для новых угроз этот метод не всегда работает. Это создает постоянную гонку между спамерами и разработчиками программ защиты. Существует возможность централизованной обработки спама на сервере через специальные службы, что также может обеспечивать защиту. Однако передача почты через такие службы может привести к проблемам с неприкосновенностью данных.

**23.1.6. Универсальность**  
Система электронной почты должна быть построена на основе открытых протоколов для обеспечения максимальной совместимости с другими системами. Для транспортировки почты используется протокол SMTP, который широко распространен в Интернете. Все системы должны поддерживать SMTP в качестве основного транспортного протокола. В будущем, скорее всего, будут использоваться расширения SMTP, такие как ESMTP, а не полностью новые и несовместимые протоколы.

Универсальность также касается внутренней связи внутри компании и поддержки различных почтовых агентов пользователя. Современные системы могут поддерживать несколько популярных протоколов для работы с почтой, что обеспечивает совместимость с различными клиентами на разных операционных системах. Использование стандартных протоколов позволяет поддерживать широкий выбор почтовых клиентов, что дает пользователям возможность выбрать наиболее удобный для себя инструмент. В отличие от этого, системы, использующие собственные протоколы, ограничивают выбор клиентов и могут не поддерживать необходимые функции.

**23.1.7. Автоматизация**  
Автоматизация в администрировании электронной почты позволяет упростить выполнение рутинных задач, таких как создание и удаление учетных записей, а также управление списками рассылки. Процесс создания учетных записей электронной почты должен быть автоматизирован в рамках процесса создания учетной записи сотрудника, что также включает добавление сотрудников в соответствующие списки рассылки. Удаление учетных записей должно быть автоматизировано на этапе увольнения сотрудников.

Также важным аспектом является автоматизация процесса перемещения учетных записей электронной почты между машинами для перераспределения нагрузки. Однако важно избегать автоматического перенаправления почты для уволенных сотрудников, чтобы избежать утечки конфиденциальной информации. Вместо этого следует отправлять уведомление о перенаправлении с новым адресом и сообщением о том, что человек больше не работает в компании.

Автоматизация администрирования списков рассылки также важна, так как позволяет пользователям самостоятельно создавать, удалять и управлять своими списками рассылки, освобождая системных администраторов от рутинной работы.

**23.1.8. Базовый мониторинг**  
Мониторинг является неотъемлемой частью администрирования системы электронной почты. Для каждого сервера, участвующего в системе, должен осуществляться мониторинг состояния: включение, подключение к сети, ответы на пинги и запросы на соответствующие порты (например, SMTP на порте 25, POP3 на порте 110, IMAP4 на порте 143). Также необходимо отслеживать использование дискового пространства, загрузку процессора и другие ресурсы, так как почтовые серверы требуют значительных вычислительных мощностей.

Мониторинг важен для выявления проблем, таких как переполнение дисков, аномальное использование процессора или петли почты. Также необходимо следить за работой почтового адреса **postmaster**, который отвечает за ошибки доставки сообщений. Этот адрес помогает отслеживать сбои и получать важную информацию для устранения неполадок. Логи на почтовых серверах также являются важным инструментом для анализа интенсивности потока сообщений и предотвращения потенциальных сбоев, когда объем сообщений резко увеличивается.

**23.1.9. Резервирование**  
Электронная почта является критически важной службой для компаний, поэтому необходимо внедрить меры избыточности, чтобы обеспечить высокую доступность и надежность. В случае сбоя системы или оборудования, должен быть разработан план восстановления.

Резервирование узлов передачи почты можно реализовать через DNS-записи MX, указывая несколько серверов с одинаковой конфигурацией для обработки почты. Однако для узлов доставки почты ситуация более сложная, так как их полное резервирование не всегда возможно. В таких случаях важно создать внутреннюю избыточность серверов с использованием технологий, таких как RAID и сетевые хранилища данных.

Для обеспечения избыточности на уровне клиентов, необходимо учитывать работу клиента с DNS-запросами, так как он может кэшировать результаты запросов. Для избыточности на уровне IP используется балансировка нагрузки и протокол виртуального резервирования маршрутизаторов (VRRP), что позволяет минимизировать влияние сбоев в сети.

При проектировании стратегии резервирования важно учитывать все компоненты системы, их взаимодействие и влияние на общую производительность.

**23.1.10. Расширение**  
Система электронной почты должна быть спроектирована с учетом возможного роста. Потребности в расширении возникают в связи с увеличением объема трафика, числа пользователей, а также с развитием новых технологий, влияющих на размер сообщений.

Системы транспортировки электронной почты должны быть готовы к увеличению интенсивности трафика. Это зависит от нескольких факторов: размера сообщений, количества сообщений на одного пользователя и числа пользователей. С ростом числа пользователей и объема сообщений, система должна быть способна обрабатывать пики нагрузки, особенно в периоды праздников или особых мероприятий.

Также необходимо учитывать неожиданные скачки трафика, например, вызванные техническими проблемами или презентациями. Для этого система должна иметь возможность быстро справляться с пиками, а также хранить большие объемы почты, если возникают проблемы с доставкой сообщений.

Системы доставки почты должны масштабироваться, чтобы обслуживать большее количество пользователей, и обеспечивать достаточный запас емкости для хранения сообщений, особенно если пользователи сохраняют почту на сервере на длительный срок. Практическое правило для расчета пиковых нагрузок — увеличение нормальной нагрузки вдвое.

**23.1.11. Вопросы безопасности**  
Системы электронной почты подвержены многочисленным угрозам, как внутренним, так и внешним, поскольку почтовые узлы часто становятся целями атак. Они предоставляют доступ как к внешнему миру, так и к внутренней корпоративной сети, и могут иметь доступ к внутренним службам аутентификации и имен. Чтобы минимизировать риски, вопросы безопасности необходимо учитывать на всех этапах разработки и эксплуатации почтовой системы.

**1. Защита от вирусов и нежелательного контента:**  
Необходимо внедрить механизмы для сканирования содержимого почты на вирусы и другие нежелательные элементы до того, как почта будет доставлена пользователю. Если это решение принято, важно выбрать систему, которая поддерживает максимальное количество форматов данных для проверки всех вложений (например, архивы формата ZIP). Тем не менее, не все угрозы можно предотвратить на уровне сервера, и сканирование также должно быть выполнено на пользовательских устройствах. Однако сканирование большого количества сообщений может создать узкие места в системе, особенно при высоких объемах трафика, что требует использования высокоскоростных дисков.

**2. Защита почтовых серверов:**  
Почтовая система должна быть интегрирована в общую архитектуру безопасности компании. Например, необходимо обеспечить защиту от передачи сообщений с подозрительными заголовками, которые могут пытаться использовать уязвимости системы. Также важно предотвращать неавторизованную отправку почты через внешние почтовые серверы.

**3. Безопасный удаленный доступ:**  
Одной из распространенных угроз является передача паролей и конфиденциальных данных по небезопасным публичным сетям. Поэтому важно внедрить безопасные механизмы удаленного доступа к почте, такие как VPN или шифрование данных, что поможет минимизировать риски при работе пользователей с электронной почтой в удаленном доступе.

**23.1.12. Распространение информации**  
Один из ключевых аспектов создания службы электронной почты — это эффективное распространение информации о ее функциях и правилах использования. Это включает в себя как информирование пользователей, так и документирование системы для системных администраторов.

**1. Информирование пользователей:**  
Пользователи должны быть ознакомлены с политиками безопасности, включая правила работы с конфиденциальной информацией, перенаправлением почты, созданием резервных копий и фильтрацией содержимого. Также важно информировать пользователей о рисках, таких как вирусы, фишинг и другие угрозы, а также о возможных последствиях перенаправления почты на нежелательные адреса.

**2. Документирование для администраторов:**  
Системные администраторы должны иметь доступ к полному набору документации, которая включает схемы архитектуры почтовой системы, процессы восстановления после отказа и процедуры для базовой отладки. Документация должна быть понятной и доступной, особенно для администраторов, работающих в разных часовых поясах и в удаленных подразделениях. Также важно обеспечить, чтобы администраторы могли самостоятельно выполнять основные задачи по отладке системы.

Таким образом, безопасность системы электронной почты требует комплексного подхода, включая как технические меры защиты, так и обучение пользователей и администраторов.

**23.2. Тонкости**  
После обеспечения основ безопасности и функциональности службы электронной почты, компании могут внедрить дополнительные улучшения для повышения удобства использования и защиты конфиденциальной информации. Это включает в себя шифрование сообщений, улучшенную политику хранения данных, а также меры для расширения функциональности почтовой системы в случае необходимости. Рассмотрим каждую из этих аспектов подробнее.

**23.2.1. Шифрование**  
Шифрование является важным шагом для защиты конфиденциальных сообщений, особенно для высшего руководства, которое может работать с чувствительной информацией. Важно, чтобы процесс шифрования был простым и быстрым, чтобы не затруднять повседневное использование почты. Шифрование должно быть интегрировано в почтовый клиент таким образом, чтобы для отправки зашифрованных сообщений достаточно было всего одного клика, а получатель мог легко их расшифровать.

Для успешного внедрения шифрования необходимо:

* Выбор шифрования, которое интегрируется в интерфейс почтового клиента.
* Обеспечение хранения и управления ключами шифрования для всех сотрудников.
* Реализация системы восстановления доступа в случае потери пароля или компрометации ключа.

Однако нужно учитывать, что системы шифрования и управления ключами являются сложными и требуют внимательного подхода к выбору решений, чтобы избежать проблем с неэффективными или ненадежными продуктами. Также стоит помнить о юридических аспектах, таких как закон Сарбейнса-Оксли, который требует, чтобы компания могла предоставить личные ключи для расшифровки сообщений по запросу государственных органов.

**23.2.2. Политика хранения электронной почты**  
Резервное копирование и хранение электронной почты должны быть настроены с учетом юридических требований и возможных судебных процессов. В некоторых случаях компания может столкнуться с необходимостью предоставить электронные письма в качестве доказательств в суде, что делает критически важным эффективное управление архивированием сообщений.

Вопросы, которые нужно учитывать при разработке политики хранения электронной почты:

* Политика удаления резервных копий, которая позволяет удалять старые письма после определенного времени, что помогает избежать излишнего накопления данных.
* Внедрение механизмов поиска актуальных сообщений в архивах, которые могут понадобиться в юридических процессах.
* Если электронная почта хранится на различных устройствах сотрудников, важно управлять резервными копиями на всех этих устройствах, включая ноутбуки и ПК, с учетом разделения системных и почтовых резервных копий.

Политика хранения данных должна быть внедрена как можно раньше, чтобы обеспечить соответствие законодательным требованиям, таким как закон Сарбейнса-Оксли, и упростить процесс поиска документов при необходимости.

Таким образом, в рамках улучшения почтовой системы, компании должны предусмотреть простоту применения шифрования, разработать политику хранения и резервного копирования электронной почты и внимательно следить за юридическими аспектами.

**23.2.3. Расширенный мониторинг**  
Для компаний, которые зависят от электронной почты для своей работы и доходов, необходимо внедрить более продвинутые методы мониторинга почтовых систем. Сквозной мониторинг является важным аспектом, поскольку он позволяет отслеживать не только базовые параметры, такие как время отправки и получения сообщений, но и более сложные процессы, которые могут влиять на доставку и обработку почты.

Сквозной мониторинг включает в себя создание теста, который воспроизводит отправку сообщений максимально реалистично. Это позволяет выявить потенциальные проблемы, которые могут быть скрыты за пределами сети компании или системы почтового сервера. Важно, чтобы мониторинг охватывал все этапы передачи сообщений и был способен обнаружить любые неполадки, включая те, которые могут возникать на внешних сервисах.

**23.2.4. Обработка больших списков**  
Многие компании используют списки рассылки для различных целей, таких как уведомления о новых продуктах, обновлениях, а также для общения с клиентами и пользователями. При этом существует особая необходимость в более сложных системах для обработки больших объемов списков.

Для эффективного управления большими списками рассылки, особенно в крупных компаниях, важно использовать специализированные программы, которые могут справляться с большим количеством адресатов и обеспечивать высокую скорость отправки сообщений. Также необходимо учитывать требования к безопасности и управлению доступом, чтобы только авторизованные лица могли управлять списками рассылки и отправлять сообщения.

Кроме того, для таких систем важно реализовать несколько резервных механизмов, чтобы предотвратить сбои при высокой нагрузке на сервер. Также важно следить за временем доставки сообщений и избегать задержек, которые могут вызвать неудобства для получателей.

Для компаний, которые работают с большими списками рассылки, рекомендуется инвестировать в коммерческие решения или воспользоваться открытым исходным кодом и нанять специалистов, имеющих опыт в проектировании таких систем. Это позволит обеспечить бесперебойную работу и оперативную доставку сообщений.

**Заключение**  
Электронная почта является неотъемлемой частью бизнеса, и ее работа должна быть надежной. Важно заранее продумать политику безопасности, мониторинга и обработки данных, чтобы избежать проблем с эффективностью и юридическими рисками. Особенно это актуально для компаний, в которых электронная почта играет ключевую роль в получении дохода или обслуживании клиентов. В таких случаях следует обратить внимание на дополнительные меры, такие как шифрование, управление списками рассылки и мониторинг всех процессов, связанных с почтовой системой.

