

ОСНОВНЫЕ МЕТОДЫ РЕЗЕРВНОГО КОПИРОВАНИЯ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Я.А. Чумбуридзе, магистрант
Волгоградский государственный университет
(Россия, г. Волгоград)

DOI:10.24412/2500-1000-2023-3-2-57-60

Аннотация. Резервное копирование – это одна из самых важных операций, которую необходимо производить для поддержания целостности данных. С помощью нее можно не только восстановить данные в случае аварийного отказа, но и создать резервную копию, которая может быть использована для восстановления, например, после хакерской атаки. В этой статье рассматриваются различные методы резервного копирования для защиты важных данных и предотвращения их потери.

Ключевые слова: резервное копирование, потеря данных, информационная безопасность, целостность.

В сегодняшнюю цифровую эпоху данные – это все. Будь то личные фотографии и документы или важная деловая информация, потеря важных данных может иметь разрушительные последствия [1]. Вот почему так важно иметь надежный метод резервного копирования. Разнообразные системы для резервного копирования информации являются одним из важнейших условий для обеспечения информационной безопасности. Наличие такой системы способствует устойчивому функционированию предприятия и предоставляет возможность быстрого восстановления данных при их потере по любой причине.

Ленточные накопители: существуют уже несколько десятилетий и когда-то были самым популярным методом резервного копирования. Они работают, записывая данные на магнитную ленту, которая затем сохраняется в автономном режиме. Хотя ленточные накопители относительно недороги и могут хранить большие объемы данных, у них есть некоторые недостатки. Во-первых, они могут быть медленными и громоздкими в использовании. Кроме того, если лента повреждена или потеряна, данные на ней могут быть потеряны навсегда.

Внешние жесткие диски: популярный метод резервного копирования для частных лиц и малых предприятий. Внешние жесткие диски относительно доступны по цене и просты в использовании, и на них

можно хранить большие объемы данных. Однако, как и ленточные накопители, они также могут быть потеряны или повреждены, а также уязвимы для вредоносных программ и вирусов.

Облачные решения для резервного копирования: облачные решения для резервного копирования в последние годы становятся все более популярными. Они работают путем резервного копирования данных на удаленные серверы через Интернет. Облачные решения для резервного копирования предлагают несколько преимуществ по сравнению с традиционными методами резервного копирования, включая легкий доступ, автоматическое резервное копирование и возможность увеличения или уменьшения масштаба по мере необходимости. Однако они требуют подключения к Интернету и могут быть более дорогими, чем другие методы резервного копирования.

Гибридные решения для резервного копирования: гибридные решения для резервного копирования сочетают в себе элементы как традиционных, так и облачных методов резервного копирования. Они работают путем резервного копирования данных как в локальные, так и в удаленные места. Гибридные решения для резервного копирования предлагают преимущества обоих методов, включая быстрое локальное резервное копирование и безопасное удаленное резервное копирование. Они

также могут быть более дорогими, чем другие методы резервного копирования, и требуют тщательной настройки для обеспечения правильной синхронизации резервных копий.

Резервное копирование может осуществляться несколькими способами:

1. Полное резервное копирование: технология, которая позволяет создавать

полные копии данных. При ее использовании можно однозначно восстановить любую выбранную ранее копию данных на любой момент времени, все файлы и папки создаются на диске для резервного копирования [2]. Создаётся полная копия. Все файлы и папки резервируются на диск, и могут быть восстановлены (рис. 1).

Полное резервное копирование



Рис. 1. Полное резервное копирование

Инкрементальное резервное копирование: процесс создания резервной копии данных, где старые данные сохраняются, а новые данные добавляются. При проведении инкрементального резервного копирования создаются несколько копий данных, а именно нулевая и инкрементные копии. Нулевая копия является полной копией

всех данных, а инкрементные копии содержат только изменения, внесенные после создания предыдущей копии [3]. Это означает, что последующие инкрементные копии будут содержать данные, которые были добавлены, изменены или удалены с момента создания предыдущей копии (рис. 2).

Инкрементальное резервное копирование

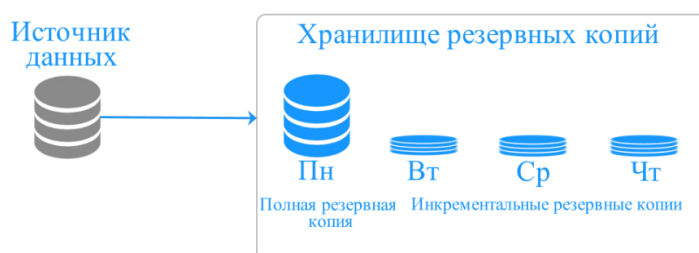


Рис. 2. Инкрементальное резервное копирование

Дифференциальное резервное копирование: использует разницу между двумя версиями данных. Первоначально создаётся полная копия, затем копируются изме-

нения. Затем при каждом дальнейшем резервном копировании будут копироваться только те изменения, которые вносились с последнего копирования [4] (рис. 3).

