

В современном мире объемы данных стремительно растут, а угрозы их потери из-за сбоев, кибератак или человеческих ошибок становятся все более серьезными. Особенно это актуально для организаций, работающих с конфиденциальной информацией. RED OS, как отечественная операционная система, обеспечивает высокий уровень безопасности и стабильности, что делает её идеальной платформой для реализации надежных стратегий резервного копирования. Разработка эффективных методов резервного копирования и восстановления данных на базе RED OS позволяет минимизировать риски потери информации и повысить отказоустойчивость IT-инфраструктуры.

Целью данной работы является разработка стратегии резервного копирования и восстановления данных для RED OS, а также создание методического пособия по её практическому применению. В рамках исследования были поставлены задачи по анализу теоретических основ, выбору оптимальных инструментов, настройке утилит и оценке их эффективности.

Резервное копирование — это процесс создания копий данных для их защиты от потерь и обеспечения возможности восстановления. [1] Основные методы резервного копирования включают: Полное копирование: создание полной копии всех данных. Обеспечивает высокую надежность, но требует значительных ресурсов. [2] Дифференциальное копирование: сохранение изменений относительно последней полной копии. Уменьшает объем хранимых данных, но требует больше времени для восстановления. [2] Инкрементальное копирование: копирование только измененных данных с момента последнего резервного копирования. Экономит место, но усложняет процесс восстановления. [2] Таким образом, мы рассмотрели основные методы резервного копирования. На рисунке представлены их сравнительные характеристики. (Рис. 1)



Рисунок 1 - Сравнительные характеристики методов

RED OS, как система, сертифицированная ФСТЭК России, обладает рядом особенностей, таких как поддержка российских криптоалгоритмов (ГОСТ) и интеграция с отечественным ПО. (Рис. 2)

Изображение выглядит как текст, снимок экрана, Шрифт, дизайн

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 2 – RED OS

Однако для неё характерны ограниченная совместимость с некоторыми сторонними инструментами и необходимость дополнительных настроек.

В ходе работы была установлена и настроена RED OS на виртуальной машине VirtualBox. (Рис. 3)

Изображение выглядит как текст, снимок экрана, веб-страница

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 3 - Подготовка образа RED OS в Virtual Box

Для реализации стратегии резервного копирования были выбраны и протестированы следующие утилиты: fwbackups: графическая утилита с поддержкой полного, инкрементального и дифференциального копирования. Проста в использовании, но не поддерживает шифрование. [3] Butterfly Backup: инструмент командной строки на основе rsync. Обеспечивает высокую производительность и поддержку шифрования. [3] Rescuezilla: утилита для создания образов системы и восстановления данных. Удобна для быстрого клонирования дисков. TestDisk: мощный инструмент для восстановления удаленных файлов и разделов. Незаменим в аварийных ситуациях.

Каждая утилита была протестирована на скорость восстановления данных и по итогам тестирования составлена сравнительная характеристика (Рис.4)

Изображение выглядит как текст, снимок экрана, Шрифт, число

Контент, сгенерированный ИИ, может содержать ошибки.

Рисунок 4 - Тестирование на скорость восстановление данных

Рекомендации по улучшению стратегии:

• для регулярного резервного копирования рекомендуется использовать утилиты, поддерживающие автоматизацию и шифрование, например, Butterfly Backup;

• для оперативного восстановления данных на уровне системы целесообразно применять Rescuezilla для создания и восстановления образов;

• в аварийных ситуациях оптимальным выбором будет TestDisk, особенно для восстановления поврежденных разделов и файлов;

• настройка мониторинга целостности резервных копий и проведение регулярного тестирования восстановления данных помогут минимизировать риски;

• стоит рассмотреть использование гибридных стратегий копирования, совмещающих локальное и облачное хранение данных, для повышения общей надежности системы.

Таким образом, для повышения эффективности стратегии резервного копирования рекомендуется использовать автоматизированные и безопасные утилиты, такие как Butterfly Backup, применять Rescuezilla для оперативного восстановления системы, а в экстренных случаях использовать TestDisk. Дополнительно важно настроить мониторинг целостности данных, регулярно тестировать восстановление и рассмотреть гибридные подходы с использованием локального и облачного хранения.

Разработанная стратегия была апробирована в ходе опроса среди студентов и преподавателей, который подтвердил её эффективность. Экономический расчет показал, что использование бесплатного образа RED OS и виртуализации позволяет минимизировать затраты. Общие расходы на реализацию проекта составили 206 183,89 рублей за первый месяц, включая аппаратное обеспечение, заработную плату администратора и прочие расходы.

В результате проведенного исследования была разработана стратегия резервного копирования и восстановления данных для RED OS, адаптированная под её особенности. Практическое тестирование утилит подтвердило их эффективность, а экономический анализ показал целесообразность внедрения предложенного решения. Разработанное методическое пособие упростит использование инструментов резервного копирования и повысит надежность информационных систем на базе RED OS.

**Литература:**

**1. Негус К. “Библия Linux. 10-е изд.” 2022. — 928с.**

**2. Официальный сайт «Киберпротект» [Электронный ресурс] Методы резервного копирования https://cyberprotect.ru/blog/backup-methods (дата обращения: 17.10.2024 г.).**

**3. Касторский А.Д. “Восстановление данных со всех носителей. Диагностика. Восстановление файлов. Резервное копирование. Восстановление системы” 2022. — 384с.**

**4. Официальный сайт RED OS. [Электронный ресурс] https://redos.red-soft.ru/?ysclid=m3nvl57vpa846158518 (дата обращения: 18.12.2024 г.).**

**5. Документация RED OS. [Электронный ресурс] https://redos.red-soft.ru/product/docs/ (дата обращения: 04.10.2024 г.).**