**Глава 24. Служба печати**  
Печать — это процесс получения бумажной копии документа, который остается важной функцией в бизнесе. Несмотря на развитие технологий, многие пользователи по-прежнему считают печать одной из наиболее критичных служб в своей работе, иногда даже более важной, чем электронная почта.

Многие системные администраторы могут не понимать, насколько важно обеспечить надежную работу службы печати, поскольку они часто предпочитают обходиться без бумаги и полагаются исключительно на электронные версии документов. Однако реальность такова, что в бизнесе бумага часто необходима для подписания контрактов, вывешивания схем и других целей, для которых цифровая версия не всегда подходит. Даже люди, работающие в технологической сфере, не могут обойтись без бумаги в некоторых ситуациях.

Таким образом, печать — это важная бытовая потребность, которая должна функционировать без сбоев. Системные администраторы должны учитывать, что печатные устройства могут быть подвержены поломкам, и всегда должен быть предусмотрен план на случай, если принтер не работает. Однако несмотря на множество изменений в технологиях печати, ключевые аспекты работы службы печати остаются неизменными.

**24.1. Основы**  
Успешная система печати начинается с четкого понимания требований и разработки политики, которая поддерживает стабильную работу службы печати. Без продуманной политики проектирование системы печати будет хаотичным, а использование системы — неудобным. Важно помнить, что хороший дизайн системы печати делает ее более предсказуемой и менее подверженной ошибкам, а также помогает снизить сложность обслуживания.

При проектировании системы печати важно учитывать такие аспекты, как:

* Надежность работы устройства.
* Легкость и удобство в использовании для пользователей.
* Процесс мониторинга состояния принтеров и картриджей.
* Разработка централизованного сервера печати, который обеспечит удобное управление и контроль за печатными задачами.

Рассмотрение политики печати также должно включать аспекты безопасности, такие как ограничение доступа к чувствительной информации и контроль над тем, кто может печатать те или иные документы.

**24.1.1. Уровень централизации**  
Одним из ключевых решений при проектировании системы печати является выбор уровня централизации. Существует несколько подходов, в зависимости от потребностей пользователей и бюджета.

**1. Личное подключение принтеров к компьютерам:**  
Некоторые пользователи предпочитают, чтобы каждый компьютер был подключен к своему собственному высокоскоростному принтеру с высоким качеством печати. Это удобно, так как пользователи могут всегда иметь доступ к своему принтеру, не зависеть от других и избегать очередей. Однако, такой подход имеет высокую стоимость, как в плане приобретения, так и в обслуживании множества принтеров.

**2. Централизованная печать:**  
Другой подход заключается в централизованной печати, где пользователи могут печатать на любом доступном принтере, а не только на персональном. В этом случае создается централизованная система с набором принтеров в разных частях здания или организации. Это позволяет пользователю "одолжить" принтер с более высоким качеством печати, если это необходимо. Такой подход является более гибким, но также может создавать определенные трудности, например, в очередях за принтерами или в организации доступа к специфическим устройствам.

**3. Компромисс между удобством и расходами:**  
Существует компромисс между количеством принтеров и расходами на их обслуживание. Большее количество принтеров увеличивает удобство, так как у каждого есть возможность легко напечатать необходимые документы. Однако большее количество принтеров приводит к увеличению расходов на оборудование, расходные материалы и обслуживание. С другой стороны, использование меньшего числа принтеров может сэкономить средства, позволяя купить более качественные устройства.

**4. Пример с централизованным принтером:**  
Пример: если 10 человек используют один принтер, стоимость одного принтера для каждого из них составит $1000. При этом можно купить более качественный сетевой принтер за эту сумму, который обслужит большее количество пользователей и будет предоставлять более высокое качество печати. Таким образом, при использовании централизованного принтера можно обеспечить лучший сервис за меньшие деньги.

**5. Проблемы с специализированными устройствами:**  
Некоторые принтеры, такие как фотопринтеры, плоттеры или другие специализированные устройства, могут требовать отдельного контроля доступа. Эти устройства могут иметь более высокие эксплуатационные расходы, и поэтому доступ к ним может быть ограничен, например, только определенными сотрудниками или подразделениями.

В общем, решение о централизации печати зависит от приоритетов организации в области удобства, стоимости и специфики работы.

**24.1.2. Политика архитектуры печати**

Каждая компания должна иметь четко определенную политику, регулирующую архитектуру печати. Основной задачей этой политики является определение структуры системы печати, включая количество принтеров, доступных пользователям, и правила подключения их к сети. Политика архитектуры печати должна включать несколько ключевых аспектов:

**1. Уровень централизованности:**  
Политика должна четко устанавливать, насколько централизованной будет система печати. Это включает в себя решения о том, сколько принтеров будет использовано в организации и как они будут распределены по офису (один принтер на коридор, этаж, здание или даже на каждую машину). Также важно определить, какие принтеры могут использовать все сотрудники, а какие — только определенные пользователи.

**2. Буферизация печати и контроль доступа:**  
Для обеспечения надежности сетевых принтеров потребуется центральная система буферизации печати, которая будет принимать и хранить задания для печати, пока принтер не будет готов их выполнить. Система буферизации может также служить для контроля доступа, определяя, кто имеет право печатать на каждом принтере. Это также позволяет перенаправлять задания на другие принтеры, если один из них выйдет из строя.

**3. Обслуживание и замена принтеров:**  
Политика должна также регулировать обслуживание принтеров. Важным вопросом является, кто будет заниматься обслуживанием — внутренний персонал или подрядчик. Также необходимо определить пороговые значения, при которых замена принтера будет более выгодной, чем его продолжение эксплуатации. В некоторых случаях замена может быть обусловлена высокими издержками на обслуживание или продолжительным временем простоя устройства.

**4. Бухгалтерская политика:**  
Политика должна описывать, как будет решаться вопрос покупки принтеров и их обслуживания. Это включает в себя определение источников финансирования, таких как центральный бюджет или специальные счета для подразделений. Также важно решить, как будет производиться оплата расходных материалов (бумага, тонер). Например, в университетах может быть введена постраничная оплата с различными тарифами для разных типов принтеров.

**5. Заказ расходных материалов:**  
Кто будет заказывать расходные материалы и управлять их пополнением — также важно определить в рамках политики. В некоторых организациях этим занимаются секретари, в других — централизованно через отдельную службу. Кроме того, не рекомендуется позволять обычным пользователям самостоятельно заменять картриджи с тонером, так как это может быть сложным и ошибочным процессом. Более эффективным будет, если эту задачу будут выполнять операторы, обученные для таких процедур.

**6. Стандарты оборудования:**  
Политика должна содержать документированный стандарт оборудования. Это включает долговременные стандарты, такие как использование определенных протоколов для печати (например, PostScript или PCL), поддержка двусторонней печати, выбор подключения к сети (например, TCP/IP или SMB) и типы рекомендуемых принтеров. Вторая часть политики должна регулярно обновляться и содержать список одобренных моделей принтеров, что помогает избежать путаницы и экономить средства, так как стандарты могут позволить получить скидки на покупку.

**7. Контроль и фильтрация заказов:**  
Все заказы на покупку принтеров и расходных материалов должны проходить через группу системных администраторов или других компетентных специалистов. Это поможет избежать ситуаций, когда сотрудники заказывают неподходящее оборудование, что может повлиять на эффективность и совместимость системы печати в организации.

Таким образом, политика архитектуры печати обеспечивает четкость, контроль и оптимизацию расходов на печатную технику и расходные материалы, обеспечивая надежную и эффективную работу системы печати в компании.

**24.1.3. Структура системы**

После того как будут определены правила для архитектуры печати, необходимо спроектировать и реализовать саму структуру системы печати. В зависимости от уровня централизации и управления, можно выбрать различные архитектуры. Рассмотрим два основных типа: **пиринговую архитектуру** и **централизованный буфер**.

**Пиринговая архитектура**

Пиринговая архитектура — это децентрализованная модель, при которой все узлы отправляют задания напрямую на принтеры в сети. Это довольно простая в настройке схема, так как для отправки задания на печать достаточно знать IP-адрес или имя принтера. Однако она может быть сложной в администрировании. Например, если принтер заменяется на более новую модель, требуется обновление драйверов на всех клиентских машинах, что может вызвать сложности.

Преимущества:

* Простота в настройке.
* Минимальная нагрузка на серверы.

Недостатки:

* Сложность управления в случае изменений (например, замена принтера).
* Потенциальные проблемы с совместимостью драйверов на клиентских машинах.
* Сложности с мониторингом и отменой заданий печати, поскольку необходимо искать машину, отправившую задание.

**Центральный буфер**

Централизованный буфер — это более централизованная архитектура, где все задания печати проходят через центральный сервер, который управляет принтерами и распределяет задания на них. Такой подход обеспечивает более высокий уровень контроля и позволяет серверу принимать интеллектуальные решения, такие как выбор принтера на основе доступности или качества печати.

Преимущества:

* Легкость в обновлении (обновления драйверов и настроек выполняются только на сервере).
* Возможность централизованного контроля и анализа печати.
* Более высокая гибкость в управлении заданиями (например, конвертация форматов или распределение заданий по различным принтерам).

Недостатки:

* Создание единой точки отказа — если сервер выйдет из строя, вся система печати будет недоступна.
* Требуется высокая производительность и надежность серверов для обеспечения бесперебойной работы.

**Варианты архитектур**

Существует несколько вариантов этих двух архитектур:

* Центральный буфер может быть с избыточностью, например, с резервными серверами, которые могут автоматически или вручную восстанавливаться после отказа.
* Пиринговая архитектура может быть улучшена с помощью автоматизированных механизмов обновления драйверов, таких как скрипты или утилиты для распространения конфигураций (например, NIS или LPRng в UNIX-системах).
* В некоторых компаниях используют архитектуру, где несколько серверов с буферизацией обслуживают группы пользователей, разделенные по зданиям или подразделениям, при этом системы могут заменять друг друга в случае отказа.

**Современные тенденции**

В последнее время пиринговая архитектура стала более популярной, поскольку современные принтеры оснащены надежными встроенными системами буферизации. Это упрощает настройку и управление печатью, поскольку пользователи могут самостоятельно подключать принтеры без помощи системных администраторов. Однако в таких системах могут возникать проблемы с отменой заданий, если не удается точно определить, какая машина отправила задание на печать.

**Важность документации**

Архитектура системы печати должна быть тщательно документирована. Это включает:

1. **Инструкция по печати** — должна объяснять, как подключиться к принтеру, какие команды использовать в операционных системах, и описывать особенности печати (например, односторонняя или двусторонняя печать).
2. **Список принтеров** — каталог всех доступных принтеров, их расположение, особенности (цвет, качество и т. д.). Этот список должен быть актуален и доступен пользователям.
3. **Метка принтера** — каждый принтер должен быть помечен своим именем или именами (например, если используется несколько моделей), а также метками на лотках для бумаги, если они предназначены для специфических материалов (пленки, бланки и т. д.).

Документация играет ключевую роль в эффективной работе системы печати, помогая пользователям ориентироваться в доступных устройствах и правилах работы с ними.

**24.1.5. Мониторинг**

Мониторинг системы печати охватывает два важных аспекта:

**1. Мониторинг буферизации и печати**

Системные администраторы должны следить за состоянием системы буферизации, чтобы гарантировать её корректную работу:

* **Очереди заданий** не должны зависать.
* **Диск буферизации** должен быть достаточно вместительным и не заполнен.
* **Логи** должны обновляться без сбоев.
* **Процессор** и другие ресурсы не должны перегружаться.
* **Диск буферизации** должен оставаться исправным.

Эти процессы должны быть частью общего мониторинга системы. Регулярное отслеживание таких параметров помогает предотвратить сбои в печати и улучшить производительность.

**2. Мониторинг состояния принтеров**

Важно следить за состоянием принтеров, таких как:

* Уровень **чернил** и **бумаги**.
* Засорение **лотков** или **бумаги**.
* Проблемы с механикой, такие как **застревание бумаги**.

Современные сетевые принтеры поддерживают **SNMP** (Simple Network Management Protocol), который позволяет системе мониторинга предупреждать администраторов о проблемах. Например, принтер может уведомить о том, что бумага заканчивается или застряла, что позволяет своевременно принять меры. Однако для некоторых аспектов, таких как наличие бумаги в непосредственной близости от принтера, автоматического мониторинга нет. В таких случаях можно либо установить регулярные проверки, либо полагаться на пользователей, которые будут сообщать о таких проблемах.

**Рекомендации для администраторов:**

* Настроить систему мониторинга для получения уведомлений о низком уровне бумаги или чернил.
* Разработать систему, при которой пользователи могут легко сообщать о нехватке материалов.

**24.1.6. Экологические вопросы**

Системные администраторы несут ответственность за экологическое воздействие системы печати. Важно минимизировать негативное воздействие печати на природу, а также оптимизировать процессы, чтобы сократить отходы.

