

Резервное копирование информации



Дата создания: 2021/12/19 07:44 (C) mihanik



Лирическое отступление.

Давно занимаюсь сопровождением информационных систем различных предприятий, давно сталкиваюсь с разными ситуациями, когда по разным причинам «рабочая информация» бывает повреждена настолько, что становится невозможным её использование. Соответственно, приходилось прибегать к восстановлению информации из резервной копии. Неоднократно.

Сразу скажу, что за более чем 20 (двадцать!) лет работы мной не было потеряно **НИ ОДНОЙ БАЗЫ ДАННЫХ** моих клиентов.

Соответственно, хочу описать основные принципы создания резервных копий, а также требования к организации резервного копирования.



Системные администраторы делятся на тех кто не делает резервных копий, и тех, кто уже их делает.

Типы резервных копий

Для себя я выделяю два вида резервных копий: «горячая копия», «холодная копия».

К каждому типу резервной копии у меня свои требования.

"Горяча копия"

Требования к резервной копии горячего типа:

- Создаётся так часто, как этого требует бизнес.
- Позволяет «откатиться» за минимальное количество времени (от нескольких минут до часа).
- Расположена на быстрых носителях и «близко» к «месту использования».

Пояснения.

Создаётся так часто, как этого требует бизнес.

Пояснений не требует.

Позволяет уверенно "откатиться" на нужную дату.

Система резервного копирования должна обеспечивать **консистентность** резервной копии, и, в случае её повреждения, возможность автоматизированной её «починки». Другими словами, мы должны быть уверены в том, что холодная резервная копия **НЕ ПОВРЕЖДЕНА**.



Это не освобождает нас от регулярного проведения тестового восстановления информации из резервной копии с последующей проверкой на корректность/работоспособность

Расположена **НЕ** на том же сервере, где используется информация.

Тут всё просто. Это на тот случай, если в «основной» сервер попадёт «ядрёная бомба», сгорит материнская плата или «стуканут» диски локального файлового хранилища.

При создании копии используются **НЕСТАНДАРТНЫЕ** протоколы, которые операционная система не поддерживает нативно.

Например, если вы используете ОС Windows, то лучше использовать протоколы FTP, SSH и прочие.

Это сделает невозможным повреждение резервной копии **вирусом-шифрователем** и **ЗНАЧИТЕЛЬНО ЗАТРУДНИТ** ручное повреждение информации злоумышленником в случае его несанкционированного проникновения на сервер.



Однако! Не стоит забывать, что логины и пароли от таких «нестандартных подключений» следует хранить в полной тайне.

Как это обычно делаю я.

Горячую копию я делаю при помощи простейших операций.

- Выгрузка базы 1С в DT-файл.
- Создание резервных копий СУБД встроенными средствами.