Дифференциальное резервное копирование

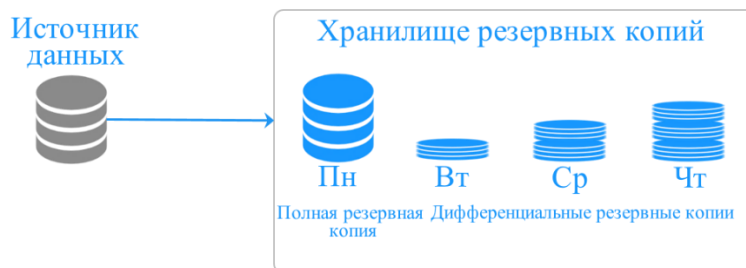


Рис. 3 Дифференциальное резервное копирование

Обратное инкрементальное резервное копирование работает аналогично инкрементальному с небольшим отличием: происходит меньше записей, а последняя запись является полной копией данных. Это означает, что при восстановлении

данных из резервной копии необходимо использовать только последнюю копию. Процесс обратного инкрементального бэкапа называется инкрементным откатом (рис. 4).

Обратное инкрементальное резервное копирование



Рис. 4. Обратное инкрементальное резервное копирование

Синтетическое резервное копирование: имеет много общего с типом обратного инкрементного резервного копирования. Синтетическое резервное копирование начинается с традиционного полного резервного копирования, за которым следует серия инкрементных резервных копий. В определенный момент инкрементные ре-

зервные копии объединяются и применяются к существующей полной резервной копии, чтобы синтезировать самую последнюю полную резервную копию в качестве новой отправной точки. Синтетическое резервное копирование собирается из полной резервной копии и последующих инкрементных резервных копий (рис. 5).

Синтетическое резервное копирование

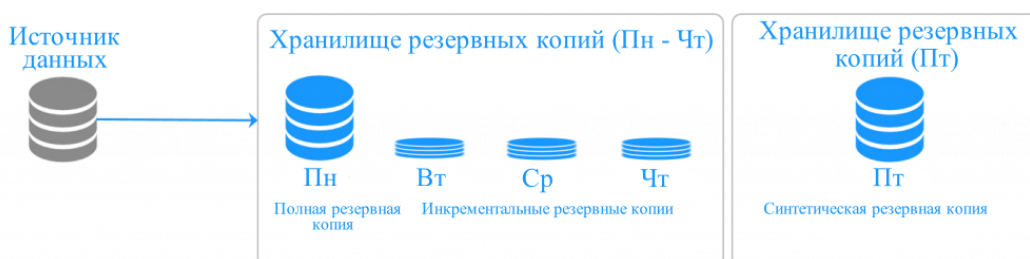


Рис. 5. Синтетическое резервное копирование

Советы по выбору правильного метода резервного копирования. При выборе метода резервного копирования необходимо учитывать несколько факторов. К ним относятся объем данных, которые необходимо резервировать, ваш бюджет и требуемый уровень безопасности. Кроме того, вы должны учитывать, как часто вам нужно создавать резервные копии ваших данных и нужен ли вам удаленный доступ к ним.

Заключение: выбор правильного метода резервного копирования имеет важное

значение для защиты ваших важных данных и предотвращения потери. Независимо от того, выбираете ли вы традиционный метод резервного копирования, такой как ленточные накопители или внешние жесткие диски, или облачное решение, важно убедиться, что ваша система резервного копирования надежна, безопасна и регулярно обслуживается. Потратив время на выбор правильного метода резервного копирования, вы можете быть уверены, что ваши данные в безопасности.

Библиографический список

1. Дегтярев, Д. И. Безопасная компиляция и архитектуры защищенных модулей / Д. И. Дегтярев, О. А. Какорина // Безопасность информационных систем и технологий в условиях цифровой экономики: Материалы IX Всероссийской научно-практической конференции с международным участием, Волгоград, 27-28 октября 2021 года / Редколлегия: О.А. Какорина, Ю.С. Бахрачева, Т.А. Попова. – Волгоград: Волгоградский государственный университет, 2021. – С. 23-26.
2. Бережной, А. Почему нельзя просто скопировать файлы. О резервном копировании, а также об инкрементальном парадоксе / А. Бережной // Системный администратор. – 2014. – № 7-8 (140-141). – С. 36-41.
3. Грибов В. В., Домбровский Е. М., Гришин С. А. Резервное копирование данных // Научная сессия ГУАП: гуманитарные науки. Сборник докладов традиционной Научной сессии, посвященной Всемирному дню авиации и космонавтики, 2020. – С. 147-149.
4. Борзыкин Д. В., Згерский Р. В., Семенов С. С. Технологии резервного копирования и хранения данных // Проблемы технического обеспечения войск в современных условиях. Сборник трудов конференции. – СПб.: ВАС, 2016. – С. 143-147.

BASIC BACKUP TECHNIQUES TO ENSURE INFORMATION SECURITY

Ya.A. Chumburidze, *Graduate Student*
Volgograd State University
(Russia, Volgograd)

Abstract. *Backup is one of the most important operations that must be performed to maintain data integrity. Using it, you can not only restore data in the event of a crash, but also create a backup copy that can be used to restore, for example, after a hacker attack. This article discusses various backup methods to protect important data and prevent data loss.*

Keywords: *backup, data loss, information security, integrity.*