**Проблемы экологии при печати:**

* **Чернила** могут быть токсичными.
* Печать уничтожает **деревья** для производства бумаги.
* Использование бумаги ведет к накоплению **отходов**, которые наполняют свалки.

**Экологически ответственные практики:**

1. **Переработка картриджей с чернилами** — это важный шаг, который должен быть включен в политику организации. Администраторы должны способствовать созданию системы сбора и переработки использованных картриджей.
2. **Снижение бумажных отходов**:
   * Стимулировать **предварительный просмотр документов** перед печатью (например, поддержка форматов PostScript).
   * Поощрять **двустороннюю печать** (дуплекс).
   * Минимизировать ненужную печать, например, устраняя разделительные страницы и бумажные формы, заменяя их веб-формами или электронными процессами.
3. **Легкость переработки** — важно создать удобную систему для пользователей, чтобы они могли легко сдать бумагу на переработку. Это включает:
   * Размещение **контейнеров для переработки бумаги** рядом с принтерами.
   * Установка **корзин для переработки отходов** в удобных местах.
4. **Совместная работа с другими департаментами** — создание системы переработки должно включать взаимодействие с отделами, ответственными за организацию работы офисных устройств (например, копиров).

**Рекомендации для администраторов:**

* Внедрить стратегию минимизации бумажных отходов, предлагая пользователям инструменты для предварительного просмотра и поддержки дуплексной печати по умолчанию.
* Обеспечить возможность переработки бумаги и картриджей с чернилами, создать удобные схемы для сбора и утилизации отходов.
* Призывать пользователей к более экологичному поведению, предоставляя простые и доступные способы сдать отходы на переработку.
* **24.2. Тонкости**
* Системные администраторы могут внести в свою службу печати интересные дополнения, которые позволят повысить качество обслуживания на уровень компании «Роллс-Ройс».
* **24.2.1. Автоматическое восстановление после отказа и балансировка нагрузки**
* Когда система печати работает с большими объемами, важно настроить автоматическое восстановление после отказа, чтобы минимизировать время простоя и повысить устойчивость системы. Это включает два ключевых элемента: обнаружение проблемы и передачу задач на резервный сервер. Если одна из систем выходит из строя, задачи должны перенаправляться на другую систему для поддержания нормальной работы. Важно также настроить балансировку нагрузки, при которой несколько серверов печати равномерно распределяют задачи, предотвращая перегрузку одного из них. В случае сбоя одного из серверов, другой должен взять на себя задачи, чтобы минимизировать время простоя. Для правильной диагностики проблем с печатью важно проверять, принимает ли сервер новые задания, нет ли застрявших заданий в очереди и не задерживаются ли они слишком долго. Администраторы должны избегать ложных срабатываний, таких как сбои в драйверах или приложениях на рабочих станциях.
* **24.2.2. Выделенный сотрудник для обслуживания**
* Принтеры — это сложные механические устройства, и их обслуживание может быть более эффективным, если этим занимается специально назначенный человек, например, клерк или оператор. Этот сотрудник будет периодически проверять принтеры на наличие бумаги, исправность и выполнять необходимое обслуживание. Он также может организовывать ремонт принтеров, взаимодействовать с поставщиками и техниками. Ответственность за заказ расходных материалов, таких как картриджи, также может быть возложена на этого сотрудника, что значительно уменьшит нагрузку на системных администраторов.
* **24.2.3. Уничтожение бумаги**
* Конфиденциальные документы, напечатанные на бумаге, требуют особого внимания при уничтожении. Компании могут решить уничтожать бумагу собственными силами или воспользоваться услугами сторонних исполнителей. Если уничтожение происходит внутри компании, необходимо выделить ответственного человека для контроля за процессом. Если используются сторонние службы, важно убедиться в их надежности, так как бывают случаи, когда бумаги не уничтожаются должным образом. Регулярные проверки таких поставщиков помогут избежать нежелательных ситуаций. Уничтожение бумаг важно для защиты конфиденциальной информации, и лучше переоценить риск утечки данных, чем недооценить его.
* **24.2.4. Борьба с недопустимым использованием принтеров**
* Старая пословица Usenet гласит: «Нельзя решить социальные проблемы при помощи технологий». Это также справедливо и для печати. Невозможно написать программу, которая бы эффективно обнаруживала использование принтеров не по назначению или выявляла расточительное использование бумаги. Однако правильный контроль и обеспечение соблюдения политик может значительно улучшить ситуацию. В вашей политике допустимого использования (раздел 11.1.2) должно быть чётко указано, какое использование принтера является недопустимым.
* Один из методов, который может помочь контролировать расходы на печать, это введение системы постраничной оплаты. В таком случае можно предоставить каждому сотруднику ограниченное количество "бесплатных" страниц в месяц или позволить подразделениям объединить этот объём. Психологический эффект от такой системы может быть значительным. Люди будут стараться не превышать норму, чтобы избежать дополнительных расходов.
* В некоторых компаниях использовался метод публичного осуждения: каждый месяц объявляли десять сотрудников, которые печатали больше всех. Это должно было мотивировать людей тратить меньше бумаги. Однако, как показала практика, некоторые сотрудники воспринимали это как соревнование и старались попасть в этот список как можно чаще. Этот подход был бы более эффективным, если бы информация о больших потребителях печати была доступна только руководству или если бы системный администратор лично подходил к этим людям и деликатно сообщал о проблемах. Важно помнить, что стыд работает только в определённых ситуациях.
* Лучше всего применить нетехнический, уравновешенный подход: разместите принтер в заметном, часто посещаемом месте. Это уменьшит желание использовать его для личных целей, сильнее любой политики или системы тарификации. Если кто-то будет использовать принтер не по назначению, обратитесь к этому человеку лично. Не стоит заострять внимание на мелких нарушениях, так как это может вызвать раздражение.
* Примером такого подхода является ситуация с 500-страничной распечаткой читов для компьютерных игр. Когда это было обнаружено, директор не стал ругать сотрудников. Вместо этого он отправил всем письмо, сообщив, что найденная распечатка не была подписана и напомнил, что небольшие личные печати допустимы, но такие важные документы не должны теряться. В конце концов, спустя неделю, документ был переработан, так как владелец так и не пришёл за ним. Больше никаких замечаний делать не пришлось.
* **Заключение**
* Печать — это обыденная услуга, и пользователи часто принимают её работу как должное. Чтобы система печати была надежной, необходимо чётко определить политику размещения принтеров, типов используемых устройств, их имен и протоколов связи. Система печати может быть децентрализованной или централизованной, и важно предусмотреть элементы резервирования и восстановления после сбоев. Не менее важен мониторинг системы, чтобы обеспечить её бесперебойную работу.
* Для пользователей нужно предоставить необходимую документацию, объясняющую, как печатать и где находятся доступные принтеры. На самих устройствах должны быть соответствующие метки.
* Экологические аспекты печати также должны быть учтены. Системные администраторы обязаны работать с другими подразделениями для создания программы переработки бумаги и предоставлять пользователям средства, помогающие минимизировать потребность в печати.

В идеальных системах печати предусмотрены механизмы автоматического восстановления после сбоев и балансировки нагрузки. Системные администраторы освобождаются от забот об обслуживании и пополнении расходных материалов, а необученные пользователи не вмешиваются в ремонт принтеров. Также в таких системах предусмотрены услуги по уничтожению важных документов. Множество проблем печати, однако, носит социальный характер и не может быть решено исключительно технологическими средствами.

**Глава 25. Хранение данных**

В системах, которыми мы управляем, хранится информация. Возможности компьютеров по хранению информации удваиваются каждые два года. Первые домашние компьютеры могли хранить 120 Кб на гибком диске. Сейчас речь идет о петабайтах — миллионах миллионов килобайтов. Каждый эволюционный скачок в емкости требовал радикального изменения методов управления данными.

Существует два ключевых факта о хранении данных. Первый из них — хранение становится всё дешевле, что кажется невероятным. Второй — оно становится всё дороже, что также сложно поверить.

Этот парадокс становится понятным, когда вы поработаете с хранением данных хотя бы недолгое время. Цена отдельных дисков постоянно снижается, и цена за мегабайт стала настолько низкой, что люди теперь говорят о цене за гигабайт. Когда в системах заканчивается дисковое пространство, люди часто жалуются на то, что могут пойти в местный компьютерный магазин и купить диск почти за копейки. Как же так? Разве может не хватать пространства?

К сожалению, стоимость подключения всех этих дисков и управления ими растет практически безгранично. Раньше диски подключались с помощью одного или двух шлейфов, которые стоили доллар за штуку. Сейчас волоконно-оптические кабели, подключаемые к контроллерам массивов данных, стоят тысячи долларов. Данные записываются несколько раз, и для доступа к данным с нескольких узлов одновременно применяются сложные протоколы. Это приводит к значительному росту расходов на системы аварийного восстановления и резервные копии. В сравнении с тем, сколько стоит управление данными, сами диски практически бесплатны.

Сдвиг основных акцентов с наличия пространства на управление данными на протяжении их жизненного цикла удивителен. Теперь обсуждается не цена за гигабайт, а цена за гигабайто-месяц. Данные, опубликованные в начале 2006 года одной из крупных IT-исследовательских фирм, показали изменение расходов на хранение. Для простых массивов с отражением различие в стоимости предложений низкого и высокого класса составляло два порядка.

Хранение данных — это широкая тема, по которой написано много хороших книг. В данной главе мы сосредоточимся на основной терминологии, некоторых размышлениях об управлении хранением и ключевых методах. Каждый из этих методов представляет собой инструмент, готовый к применению при необходимости.

**Основы**

Чтобы хранение данных не стало войной между поставщиками и потребителями, мы предлагаем радикальную идею, что хранение должно управляться как ресурс сообщества. Это задает управление хранением в направлении, где каждый может работать для достижения общих целей по пространству, времени работы, производительности и расходам. Хранение должно управляться так же, как и любая другая служба, и у нас есть советы в этой области. Производительность, устранение неполадок и оценка новых технологий являются обязанностью группы обслуживания систем хранения.

Но начнем мы с краткого экскурса в терминологию и технологии хранения данных.

**25.1.1. Терминология**

Как системному администратору, вам может быть уже знакомо множество терминов из области хранения данных. Поэтому мы кратко выделим основные термины и ключевые принципы, которые будут использоваться в этой главе.

**25.1.1.1. Основные элементы отдельных дисков**

Для понимания производительности различных систем хранения важно разбираться в компонентах, из которых состоят диски, и основных операциях жесткого диска. Знание узких мест этих элементов помогает понять узкие места и улучшения в более сложных системах.

* **Шпиндель, пластины и головки**: Жесткий диск состоит из нескольких пластин, на которых записаны данные. Пластины крепятся на одном шпинделе и вращаются вместе. Данные на пластинах записываются на дорожках, которые представляют собой окружности, радиус которых зависит от их расположения на пластине. Дорожки, находящиеся дальше от центра, длиннее и имеют больше блоков данных. Головки диска считывают и записывают данные, находясь над соответствующими дорожками. На каждой пластине есть одна головка, но все они перемещаются вместе. Обычно за раз считывается целая дорожка или цилиндр. Время, необходимое для перемещения головок в нужное место (время поиска), больше, чем время, требуемое для полного оборота диска.
* **Контроллер диска**: Это электроника, которая реализует протоколы доступа к диску, такие как SCSI или ATA. Контроллер связывается с узлом, к которому подключен диск, и управляет обменом данных между диском и системой. Для контроллеров важны стандарты и улучшения производительности, такие как буферизация или кэширование.
* **Адаптер главной шины (HBA, Host Bus Adapter)**: HBA управляет связью между диском (или дисками) и сервером. Использует протоколы доступа к данным для передачи информации. Интеллектуальные HBA могут повышать производительность. Обычно такие адаптеры располагаются на материнской плате или в виде карт расширения.

**25.1.1.2. RAID: Избыточный массив независимых дисков**

RAID (Redundant Array of Independent Disks) — это метод, использующий несколько независимых жестких дисков для создания хранилища, которое может быть больше, надежнее или быстрее, чем один диск. Каждый метод RAID называется уровнем (см. таблицу 25.1).

* **RAID 0** (распределение данных): Данные распределяются по нескольким дискам, что позволяет создать один большой диск. RAID 0 обеспечивает большую скорость, так как несколько операций чтения и записи могут выполняться параллельно на разных дисках. Однако, если один диск выходит из строя, все данные теряются. Это повышает риски, так как вероятность сбоя возрастает с количеством дисков.
* **RAID 1** (отражение): Использует два или более диска для записи одних и тех же данных. Все операции записи выполняются на обоих дисках одновременно. Это повышает надежность: если один диск выходит из строя, система продолжает работать. Скорость записи определяется самым медленным диском, но чтение данных может быть ускорено за счет распределения операций между дисками.
* **RAID 2 и 3**: Эти методы используются реже, но RAID 3 может быть полезен для потоковых данных и видеоприложений, так как он предоставляет хорошую производительность при последовательном чтении.
* **RAID 4**: Похож на RAID 5, но использует один диск для хранения данных четности. Обычно медленнее, чем RAID 5, но может быть быстрее, если система специально настроена для этого.
* **RAID 5** (распределенный контроль четности): Повышает надежность, аналогично RAID 1, но с меньшими затратами. Включает один дополнительный диск для хранения данных восстановления. Если один диск выходит из строя, данные на нем восстанавливаются с помощью информации на других дисках. RAID 5 обеспечивает высокую скорость чтения, но может иметь большую задержку записи из-за необходимости вычисления и записи информации восстановления.
* **RAID 6**: Аналогичен RAID 5, но имеет два диска для хранения информации восстановления, что повышает надежность, но может снизить скорость записи.
* **RAID 10** (RAID 1 + 0): Сочетает преимущества RAID 0 (повышение производительности за счет распределения данных) и RAID 1 (повышение надежности через отражение). Это система, состоящая из нескольких блоков RAID 0, каждый из которых отражается с использованием RAID 1. Это уменьшает влияние потери диска на производительность по сравнению с RAID 5.

RAID-системы часто поддерживают функцию "горячей замены", позволяющую заменить неисправный диск на новый без остановки работы системы.

**25.1.1.3. Тома и файловые системы**

**Том** — это элемент хранилища данных, который сервер воспринимает как логический диск. Ранее томом был только отдельный диск, однако с развитием технологий, таких как разделы и RAID-системы, томами могут быть более сложные структуры хранения данных. Сервер видит том как единое целое, даже если он состоит из нескольких физических частей.

Каждый том отформатирован файловой системой, которая определяет способ организации данных на этом томе. Разные файловые системы были разработаны для решения конкретных задач, улучшения производительности или обеспечения надежности. В Windows распространены такие файловые системы, как FAT, DOS FAT32 и NTFS. В UNIX/Linux-системах популярны UFS, UFS2, EXT2/EXT3, ReiserFS и другие. Некоторые файловые системы используют **протоколирование**, что помогает ускорить запись данных и восстановление после сбоя, записывая изменения в упрощенном виде и затем применяя их за один раз.

**25.1.1.4. DAS: хранилище прямого подключения**

**DAS (Directly Attached Storage)** — это хранилище, которое подключено непосредственно к серверу, обычно через кабели, но не по сети. Это может быть простой жесткий диск или RAID-массив, подключенный напрямую к серверу. В DAS хранилище и сервер находятся в тесной связи, но не через сетевую инфраструктуру, что делает это решение простым и быстрым, но ограниченным в возможностях.

**25.1.1.5. NAS: хранилище сетевого подключения**

**NAS (Network-Attached Storage)** — это технология, при которой хранилище подключается к сети и доступно для клиентов через сетевые протоколы. В UNIX-системах для этого используется NFS (Network File System), а в системах Windows — CIFS (Common Internet File System). NAS предоставляет возможность централизованного хранения файлов и их совместного использования множеством пользователей и устройств в сети. Такие решения часто предлагают поставщики, например, Network Appliance и EMC для крупных организаций, а для малого бизнеса — такие компании как Linksys.

**25.1.1.6. SAN: сети хранения данных**

**SAN (Storage Area Network)** — это специализированная сеть, которая соединяет серверы и системы хранения данных с помощью высокоскоростных соединений и протоколов, оптимизированных для работы с данными. В SAN серверы могут подключаться к любому тому системы хранения, будь то диск или группа RAID. Серверы взаимодействуют с системой хранения на уровне блоков, а не файловой системы, что позволяет улучшить производительность и гибкость. Одной из особенностей SAN является возможность подключения нескольких серверов к одному тома через кластерные файловые системы. Это упрощает резервное копирование, так как один сервер может использовать общий ресурс, например, магнитную ленту. SAN также помогает улучшить использование хранилища, так как дисковое пространство не ограничено изоляцией между серверами.

**25.1.2. Управление хранением**

Управление хранением данных включает сочетание процессов и технологий для эффективного использования и контроля хранилищ. Успешные решения в области управления хранением не предполагают, что системные администраторы будут работать как "полиция", а наоборот, обеспечивают сотрудничество с пользователями. Зачастую пользователи обращаются к системным администраторам с запросами на дополнительное дисковое пространство для конкретных приложений. Применение принципов, направленных на предотвращение проблем с хранением, может существенно снизить количество экстренных запросов и повысить эффективность работы с хранилищами.

**25.1.2.2. Проведите оценку потребностей хранения**

Первый шаг в оценке потребностей хранения данных — это не анализ текущего использования систем, а общение с подразделениями и группами, которые используют эти системы. Это необходимо для того, чтобы понять их реальные потребности. Начинать с анализа существующих ресурсов может вызвать у сотрудников беспокойство, так как они могут подумать, что их ресурсы будут перераспределены без учета их мнения.

Важно наладить доверительные отношения с пользователями, чтобы понять их потребности. Один из способов — это использование данных о росте объемов хранения за последний год. Это поможет не только продемонстрировать рост их объема хранения, но и обучить их, а не критиковать, помогая выявить реальные потребности.

Некоторые группы могут предоставлять неточные данные, боясь нехватки ресурсов, в то время как другие, несмотря на нехватку, не жалуются, полагая, что все находятся в одинаковой ситуации.

**Какие вопросы нужно задавать при оценке потребностей в дисковом пространстве?**

Необходимо узнать о текущем и прогнозируемом использовании дисков в течение 6-18 месяцев. Хорошо использовать привычные единицы измерения, такие как кварталы или семестры, чтобы пользователи могли точнее указать прогнозы. Важно также поинтересоваться, какие приложения запускаются в группе, и какие проблемы возникают при их использовании.

Кроме того, хотя вы можете наблюдать за использованием дискового пространства, перегрузка некоторых элементов инфраструктуры может не быть заметна по простым показателям. Сведения, предоставленные пользователями, могут выявить проблемы, которые не видны при стандартном анализе.

**25.1.2.3. Отражайте группы в инфраструктуре хранения**

Когда вы соберете информацию о текущих и будущих потребностях пользователей в системах хранения, следующим шагом будет отражение групп и подгрупп в инфраструктуре хранения. На этом этапе нужно решить, стоит ли группировать пользователей по схожим потребностям в приложениях или по структуре отчетности и рабочих групп.

Если возможно, лучше распределять пользователей по подразделениям или группам, а не по текущему использованию. Большинство проблем с ресурсами хранения связаны с политическими и финансовыми вопросами. Создание рабочих групп с общим доступом к серверу или тому системы хранения позволяет разрешить споры о распределении ресурсов внутри этой группы. Также важно использовать групповые разрешения на запись, чтобы ограничить доступ к хранилищу только для членов группы.

Некоторые пользователи, распределенные по нескольким подразделениям или группам, могут иметь схожие, но необычные требования. В таких случаях стоит создать общее хранилище, которое удовлетворяет их потребности. Сервер хранения может быть разделен на несколько томов, изолируя каждую группу на своем разделе. Это помогает избежать конфликтов из-за ресурсов и устраняет необходимость участия системных администраторов в разрешении конфликтов.

Если в вашей среде поддерживаются квоты, и пользователи не против их применения, можно установить индивидуальные квоты внутри группы для контроля использования пространства. Временно установив групповые квоты, можно перераспределить объемы хранения.

Однако многие пользователи будут против применения квот, аргументируя это снижением производительности в критических ситуациях. Например, если инженер сталкивается с ограничением квоты и не может продолжить работу, это может нарушить график проекта. Важно выслушать их аргументы и рассмотреть возможные компромиссы, такие как экстренные запросы с гарантированным временем ответа.

**25.1.2.4. Разработайте политику хранения запасных частей**

В большинстве компаний имеются запасы часто требуемых запчастей. Однако хранение этих запасных частей требует особого внимания. Ранее типы дисков для систем хранения сильно различались, что позволяло проще выделить запасные диски для инфраструктурного использования. Сегодня многие массивы хранения и серверы рабочих групп используют одинаковые диски, что усложняет процесс выделения запчастей для конкретных нужд.

Лучше всего отделять запасные диски общего назначения от запасных дисков для инфраструктуры хранения. Прогнозировать количество необходимых дисков можно, основываясь на сбоях аналогичного оборудования в прошлом. Это позволит оценить, сколько запасных дисков потребуется для поддержания системы в рабочем состоянии.

При росте объемов хранилищ необходимо не только планировать закупку новых дисков, но и учитывать возможную модернизацию серверов, например, процессоров и памяти. При расширении хранилищ за счет новых систем следует заранее закупить запчасти для этих систем, чтобы они были доступны в случае поломки.

**25.1.2.5. Планируйте будущее хранение**

Особенностью работы с запасными частями для систем хранения является то, что когда пользователь запрашивает новый диск, ему часто нужно гораздо больше, чем просто сам диск. Например, если отказал системный диск, помимо нового диска пользователю потребуется и установка ОС. Если у пользователя заканчивается пространство и он хочет установить новый диск, необходимо обеспечить не только дополнительное место, но и резервное копирование.

Важно, чтобы системные администраторы помогали пользователям, а не становились препятствием. Нужно понимать, что каждый раз, когда диск покидает склад, возможно, потребуется что-то еще. Важно предвидеть такие проблемы заранее, чтобы минимизировать их последствия в будущем.

Для упрощения этого процесса можно организовать резервное копирование на рабочих станциях, где программы смогут автоматически обнаружить новый раздел и начать его копирование. Также стоит предоставить пользователям доступ к сетевым загрузочным дискам и инструкциям по установке ОС на новый диск, что позволит ускорить процесс замены дисков и восстановления системы.

Планирование регулярных технологических перерывов поможет своевременно обновлять системы хранения, удовлетворяя перспективные требования пользователей и предотвращая дефицит места.

**25.1.2.6. Создайте стандарты хранения**

Наличие стандартов хранения помогает контролировать и упрощать процесс закупок и поддержания оборудования. Если в организации есть стандарты хранения, люди с меньшей вероятностью смогут проводить заказ нестандартного оборудования, ожидая, что вы будете поддерживать все системы.

Стандартизация решений по хранению помогает избежать поддержания несовместимого оборудования и упрощает работу с системами. Стандарты могут быть простыми (например, определение закупок только определенного бренда) или более сложными (подробные требования к поставщикам и оборудованию). Стандарты необходимы для обеспечения целостности системы и упрощения процесса интеграции.

Преимущества стандартизации включают создание единого набора запасных частей и минимизацию количества различных систем, с которыми должен работать системный администратор. Установка стандартов помогает унифицировать среду и улучшить работу с оборудованием.

Если в вашей организации уже есть стандарты для определенных типов запросов, начните с их изучения и добавления стандартов для систем хранения. Если стандартов нет, проявите инициативу и начните работу с финансовым отделом и руководителями для создания базы стандартов и унифицированных запасных частей.

**25.1.3. Хранение как служба**

Когда рассматриваете систему хранения, полезно думать о ней не как о статичном объекте, а как о сервисе, предоставляющем определенные услуги. Это подход позволяет применить стандартные принципы управления сервисами, такие как SLA (Service Level Agreement) и мониторинг доступности, чтобы обеспечить соблюдение договорных условий.

**25.1.3.1. SLA хранения**

SLA для хранения данных включает в себя несколько ключевых аспектов:

1. **Объем пространства**: для разных отделов, таких как инженерия, финансы или группа качества, требования могут различаться по объему доступного дискового пространства. Например, инженерам нужно пространство для ежедневной работы, а финансистам — большее количество на квартальные отчеты.
2. **Время ответа**: это задержка, с которой система отвечает на запросы пользователей, что важно для служб, где критично время, например, при тестировании или сдаче экзаменов.
3. **Время на исправление неполадок (MTTR)**: SLA должен также включать требования по времени на устранение неисправностей, чтобы предотвратить длительные простои.

Все эти показатели должны быть измеряемыми с помощью стандартных инструментов тестирования, что позволит проверять, соответствует ли система заявленным характеристикам в реальных условиях.

**25.1.3.2. Надежность**

Независимо от того, насколько тщательно вы проектируете систему хранения, сбои — это неизбежность. Однако можно минимизировать их влияние, чтобы система продолжала работать, даже если отдельные компоненты выходят из строя.

* **RAID**: Все уровни RAID, кроме RAID 0, обеспечивают избыточность данных, что делает систему более устойчивой к сбоям. При использовании RAID с горячей заменой дисков можно значительно повысить надежность. Однако важно осуществлять постоянный мониторинг состояния системы и иметь запасные диски для замены.
* **NAS**: Системы NAS также могут быть настроены с поддержкой RAID, но их надежность зависит от качества сети. Для увеличения надежности стоит подключать интерфейсы NAS к разным коммутаторам, что обеспечит отказоустойчивость.

Чтобы обеспечить нужный уровень надежности, важно понять, что идеальная отказоустойчивость стоит очень дорого. В большинстве случаев организации не могут позволить себе полностью отказоустойчивые системы, поэтому нужно находить компромисс между стоимостью и уровнем доступности.

**Реальные требования к времени безотказной работы и стоимость системы защиты данных:**

* Высокая доступность данных и защита от потерь данных стоят дорого, особенно при использовании таких технологий, как Непрерывная защита данных (CDP), которая является наиболее дорогим решением.
* Системные администраторы должны информировать руководство о стоимости обеспечения высокой доступности и о том, что важно учесть эти расходы при принятии решений о бюджете и рентабельности инвестиций.

В конечном итоге, важно найти баланс между затратами на защиту данных и теми рисками, которые организация готова принять.

**25.1.3.3. Резервное копирование**

Стратегия резервного копирования — это ключевой элемент системы хранения данных. Важно понимать, что системы RAID, NAS и SAN не являются полными решениями для резервного копирования, хотя они могут повышать надежность и упрощать процесс.

### RAID и резервное копирование

RAID — это не стратегия резервного копирования. Хотя RAID увеличивает надежность за счет избыточности, потеря данных все равно возможна при повреждении нескольких дисков, стихийных бедствиях или ошибках оборудования. Например, в случае поломки двух дисков из системы RAID 5 или RAID 6 данные могут быть утрачены. Более того, восстановление данных с зеркальных дисков RAID не поможет в случае физического разрушения оборудования, например, при пожаре.

Для полноценной защиты данных необходимы регулярные резервные копии на внешних носителях, таких как магнитные ленты или другие диски. Системы RAID могут помочь в случае ошибок, связанных с удалением файлов или частичными повреждениями, но они не являются заменой традиционным резервным копиям.

### Зеркальные тома RAID

Использование зеркальных томов RAID для резервного копирования — популярная практика, особенно в случае, когда нужно создать "статичную" копию данных. В таком случае один из зеркальных томов временно отсоединяется, чтобы создать резервную копию данных. После завершения копирования зеркало снова подключается и синхронизируется. Такой подход помогает избежать влияния резервного копирования на нормальную работу системы. Однако важно понимать, что во время выполнения резервного копирования данные не защищены, и производительность системы может замедлиться.

### Ускорение резервного копирования с помощью зеркальных томов RAID

Для ускорения резервного копирования можно использовать конфигурацию с несколькими зеркальными томами (например, три зеркала). Один из них временно отключается для создания резервной копии, в то время как данные на других двух зеркалах продолжают быть доступными, что позволяет минимизировать воздействие на производительность.

### NAS и резервное копирование

В случае NAS-систем резервное копирование упрощается, поскольку все данные пользователей централизованы на сервере NAS. Задача резервного копирования становится проще, так как все важные данные находятся в одном месте, и копии можно делать без вмешательства пользователей. Это позволяет уменьшить нагрузку на серверы приложений и другие вычислительные ресурсы.

### SAN и резервное копирование

SAN-системы значительно упрощают процесс резервного копирования. Они обеспечивают централизованное решение для записи резервных копий, например, через подключение устройств к SAN, что позволяет серверам совместно использовать дорогостоящее оборудование для резервного копирования. Также выделенная сеть для трафика данных позволяет разделить обычный рабочий трафик и трафик резервного копирования, что улучшает производительность.

Системы SAN также могут создавать образы LUN (логических единиц хранения), которые позволяют создавать резервные копии данных в автономном режиме без влияния на работу серверов. Это помогает проводить резервное копирование в любое время, не прерывая нормальной работы системы.

**25.1.4. Быстродействие**

Под быстродействием системы хранения данных понимается время, которое требуется пользователям для чтения и записи данных. Если система слишком медленная, пользователи могут искать способы обхода, например, подключать дополнительные диски. Чтобы оптимизировать производительность, необходимо использовать измерения и данные, а не полагаться на догадки.

**Общие принципы оптимизации быстродействия**

1. **Не обращайтесь к сети, если можно использовать диск.**
2. **Не обращайтесь к диску, если можно использовать память.**
3. **Не обращайтесь к памяти, если можно использовать чип.**
4. **Инвестируйте в технологии и не бойтесь тратить деньги на улучшения производительности.**

**Оптимизация с помощью RAID**

RAID-конфигурации могут существенно влиять на быстродействие.

* **RAID 0** — Максимизация быстродействия как чтения, так и записи за счет распределения операций по нескольким дискам, что позволяет выполнять параллельные операции. Однако эта конфигурация не обеспечивает избыточности, и потеря одного диска приведет к потере всех данных.
* **RAID 1** — Повышает быстродействие чтения, если операции чтения распределяются между дисками. Однако скорость записи ограничена производительностью самого медленного диска в зеркальном массиве.
* **RAID 3** — Обеспечивает отличное быстродействие при последовательном чтении, что идеально подходит для хранения больших графических файлов, видеоданных и архивированных данных, которые не часто изменяются.
* **RAID 4 и RAID 5** — Хороши для быстрого чтения данных, так как диски могут работать параллельно. Однако скорость записи снижена, потому что запись на блоки данных требует дополнительных операций чтения и записи на диск контроля четности. В RAID 5 операция записи более сложная, так как требуется обновить диск с контролем четности после каждого изменения.
* **RAID 10** — Обеспечивает высокое быстродействие как при чтении, так и при записи. Это сочетание RAID 1 и RAID 0, обеспечивающее избыточность без потери производительности. Однако скорость записи зависит от самого медленного зеркального диска.

**NAS и быстродействие**

Системы хранения данных на базе NAS помогают изолировать нагрузку по передаче файлов от других серверов, что облегчает управление данными и повышает быстродействие. Перемещение хранения данных на серверы NAS уменьшает нагрузку на другие вычислительные ресурсы. Это позволяет снизить загрузку серверов и ускорить доступ к файлам для пользователей. Хотя полная оптимизация не всегда возможна (например, нужно будет запускать клиентский протокол для доступа к NAS), это решение часто дает явные преимущества в производительности.

**25.1.5. Оценка новых решений по хранению**

При выборе решения для хранения данных важно учитывать модель использования, пропускную способность и конфигурацию системы. Анализ этих факторов поможет сделать осознанный выбор и избежать скрытых проблем. Нужно быть особенно внимательным к «подводным камням», например, к решению, которое кажется дешевым из-за использования ресурсов вашего сервера для выполнения части работы.

**Основные моменты для оценки решений:**

* **Тестирование системы:** Даже если решение выглядит привлекательным по цене, оно может иметь скрытые недостатки, например, слишком медленные диски или неудачные конфигурации. Всегда тестируйте систему перед ее окончательной доставкой и настройкой.
* **Нестандартные компоненты:** Некоторые компании могут использовать менее качественные компоненты, чтобы снизить цену. Это может привести к ухудшению производительности или проблемам с совместимостью. Важно настаивать на соблюдении стандартов компонентов.

**25.1.6. Распространенные проблемы**

Системы хранения данных могут столкнуться с различными проблемами, если не были учтены граничные условия на каждом уровне системы.

**Основные типы проблем:**

1. **Физическая инфраструктура:** Современные серверные и информационные центры часто проектируются с учетом старых систем, и проблемы с электропитанием или охлаждением могут вызывать ошибки в работе. Несоответствие мощности и температуры может привести к сбоям в работе системы хранения. Контроль питания должен быть включен в мониторинг.
2. **Превышение времени ожидания:** Проблемы с превышением времени ожидания могут возникать, особенно в сильно оптимизированных системах, когда изменения в сети (например, изменение топологии) увеличивают задержки. Это может вызвать проблемы с подключением к устройствам NAS или SAN.

**Примеры распространенных проблем:**

* **Проблемы с питанием:** Нестабильное питание может привести к непредсказуемым сбоям. Например, в одном случае блок NAS стал стабильным после изменения его расположения для обеспечения лучшего питания.
* **Тайм-ауты:** В случае с NAS-системами или другими решениями хранения данных можно столкнуться с превышением времени ожидания, если сеть перегружена или если устройство не может обработать запросы вовремя.

При выборе решения для хранения данных важно учесть все эти аспекты, чтобы избежать скрытых проблем, которые могут возникнуть на разных уровнях системы.

**25.2. Тонкости**

После рассмотрения основ хранения данных как управляемой службы и требований, которые с этим связаны, важно рассмотреть методы улучшения работы вашей службы хранения, оптимизируя её для конкретных приложений.

**25.2.1. Оптимизация использования RAID по приложениям**

Системы RAID предлагают различные уровни производительности и надежности, которые можно настроить в зависимости от нужд конкретных приложений. Основная идея — выравнивание размера блока данных с размером блока, который используется в вашем приложении, что позволяет значительно повысить быстродействие.

**25.2.1.1. Настройка распределения данных**

В некоторых случаях настройка блока распределения данных в RAID под размер блока, используемый в приложении, может сильно повысить производительность. Например, для базы данных Oracle, если размер блока в базе данных будет равен размеру блока распределения данных в массиве RAID, это приведет к лучшему быстродействию.

Пример:

* Для базы данных с блоками размером 32 КБ, обслуживаемой RAID 5 из пяти дисков, можно настроить размер блока распределения в 8 КБ (4 диска с данными и 1 диск с четностью). Если увеличить количество дисков в массиве, например, до девяти, можно улучшить производительность, используя размер блока в 4 КБ.

Важно помнить, что не все приложения требуют такой глубокой настройки. Также необходимо, чтобы размер блока был поддерживаем всем путем ввода/вывода, иначе производительность может снизиться из-за несоответствия с блоками операционной системы.

**25.2.1.2. Упорядочение записи**

Некоторые приложения могут сталкиваться с проблемами производительности, если несколько операций записи происходят одновременно в независимые потоки данных. Например, если один процесс записывает большое количество данных в файл лога, а другой процесс работает с данными на том же диске, это может привести к замедлению работы.

Решение: переместить файл лога на другой диск, чтобы разгрузить основной диск от интенсивных операций записи. Это также применимо к базам данных, процессам сборки программ, файлам с протоколированием транзакций и другим интенсивно записывающим системам. Разделение потоков записи по различным дискам помогает улучшить быстродействие.

Пример:

* Для базы данных можно разместить данные таблиц на медленном, но надежном RAID-массиве, а индексы и виды (часто обновляемые данные) — на более быстром, но менее надежном зеркальном массиве. Даже если быстрый массив потеряет диск, благодаря резервным копиям восстановление данных будет быстрым и не повлияет сильно на доступность.

Таким образом, эффективная настройка RAID и грамотное распределение потоков записи помогают повысить производительность и надежность хранения данных в различных приложениях.

### 25.2.2. Пределы хранения: отставание плотности доступа к диску

Современные жесткие диски обеспечивают невероятную плотность хранения данных, но скорость их работы не растет с такой же скоростью. Например, диск, который раньше мог вмещать 500 МБ данных, теперь может хранить несколько терабайт, но производительность увеличивается лишь на 10-20%, в то время как емкость увеличивается на 40-60%. Это приводит к растущему разрыву между объемом данных, который может вмещать диск, и его возможностью быстро выполнять операции ввода/вывода (I/O). Этот разрыв называется плотностью доступа к диску (Disk Access Density, DAD) и измеряется в операциях ввода/вывода на гигабайт емкости (операции/с/Гб).

При выборе дисков многие пользователи ошибочно ориентируются только на емкость, не принимая во внимание DAD. Диски с высокой емкостью подходят для ресурсов с низкими требованиями по производительности, но для приложений с высокой интенсивностью ввода/вывода (особенно записи) нужно обращать внимание на лучший DAD. В таких случаях использование меньших по размеру, но более быстрых дисков может быть более эффективным, несмотря на дополнительные расходы на питание, охлаждение и пространство в корпусе.

Примером может служить база данных, в которой активно обновляются только некоторые таблицы. Чтобы обеспечить лучший доступ к данным, часто используемые таблицы могут быть размещены на более быстрых, но меньших дисках. Это может привести к повышению производительности.

### 25.2.2.1. Фрагментация

Когда данные записываются на диск, операционные системы стремятся расположить все блоки одного файла на одной дорожке, что позволяет ускорить чтение. Однако, по мере заполнения диска становится все сложнее найти смежные блоки для записи новых файлов, что приводит к фрагментации.

Ранее системные администраторы часто дефрагментировали диски, чтобы улучшить производительность. Однако в современных операционных системах фрагментация не так сильно влияет на быстродействие, особенно если файл был фрагментирован случайным образом. Дефрагментация может даже представлять собой риск из-за возможных ошибок в программах и проблем с потерей данных, если произойдут сбои в процессе.

В многопользовательских системах, таких как серверы NFS или CIFS, фрагментация может не сильно повлиять на производительность, особенно если операционная система уже оптимизирует запросы для минимизации движения головки диска. В таких случаях дефрагментация может не быть необходимой и только добавляет дополнительные риски.

### 25.2.3. Непрерывная защита данных (CDP)

Непрерывная защита данных (Continuous Data Protection, CDP) — это процесс копирования изменений данных в определенные временные промежутки в одно или несколько дополнительных средств хранения. Это позволяет восстанавливать данные до определенного момента времени, повторяя изменения или отменяя их. CDP используется для минимизации времени восстановления и предотвращения потери данных.

CDP обычно используется в системах, где данные имеют критическое значение (например, финансовая информация) или где изменения происходят очень часто. Хотя CDP может быть дорогим, оно оправдано в случае, если потеря данных может привести к серьезным последствиям, таким как потеря прибыли или выполнение обязательств.

### Заключение

В этой главе были рассмотрены основные типы систем хранения данных, их преимущества и применимость для различных приложений. Основной принцип — строить решения по хранению, исходя из нужд конкретных приложений, и строить уровни избыточности для обеспечения надежности, с минимальной потерей производительности.

Хотя стоимость дисков снижается, управление ими становится дороже. Применение концепций, таких как RAID, позволяет оптимизировать решения для хранения, улучшая производительность в зависимости от потребностей приложений. Важным моментом остается растущий разрыв между плотностью хранения и скоростью доступа к данным, который будет только увеличиваться в будущем.

### Глава 26. Резервное копирование и восстановление

Резервные копии – это неотъемлемая часть любой системы хранения данных. Несмотря на то, что они часто воспринимаются как неудобные и дорогостоящие, они играют критическую роль в обеспечении возможности восстановления данных, которые могут быть утеряны, повреждены или удалены по ошибке. Резервное копирование — это как страховка: никто не хочет ею пользоваться, но она необходима на случай катастрофы.

#### Задача резервного копирования

Основной задачей резервного копирования является обеспечение возможности быстрого восстановления данных в случае их потери. Потеря данных может произойти по множеству причин, таких как поломка оборудования, случайное или преднамеренное удаление файлов, катастрофы и другие непредвиденные обстоятельства. Именно возможность восстановить данные в случае непредвиденной потери делает резервное копирование таким важным.

#### Резервное копирование и восстановление данных

Часто существует путаница, потому что резервное копирование — это не самоцель, а лишь средство для обеспечения восстановления данных. В идеале система должна называться не "система резервного копирования", а "система резервного копирования и восстановления", или еще точнее — "система восстановления данных", так как конечной целью является восстановление, а не сам процесс копирования.

В этой главе рассматривается подход к резервному копированию, ориентированный на теорию планирования, а не на технические детали, такие как команды в операционных системах для выполнения резервных копий, которые, скорее всего, читатель уже знает. Мы сосредоточимся на ключевых компонентах современных систем резервного копирования, таких как автоматизация, централизация и управление запасами, которые помогут при принятии решения о покупке решения для резервного копирования.

#### Экономические аспекты резервного копирования

Исследования показывают, что стоимость приобретения дисков составляет лишь около 20% от общих затрат на хранение данных, в то время как большая часть расходов идет на резервное копирование. Легко приобрести диск, но гораздо сложнее обеспечить полноценную службу хранения данных, которая бы включала эффективное резервное копирование и восстановление. Это важный аспект, поскольку именно системы резервного копирования и восстановления могут значительно увеличить затраты на хранение данных.

#### Основные типы резервного копирования

* **Полное резервное копирование**: это процесс полного копирования всех файлов раздела. В UNIX-системах это называется «резервное копирование уровня 0».
* **Инкрементальное резервное копирование**: это копирование всех файлов, которые изменились с последнего резервного копирования. В UNIX это называется «резервное копирование уровня 1». Инкрементальные резервные копии имеют тенденцию расти со временем, поскольку каждое новое инкрементальное резервное копирование включает изменения, сделанные с последнего копирования. Например, если полное резервное копирование выполняется в воскресенье, а инкрементальные — в следующие дни недели, то резервная копия в пятницу будет включать все файлы, которые были в предыдущих инкрементальных копиях с понедельника по четверг, а также изменения, произошедшие в четверг.
* **Инкрементальные резервные копии уровней 2 и выше**: в некоторых системах инкрементальные копии могут собирать все файлы, измененные с момента последнего инкрементального резервного копирования, а не с последнего полного. Эти копии могут быть названы инкрементальными уровня 2, 3 и так далее, в зависимости от того, с какого резервного копирования они собирают изменения.

### 26.1. Основы

Процесс создания системы резервного копирования и восстановления начинается с определения желаемого конечного результата — того, что именно вы хотите получить от системы восстановления. Целью является обеспечение возможности восстановления данных в случае потери, сбоя или других непредвиденных ситуаций. Разные причины, по которым требуется восстановление данных, влияют на дальнейшие решения, включая разработку политики, создание графика резервного копирования и выбор методов восстановления.

#### Структура документации для системы резервного копирования:

1. **Корпоративные инструкции**: Документ, который определяет терминологию, минимальные и рекомендуемые требования для системы восстановления данных.
2. **SLA (Service Level Agreement)**: Соглашение, которое определяет требования к конкретному месту или приложению, руководствуясь корпоративными инструкциями.
3. **Политика**: Документирует, как SLA будет реализовано в общих терминах, доступных и понятных для всех пользователей.
4. **Процедура**: Показывает, как должна реализовываться политика. Это набор шагов, который объясняет, как именно будут выполняться действия по резервному копированию и восстановлению.
5. **График**: Подробное расписание резервного копирования для каждого диска, может быть статическим или динамическим. Он переводит политику на язык конфигурации программы резервного копирования.
6. **Рабочие вопросы**: Включают в себя вопросы, касающиеся расходных материалов (например, стоимость носителей для резервных копий) и бюджетирования. Для успешного выполнения SLA как в процессе резервного копирования, так и восстановления, требуется тщательное планирование времени и емкости системы.

Все эти элементы должны быть документированы как для пользователей, так и для системных администраторов, чтобы обеспечить четкость в действиях и соблюдение стандартов.

#### Ключевые компоненты для построения системы:

После того как определены основные принципы, можно приступать к созданию системы резервного копирования и восстановления. В современных системах есть три ключевых компонента, которые обеспечивают эффективность работы:

* **Автоматизация** — процесс автоматического выполнения резервного копирования и восстановления.
* **Централизация** — управление всеми резервными копиями в одном месте для удобства мониторинга и восстановления.
* **Управление запасами** — управление количеством и состоянием носителей для резервного копирования, что гарантирует наличие нужных ресурсов.

### 26.1.1. Причины для восстановления данных

Восстановление данных требуется по трем основным причинам. Понимание этих причин поможет настроить систему резервного копирования и восстановления так, чтобы она могла эффективно справляться с каждым типом проблемы.

1. **Случайное удаление файлов**: Пользователь случайно удаляет один или несколько файлов, и требуется восстановить их. Это один из самых распространенных сценариев, требующих системы восстановления данных.
2. **Сбой диска**: В случае поломки жесткого диска все данные теряются, и необходимо провести полное восстановление всех файлов с резервной копии. Это требует, чтобы система обеспечения резервного копирования могла работать с большими объемами данных.
3. **Просмотр архивных данных**: Иногда необходимо регулярно хранить архивные данные для восстановления в случае катастрофы или по правовым и финансовым причинам (например, для аудита или выполнения обязательств). Система резервного копирования должна обеспечивать доступ к этим архивам в любой момент.

Разработка системы резервного копирования и восстановления, учитывая эти три типа сценариев, помогает создать гибкую и надежную систему, которая может справиться с любыми неожиданностями, происходящими с данными.

### 26.1.1.1. Случайное удаление файлов

В случае случайного удаления файлов пользователи предпочли бы возможность быстро восстановить файл в том виде, в каком он существовал на момент удаления. Однако это обычно невозможно, поскольку для восстановления данных требуется определенное время. В офисной среде, как правило, можно ожидать восстановления файла на следующий день, а процесс может занять 3-5 часов. Однако в таких высоко регулируемых сферах, как финансовый сектор или электронная коммерция, требования к скорости восстановления могут быть значительно выше.

Современные системы резервного копирования позволяют упростить этот процесс. Например, пользователи могут восстанавливать свои данные мгновенно, если лента ещё в приводе, или через некоторое время, если требуется загрузка ленты для восстановления. Важно отметить, что хотя лента часто используется как носитель для резервных копий, существуют и другие альтернативные методы хранения данных.

Для повышения удобства восстановления пользователи могут выполнять восстановление самостоятельно, что делает процесс более гибким и быстрым. Эта возможность была внедрена ещё в 1980-е годы:

* В начале 1980-х годов операционная система VAX/VMS от DEC (ныне HP через Compaq) позволяла сохранять предыдущие версии файлов, к которым можно было обращаться, указывая номер версии.
* В 1988 году в Bell Labs была разработана система File Motel, которая записывала инкрементальные резервные копии на оптические пластины.
* В 1990-х годах компания NetApp представила технологию создания образов файловых систем с возможностью хранения нескольких версий на диске.

Эти системы становятся всё более популярными с развитием технологий и снижением стоимости, а также с ростом ценности информации. Они помогают системным администраторам снизить нагрузку, переводя восстановление файлов в режим самообслуживания. Это дает пользователям возможность вернуть удалённые данные без вмешательства администраторов, что улучшает их взаимодействие с системой и повышает производительность. Также, пользователи могут более эффективно управлять своими рабочими процессами, зная, что всегда могут восстановить удалённые данные.

### 26.1.1.2. Сбои дисков

Сбои дисков представляют собой второй тип восстановления данных, который приводит к полной потере файловой системы. Это вызывает две основные проблемы: потерю обслуживания и потерю данных. В критических системах, например в электронной коммерции и финансовой сфере, используется RAID, что позволяет избежать потери обслуживания в случае поломки диска, минимизируя при этом потерю данных и снижения производительности.

Однако в некритических системах пользователи обычно могут ожидать восстановление в течение дня. Потеря данных в таких случаях может быть менее критичной, и зачастую утрата одного рабочего дня рассматривается как приемлемый риск. В некоторых случаях проблемы могут быть менее срочными, если данные на диске недоступны, но система продолжает работать.

Процесс восстановления после сбоя диска обычно занимает много времени. Восстановление может занять длительный период, поскольку восстанавливаются гигабайты данных, и доступ к данным не возможен до тех пор, пока не будет восстановлен последний файл. Этот процесс состоит из двух этапов:

1. Восстановление из последней полной резервной копии.
2. Восстановление всех инкрементальных резервных копий, сделанных после последнего полного резервного копирования.

Таким образом, время восстановления данных при сбое диска может быть значительным, особенно если система должна обработать большие объемы данных.

### 26.1.1.3. Просмотр архивных данных

Третий тип запросов на восстановление данных связан с необходимостью воспроизведения среды в определённый момент времени, например, через квартал, полгода или год назад. Это может быть связано с аварийными ситуациями или судебными процессами, когда необходимо предоставить архивные данные. Работа по созданию архивных копий аналогична выполнению полного резервного копирования, но с несколькими важными отличиями:

1. **Полные резервные копии:** Архивы представляют собой полные резервные копии. В отличие от обычных резервных копий, которые могут включать как полные, так и инкрементальные копии, архивы обычно не перемешиваются с другими типами резервных копий на одной ленте.
2. **Отделение архивных копий:** В некоторых компаниях могут требоваться отдельные архивные ленты, отличные от других резервных копий. В таком случае архивные копии создаются путём создания второго набора полных резервных копий или копированием уже существующих полных резервных копий на другие ленты. Это более сложный процесс, но при автоматизации он может быть выполнен без вмешательства человека.
3. **Хранение архивов вне офиса:** Архивные ленты обычно хранятся в месте, отличном от основного офиса, что добавляет уровень безопасности и защиты данных.
4. **Долговечность архивных лент:** Архивные ленты обычно хранятся дольше, чем обычные резервные копии. Однако со временем носители могут устаревать, и для их использования может потребоваться оборудование для чтения старых лент, а также соответствующее программное обеспечение.
5. **Правила для архивов:** Если архивы являются частью плана аварийного восстановления, для них могут действовать особые правила и законы, особенно в контексте сохранности данных для юридических или финансовых целей.

Кроме того, при создании архивных копий важно учитывать средства и инструменты, которые используются для работы с данными. Эти инструменты часто обновляются, и если архивные копии включают резервное копирование всей среды, необходимо обеспечить включение в архив инструментов и их особого набора возможностей. Важно также хранить документацию, связанную с восстановлением архивов, вместе с самими архивными данными.

### 26.1.2. Типы восстановления

Интересно, что три типа запросов на восстановление данных соответствуют трем различным типам пользователей:

1. **Восстановление отдельных файлов** — требуется пользователям, которые случайно удалили данные. Это типичный запрос от непосредственных пользователей данных.
2. **Архивные копии** — нужны для потребностей юридических и финансовых отделов, которые могут запрашивать данные для целей, связанных с правовыми вопросами, судебными разбирательствами и т. д. Эти запросы не делают непосредственно те, кто работает с данными, а скорее другие отделы, нуждающиеся в долгосрочной сохранности информации.
3. **Полное восстановление после поломки диска** — это задача для системных администраторов, которые должны выполнить восстановление данных согласно SLA (соглашению об уровне обслуживания). Такие восстановления часто являются частью корпоративной инфраструктуры и требуют особого внимания.

В среде, где обслуживание тарифицируется с высокой точностью, могут применяться разные тарифы для каждого типа восстановления. Например, различные группы пользователей могут оплачивать специфические услуги восстановления данных, как это происходит с другими корпоративными услугами. Для этого могут быть использованы разные программные обеспечения, а также могут возникнуть требования к физическому хранению данных и управлению лентами.

### 26.1.3. Корпоративные инструкции

Корпоративные инструкции по восстановлению данных являются важным документом для организации, который определяет требования к системам восстановления данных. Такие инструкции должны базироваться на правовых требованиях и минимальных требованиях, а не на детализированном описании реализации. Они должны быть достаточно гибкими для применения в разных ситуациях, с учётом особенностей бизнеса.

Основные аспекты, которые должны быть учтены в корпоративных инструкциях:

1. **Цели резервного копирования**: Документ должен начинаться с объяснения того, почему необходимы резервные копии данных, что составляет резервную копию и какие данные должны быть включены в процесс резервного копирования. Особое внимание следует уделить различным категориям данных (финансовые, важные для выполнения задач, проектные и т. д.), для которых должны быть определены отдельные требования.
2. **Разные SLA для типов данных**: Для различных типов данных должны быть установлены отдельные соглашения о уровне обслуживания (SLA). Например, для финансовых данных может быть более жёсткое требование по частоте резервного копирования и времени восстановления, чем для обычных данных.
3. **Планирование времени резервного копирования**: Очень важно тщательно планировать время для выполнения резервного копирования. Нельзя использовать стандартный временной промежуток (например, с полуночи до утра) для всех систем, поскольку это может сильно повлиять на производительность. Важно выбирать время для резервного копирования вне периодов пиковой нагрузки, чтобы минимизировать влияние на работу системы.
4. **Баланс потребностей**: При создании инструкций важно учитывать интересы разных подразделений (например, юридического отдела, бухгалтерии, системы безопасности). Эти подразделения могут требовать разных условий хранения и резервного копирования данных, например, короткие сроки хранения электронной почты в юридическом отделе или долгосрочное хранение финансовых данных в бухгалтерии.
5. **Опрос и консенсус**: Чтобы создать эффективные корпоративные инструкции, необходимо провести опрос среди различных групп (юридического отдела, высшего руководства, системных администраторов и пользователей). Нужно добиться консенсуса и учесть все требования и пожелания, обеспечив их соблюдение.
6. **Инструкции для небольших компаний**: В небольших компаниях может быть достаточно простой инструкции вроде «создавать резервные копии». Но с ростом компании важно разработать более детализированные инструкции с учётом требований инвесторов и юридических консультантов.

### 26.1.4. SLA и политика восстановления данных

SLA (Service Level Agreement) — это документ, который фиксирует обязательства по обслуживанию и его быстродействию, включая требования к восстановлению данных. Политика восстановления данных создаётся на основе SLA и определяет, как будет обеспечиваться выполнение этих обязательств.

Ключевые моменты при создании SLA и политики восстановления:

1. **Типы восстановления**: В SLA должны быть описаны три основных типа восстановления (индивидуальные файлы, архивные копии, полное восстановление после сбоя) и требования к каждому из них.
2. **Время восстановления и хранение**: В SLA должно быть указано, как быстро должны восстанавливаться данные, сколько времени будут храниться резервные копии, как часто должно выполняться резервное копирование и в какой промежуток времени оно может быть выполнено.
3. **Пример SLA**: Например, для восстановления данных в один рабочий день за последние полгода, для восстановления после сбоя диска за 4 часа с потерей данных не более чем за два рабочих дня. Архивы должны быть полными и создаваться каждый квартал, храниться вечно. Для критических данных могут быть установлены более высокие требования по частоте копирования и времени хранения.
4. **Политика на основе SLA**: Политика восстановления данных будет основываться на SLA, определяя частоту и типы резервных копий (например, полное или инкрементальное резервное копирование). Важно чётко прописать правила и требования для выполнения политики, чтобы она соответствовала нуждам бизнеса.

Таким образом, корпоративные инструкции и SLA должны быть взаимосвязаны и учитывать все необходимые требования для эффективного восстановления данных в случае аварий.

### 26.1.5. График резервного копирования

После того как SLA и политика восстановления данных установлены, следующим шагом становится создание графика резервного копирования, который будет учитывать, когда и какие данные нужно копировать с различных узлов системы. График резервного копирования должен учитывать требования SLA, а также гибкость в изменении в зависимости от меняющихся условий. Хотя SLA обычно остаётся неизменным, график может изменяться относительно текущих нужд и условий.

#### Основные аспекты создания графика:

1. **Частота резервного копирования**:
   * Резервное копирование должно выполняться регулярно, чтобы минимизировать потерю данных. Например, в случае поломки не зарезервированного диска, данные не должны теряться более чем за два дня.
   * Полное резервное копирование, которое занимает больше времени, обычно выполняется в выходные дни (например, с вечера пятницы до воскресенья), а инкрементальные резервные копии — в будние дни.
2. **Частота полного резервного копирования**:
   * В примере указано, что полное резервное копирование выполняется ежемесячно, но может быть разумным сделать это чаще (например, каждые четыре недели), чтобы избежать накопления слишком больших инкрементальных копий.
   * Чем чаще выполняется полное резервное копирование, тем меньше будет использовано места на лентах, так как инкрементальные копии, как правило, становятся всё больше по мере увеличения промежутка между полными копиями.
3. **Автоматизация**:
   * Современные программы для резервного копирования позволяют автоматически генерировать график на основе заданных требований. Например, система может сама рассчитать, когда необходимо выполнить полное или инкрементальное копирование, а также отправлять уведомления по электронной почте о необходимости заменить ленту.
4. **Пример с данными**:
   * Допустим, для раздела объёмом 4 ГБ задано полное резервное копирование каждые 28 дней, а инкрементальные копии выполняются ежедневно. В первый день месяца используется 4 ГБ для полного резервного копирования, на второй день — 200 МБ для инкрементальной копии, на третий — 400 МБ и так далее, пока к 11-му и 12-му дням объём инкрементальных копий не достигнет 2 ГБ и 2,2 ГБ, что больше, чем объём полной копии.
5. **Эффективность различных циклов**:
   * Таблица, представленная в главе, показывает, что использование различных циклов (ежедневный, 7-дневный, 14-дневный и т. д.) оказывает влияние на объём используемой ленты.
   * Наихудший вариант — это ежедневное полное резервное копирование, при котором на ленту записывается 168 ГБ данных, что является неэффективным использованием ресурсов. Лучше использовать цикл с меньшей частотой полного резервного копирования, например, 7 или 14 дней, что существенно снизит потребление ленты.
   * В случае с 7-дневным циклом используется 49,2 ГБ данных, что является оптимальным вариантом с точки зрения использования ленты.

### 26.1.6. Планирование времени и емкости

Важным аспектом при организации резервного копирования и восстановления данных является правильное планирование времени и емкости, так как оба эти процесса ограничены определёнными факторами.

#### Время и ограничения на скорость:

1. **Ограничения на скорость резервного копирования**:
   * Скорость резервного копирования ограничивается самым медленным звеном цепи, будь то скорость чтения с диска, скорость записи на резервный носитель (например, магнитную ленту), полоса пропускания сети или задержка между диском и носителем.
   * Часто производители приводов для магнитных лент указывают скорости и емкости, которые могут значительно отличаться от реальной производительности. В действительности, различие в скорости может быть настолько большим, что разница может составлять до 1500%.
   * Некоторые ошибки при проектировании резервного копирования, такие как "эффект чистки обуви" (когда привод вынужден перемещаться взад и вперёд по одной и той же области ленты), могут замедлить процесс записи.
2. **Ограничения на скорость восстановления**:
   * Восстановление данных также зависит от самого медленного компонента системы, однако на скорость восстановления влияет ещё ряд других факторов. Например, время восстановления может быть значительно затруднено из-за поиска нужного файла на ленте, если система не поддерживает быстрый доступ или перемотку.
   * Восстановление целого диска также может занять значительно больше времени, чем его резервное копирование. Это связано с тем, что скорость записи файловой системы обычно гораздо ниже скорости чтения, и восстановление часто происходит с меньшей эффективностью.

#### Управление временем и емкостью:

1. **Проблемы с производительностью**:
   * Быстродействие системы может существенно снизиться из-за перегрузки сети или из-за медленного поступления данных от сервера к устройству записи на ленту. Например, если сеть перегружена, скорость резервного копирования может быть ограничена пропускной способностью сети, а не характеристиками устройства хранения.
2. **Использование выделенных сетей**:
   * Для решения проблем с производительностью многие организации используют выделенные сети для резервного копирования, что позволяет изолировать трафик резервного копирования от основной сети. Одним из примеров такой сети является SAN (Storage Area Network), которая может значительно повысить эффективность резервного копирования.
3. **Использование буферов на дисках**:
   * Для улучшения производительности часто используется подход **диск-диск-лента (D2D2T)**. Суть заключается в том, что сначала данные копируются с серверов на диски узла резервного копирования, а затем уже с этих дисков на ленту. Это позволяет более эффективно использовать пропускную способность локальных дисков, а также ускорить процесс записи на ленту.
4. **Тестирование производительности**:
   * Чтобы точно определить, соответствуют ли ваши временные требования, необходимо проводить тестирование как для резервного копирования, так и для восстановления данных. Тестирование помогает подтвердить правильность выбранной структуры и выявить потенциальные проблемы.
   * С опытом можно научиться предсказывать, какие подходы будут наиболее эффективными, но учитывая, что системы резервного копирования и восстановления часто изменяются, полезным будет также опыт других людей, таких как консультанты или специалисты в области резервного копирования.

### 26.1.7. Планирование расходных материалов

При организации системы резервного копирования и восстановления данных важно не только правильно настроить процесс, но и планировать расходные материалы, такие как ленты и чистящие ленты. Неправильное планирование может привести к неожиданным расходам, поэтому важно заранее рассчитать потребности в материалах и их стоимость.

Вначале, когда ленты для перезаписи еще нет, потребуется закупка новых лент. Например, если ежедневно используется 8 лент (6 дней в неделю), то за 6 месяцев потребуется 1248 лент, что при цене $80 за штуку составит $99,840. В следующие 6 месяцев инкрементальные резервные копии можно будет перезаписать, и новые ленты понадобятся только для полных копий. Для полных копий потребуется 9 лент в неделю, а инкрементальные будут требовать на одну ленту больше. В таком случае за полгода потребуется 260 лент, что при сниженной стоимости $70 за штуку обойдется в $18,200.

Расходы на ленты за первый год составят $118,040, а за второй и третий годы — $36,400 в год. Общая сумма расходов за три года составит $190,840. Средние ежемесячные расходы на ленты за первые три года составят около $5301.

Через три года все ленты первого года (кроме архивных) можно будет перезаписать. Это снизит потребность в новых лентах, и в следующие годы потребуется закупать только 70–80 лент в год, что обойдется в $5–6 тыс. в год.

Если изменить политику хранения лент, например, хранить полные резервные копии только один год (кроме архивных), то расходы на ленты значительно сократятся. Во втором, третьем и четвертом годах ленты можно будет перезаписать, за исключением 72 лент для архивов. Это позволит уменьшить расходы на ленты, и общая сумма за три года составит около $129,240, а за четыре года — $134,840.

### 26.1.8. Вопросы процесса восстановления

Процесс восстановления данных требует внимательного планирования и учета различных факторов. Важно заранее сформировать ожидания пользователей, чтобы они понимали, как будет происходить процесс восстановления файлов и какие требования для этого существуют. Необходимо ясно обозначить, что резервное копирование выполняется только для данных на серверах и что файлы с локальных дисков не включаются в резервные копии. Также следует предоставить информацию о том, как пользователи могут запросить восстановление файла, включая контактные данные и инструкцию по отправке запроса.

Безопасность играет ключевую роль в процессе восстановления. Важно проверить, имеет ли человек, запрашивающий восстановление, право на доступ к данным. Восстановление должно происходить с учётом сохранения прав доступа и владельца файла, а также без перезаписи существующих данных, если это не предусмотрено. Восстановление данных в чужую директорию, особенно если она принадлежит сотруднику, не связанному с проектом, может создать угрозу безопасности.

По мере роста компании становится важнее иметь чётко установленную процедуру для проверки правомерности запросов на восстановление данных, поскольку в больших организациях сложно удостовериться в правомерности доступа к информации.

Кроме того, процесс восстановления должен быть хорошо документирован и доступен нескольким специалистам. Это позволит избежать зависимости от одного человека, который создал систему восстановления. Документация должна содержать инструкции для различных типов восстановления, от простого восстановления файлов до полного восстановления системы. Все эти процедуры должны быть обучены нескольким людям, а документация должна быть доступна как в сети, так и в печатном виде рядом с оборудованием для резервного копирования.

Для выполнения восстановления в случае поломки системы также важна контактная информация служб поддержки, номера контрактов и пароли для доступа к сервисному обслуживанию.

### 26.1.9. Автоматизация резервного копирования

Отсутствие автоматизации в процессе резервного копирования — это не только опасность, но и неоправданная неэффективность. Чем больше процессов автоматизируется, тем меньше вероятность человеческой ошибки, и тем более надежным становится выполнение резервного копирования. Без автоматизации задача по созданию резервных копий превращается в утомительную обязанность, и в случае ошибки невозможно будет дать удовлетворительный ответ на вопрос о причине отсутствия резервных копий.

Процесс резервного копирования можно автоматизировать в нескольких аспектах: выполнение команд, создание графиков и управление лентами, включая их инвентаризацию. Ранее все команды вводились вручную, а резервное копирование часто выполнялось в конце рабочего дня. Графики для копирования создавались вручную, а инвентаризация лент была минимальной. С развитием автоматизации появились скрипты, которые воспроизводили команды, вводимые вручную, но задача принятия решения о необходимости выполнения резервного копирования оставалась на усмотрение человека. Позже автоматизированные программы предложили динамические графики, которые значительно улучшили процесс. Автоматизированные системы также стали управлять физическим процессом работы с лентами, требуя от клерков замены определённого набора лент.

Хотя не везде требуется высокая степень автоматизации, хотя бы два уровня автоматизации должны быть внедрены в любой организации. Очень важно, чтобы системы, на которых резервное копирование выполняется вручную, особенно если они находятся за пределами корпоративного брандмауэра, также получили минимальную автоматизацию. Без автоматизации резервное копирование не будет выполняться.

Отсутствие автоматизации резервного копирования — это пустая трата ресурсов и времени. С автоматизацией ежедневная задача резервного копирования может быть выполнена менее квалифицированным сотрудником, что значительно дешевле. Даже если высокооплачиваемый системный администратор тратит час в день на замену лент, это расходует дорогостоящие ресурсы, которые могли бы быть использованы для более сложных задач. Это отражает принцип, почему руководители компании не тратят время на рутинные задачи, такие как отправка факсов, и передают их менее высокооплачиваемым сотрудникам.

Однако есть и худший вариант — плохая автоматизация. В этом случае автоматизируются многие аспекты задачи, но умственная нагрузка для решения проблем остается высокой. Хорошая автоматизация не только выполняет рутинную работу, но и сокращает умственные усилия, которые необходимы для выполнения задачи.

### 26.1.10. Централизация

Централизация — ключевая задача для создания эффективной системы резервного копирования. Это решение важно, потому что резервное копирование дорогое и критически значимое. Правильные инвестиции позволяют распределить стоимость системы по множеству систем, минимизируя затраты.

Централизация помогает снизить два основных типа расходов. Замену ленты можно считать дорогой процедурой, так как она требует трудозатрат и использования дорогого оборудования с высокоточными механическими элементами. Без централизации привод для ленты должен быть подключен к каждой машине, нуждающейся в резервном копировании, что влечет за собой значительные расходы на оборудование и физическую работу.

Сетевые системы резервного копирования позволяют подключить одно или несколько крупных устройств резервного копирования, которые могут взаимодействовать с различными узлами. Сетевое резервное копирование стало популярным после появления надежных и избыточных сетей. Приводы с автоматической заменой лент могут хранить большое количество лент и оснащены роботизированными манипуляторами, которые автоматически извлекают и помещают ленты в нужные блоки. Такие системы дорогие, но их стоимость делится между всеми подключенными системами, что значительно снижает расходы на трудозатраты. Эти устройства также обеспечивают автоматизацию многих процессов.

### 26.1.11. Инвентаризация лент

Без инвентаризации ленты с резервными копиями практически бесполезны. Инвентаризация критична для быстрого восстановления данных. В крупных автоматизированных системах резервного копирования инвентаризация обычно ведется в сети, и система обновляет индексы после каждого копирования. В некоторых случаях можно распечатывать минимальный указатель лент и хранить его в журнале.

Инвентаризация также может храниться в защищенных системах, например, RAID. Чем лучше инвентаризация, тем быстрее можно найти и восстановить нужные файлы. Без инвентаризации процесс восстановления потребует времени, поскольку необходимо будет читать ленты в хронологическом порядке или искать данные вручную. Если система хранит детальную опись по каждому файлу на лентах, поиск и восстановление могут быть выполнены гораздо быстрее с помощью запросов к базе данных. Например, если необходимо восстановить файлы из разных директорий, программа точно определит, в каких резервных копиях находятся нужные данные, и загрузит соответствующие ленты для восстановления.

Однако хранение детальной инвентаризации требует большого объема дискового пространства. Некоторые коммерческие решения находят баланс, поддерживая полную инвентаризацию для недавно использованных лент, а для старых лент — лишь простую инвентаризацию разделов. При необходимости восстановить более старые файлы полная инвентаризация может быть восстановлена по запросу.

Программа для резервного копирования должна уметь восстановить инвентаризацию в случае ее потери. Это должно быть реализовано так, чтобы можно было быстро перестроить инвентаризацию, загрузив последние ленты и автоматически создав новую. Хорошая инвентаризация также отслеживает количество перезаписей ленты, что важно, так как технологии хранения на лентах теряют надежность после определенного числа перезаписей. Программа должна уведомлять о необходимости уничтожения изношенных лент.

В экстренных ситуациях, когда доступ к инвентаризации невозможен, система должна обеспечивать возможность восстановления данных с лент без этой информации.

### 26.2. Тонкости

Теперь, когда мы рассмотрели основы надежной системы резервного копирования и восстановления, необходимо обратить внимание на тонкости, которые помогут эффективно поддерживать систему в будущем.

#### 26.2.1. Пробное восстановление

Пробное восстановление — это важная мера для проверки работы системы резервного копирования. Рекомендуется периодически выполнять восстановление всего диска, чтобы определить скорость восстановления и выявить узкие места. Это особенно важно, так как восстановление всего диска может занять значительно больше времени, чем восстановление отдельных файлов или директорий.

При пробном восстановлении следует отслеживать такие параметры, как использование диска, ленты и сети, чтобы выявить потенциальные проблемы в производительности. Если вы не видите ожидаемого быстродействия, можно проанализировать собранные данные для оптимизации системы.

Если свободного места для пробного восстановления нет, можно провести его при установке нового сервера, проверив его перед вводом в эксплуатацию. Важно также выполнять пробное восстановление с использованием как внутренних, так и внешних лент, если они хранятся вне основного местоположения.

Кроме того, проверку качества данных, полученных при пробном восстановлении, должен проводить не тот же человек, который отвечает за резервное копирование. Это обеспечивает сбалансированность и контроль в системе.

#### 26.2.2. Резервные носители и внешнее хранение

Ленты с резервными копиями необходимо хранить в безопасном месте. Хранение их в незапертой комнате или шкафу, несмотря на дорогие системы безопасности, бессмысленно. Резервные копии — это важные данные, которые должны быть надежно защищены.

Хранение резервных копий в серверной или в помещении, где может произойти затопление, также не является оптимальным решением. Для защиты от природных катастроф ленты должны храниться в другом, безопасном месте, которое не подвергается таким рискам.

Внешнее хранение резервных носителей является хорошей альтернативой. Оно позволяет хранить ленты на безопасном расстоянии от компьютеров, где они были созданы. Это может быть сделано не обязательно дорого и сложно. Ленты можно хранить в другом здании или у сторонних поставщиков услуг.

Однако нужно учитывать компромисс между удобством и риском. Хранение копий в другом месте снижает вероятность повреждения или утраты при транспортировке, но это может быть трудоемким процессом. Лучше всего хранить вне организации полные резервные копии за последний месяц, так как большинство восстановлений касается данных текущего месяца.

При выборе места для внешнего хранения следует учитывать безопасность, доступность и условия конфиденциальности. Множество вариантов хранения, от неофициальных систем до коммерческих служб, могут быть использованы в зависимости от ваших потребностей и бюджета.

### 26.2.3. Базы данных высокой доступности

Базы данных, как приложения с особыми требованиями, требуют особого подхода к резервному копированию. Эти данные часто управляются на уровне внутренней структуры базы, где размещение и доступ к данным могут быть недоступны для программ резервного копирования. Это означает, что база данных обычно записывается на ленту как единый файл. Однако если данные в этом файле изменяются в процессе записи, это может привести к повреждению данных, так как информация о размещении данных на ленте может быть неполной или некорректной. Чтобы избежать этого, базы данных часто нужно временно «закрывать», чтобы транзакции не происходили во время резервного копирования.

Для баз данных с высокими требованиями к доступности, отключение базы данных на ночь для резервного копирования является неприемлемым, так как это снижает их доступность. При этом важно минимизировать риски, связанные с отсутствием резервного копирования во время работы базы. Некоторые производители программного обеспечения предлагают модули для резервного копирования баз данных в активном состоянии, которые минимизируют риски, но идеальным вариантом остается выполнение резервного копирования, когда база данных не работает.

Один из распространенных методов — это «зеркальное отражение» базы данных, например, с использованием RAID 1 + 0. В таком случае база данных может быть временно остановлена для отключения зеркального раздела. Эти диски, которые не подвергаются транзакциям, могут быть безопасно записаны на ленту. После завершения копирования зеркальные диски снова подключаются к базе данных, и данные обновляются автоматически. В большинстве систем имеется три копии базы данных высокой доступности: одна активная, одна зеркальная, и еще одна — для резервного копирования.

### 26.2.4. Изменения технологий

Системы резервного копирования и восстановления постоянно эволюционируют, и нет одного универсального решения, которое подойдет на протяжении всей карьеры системного администратора. Вместо этого нужно ориентироваться на общие категории и следовать за развитием технологий.

Технологии хранения данных, такие как диски и ленты, постоянно развиваются, но с разной скоростью. В определенные моменты технология хранения на лентах будет лидировать, и вы будете уверены, что сможете создать резервные копии всех данных. В следующие годы диски будут занимать лидирующие позиции, и возникнут сомнения в том, можно ли успеть выполнить резервное копирование всех данных.

Размеры дисков увеличиваются постепенно: каждые несколько месяцев появляются более вместительные диски. Общий объем памяти удваивается каждые 15–18 месяцев, и приложения довольно быстро начинают использовать все доступное пространство, что приводит к необходимости резервного копирования дисков, содержащих вдвое больше данных каждый год.

Емкость лент росла более значительными шагами, но в течение нескольких лет. Поскольку потребители не так охотно модернизируют оборудование для резервного копирования на ленты, отрасль предлагает обновления с полной заменой оборудования каждые 2–3 года. Однако следует избегать частой модернизации, так как это может привести к необходимости работы с множеством разных форматов лент. Большинство компаний используют те технологии, которые были актуальными на момент установки системы, и часто имеют старые системы, которые еще не были модернизированы.

### 26.3. Заключение

Резервное копирование и восстановление данных являются основой для обеспечения безопасности и доступности информации в любой компании. Это критически важная часть политики управления информационными технологиями, которая помогает минимизировать риски потери данных.

**Типы запросов на восстановление:**  
Существует три основных типа запросов на восстановление данных:

1. **Случайное удаление файлов** — требует быстрого и точного восстановления.
2. **Восстановление после поломки дисков** — часто требует более сложного процесса восстановления, включая работу с резервными копиями.
3. **Просмотр архивных данных** — обычно относится к восстановлению данных из более старых резервных копий, что может иметь разные SLA и технические требования.

Каждый из этих запросов может требовать различных уровней обслуживания и отдельных решений для каждого типа данных или группы пользователей.

**Политика резервного копирования:**  
Создание четкой политики резервного копирования помогает устанавливать четкие правила для различных типов данных и служб. На основе этой политики строится график резервного копирования, где определяется, сколько времени должно пройти между инкрементальными резервными копиями и полными резервными копиями. Современные системы резервного копирования могут автоматически создавать динамические графики, что упрощает управление временем, ресурсами и затратами.

**Автоматизация процесса:**  
Для минимизации человеческих ошибок и затрат времени на ручную работу системы резервного копирования должны быть автоматизированы. Современные системы позволяют делегировать многие процессы — от планирования до восстановления — другим специалистам или программам, освобождая системных администраторов для более важных задач, таких как проектирование архитектуры и расширение инфраструктуры.

**Централизованные системы резервного копирования:**  
Централизованные решения для резервного копирования позволяют эффективно использовать ресурсы и снизить стоимость, обеспечивая более высокую масштабируемость и управляемость. В таких системах важную роль играют инвентаризационные системы, которые позволяют отслеживать как файлы, так и носители данных, что помогает эффективно управлять процессом восстановления и перезаписи лент.

**Экономические аспекты:**  
Системы резервного копирования требуют значительных затрат на оборудование и расходные материалы. Важно учитывать экономические подходы, которые могут снизить эти расходы, одновременно минимизируя риски. Администраторам необходимо быть готовыми к обновлению и расширению своих систем резервного копирования каждые 3-5 лет, чтобы оставаться в курсе изменений в технологиях.

**Тонкости и дополнительные меры:**  
После построения основной системы резервного копирования важно обратить внимание на такие моменты, как регулярные проверочные восстановления для убедительности в корректности работы системы. Также необходимо обеспечить безопасное внешнее хранение резервных носителей, чтобы защитить данные от потерь в случае катастрофы в основном офисе.

**Роль восстановления:**  
Восстановление данных — это одна из важнейших услуг для пользователей, и неспособность восстановить критически важную информацию может привести к серьезным последствиям для бизнеса. Однако успешное восстановление может сыграть ключевую роль в репутации системного администратора и всей компании, делая их надежными и заслуживающими доверия в глазах пользователей.