Лекция 9

Технологии защиты данных, резервного копирования и восстановления

6B06201 - Радиотехника, электроника и телекоммуникации

А.А. Хохлов • Алматы, 2026

Цель лекции

- Сформировать системное представление о технологиях обеспечения сохранности, целостности и восстановления данных в корпоративных системах хранения.
- Изучить основные причины потери и повреждения информации, принципы организации резервного копирования и показатели допустимой потери данных и времени восстановления RPO и RTO.
- Рассмотреть механизмы моментальных снимков Snapshot, технологии HyperSnap, полного клонирования HyperClone и непрерывной защиты данных HyperCDP, а также особенности создания согласованных точек восстановления.
- Изучить принципы неизменяемого хранения WORM/HyperLock, защиты резервных копий от несанкционированного изменения и удаления.
- Сформировать понимание организации аварийного восстановления, выбора соответствующих технологий защиты и проверки работоспособности восстановленных информационных сервисов.

Результаты обучения

По завершении лекции обучающийся сможет:

- Объяснять назначение резервного копирования, показатели RPO и RTO и основные принципы восстановления данных.
- Сравнивать технологии HyperSnap, HyperClone, HyperCDP и WORM по механизмам работы и областям применения.
- Выбирать подходящие способы защиты информации и описывать последовательность восстановления данных при различных аварийных ситуациях.

Почему защита данных - комплексная задача

Физические отказы

Накопители, контроллеры, сеть, питание и площадка.

Логические ошибки

Удаление файлов, сбои приложения, повреждение базы.

Злонамеренные действия

Шифровальщики, компрометация прав, удаление копий.

Доступность оборудования ≠ возможность восстановления любой версии данных

Защита данных: четыре взаимодополняющих механизма

Отказоустойчивость

RAID, резервные пути и контроллеры

Snapshot

Быстрая локальная точка состояния

Клон / CDP

Изолированная рабочая копия / частые точки

Backup

Независимая копия для аварийного восстановления

Ни один механизм не заменяет все остальные.

Цели восстановления: RPO и RTO

Две независимые характеристики устойчивости бизнес-сервиса



RPO - допустимая потеря изменений

RTO - допустимое время простоя

Пример

База данных и архив могут иметь разные нормативы восстановления.

Резервное копирование: независимое восстановление



- Полные и инкрементальные копии выбираются по профилю изменений.
- Проверяют не только выполнение задания, но и читаемость копии.
- Нужны отдельные учётные данные и тестовое восстановление.

Snapshot и HyperSnap: состояние на момент времени



Redirect-on-Write

Изменённый блок размещается в новом месте; снимок сохраняет ссылку на прежнюю версию.

Ограничение

Локальный снимок обычно зависит от исходного массива и метаданных.

Практика работы со снимками

Создание

Вручную или по расписанию; контроль количества версий.

Использование

Просмотр, анализ и оперативное восстановление.

Откат

Возврат к точке t_0 может отменить последующие изменения.

Для нескольких зависимых томов необходима согласованная точка состояния приложения.

HyperClone: независимый экземпляр данных



Применение

Тестирование обновлений, анализ производственных данных, восстановление повреждённого тома.

Важно

Клон в том же массиве имеет общие инфраструктурные риски с оригиналом.

CDP и HyperCDP: частые точки защиты

Преимущество

Снижение возможной потери изменений благодаря близким точкам восстановления.

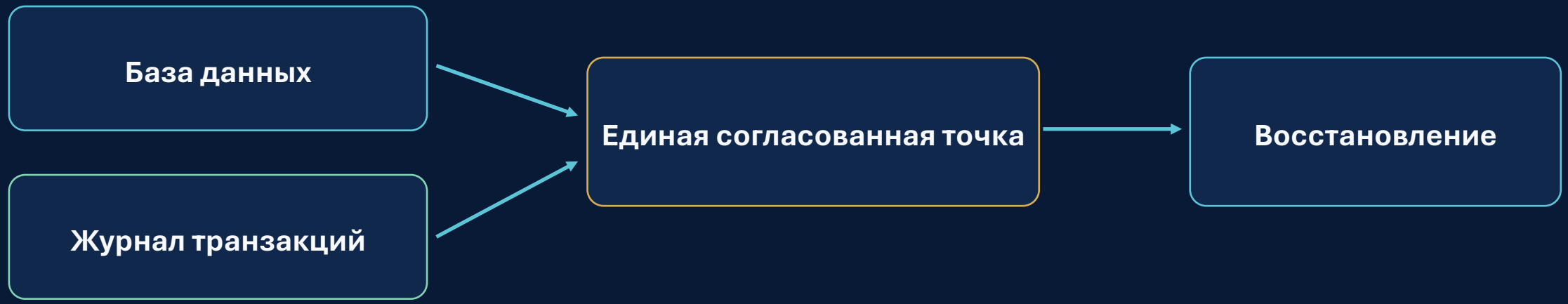
Ограничение

Реальная детализация определяется политикой, продуктом и доступной ёмкостью.



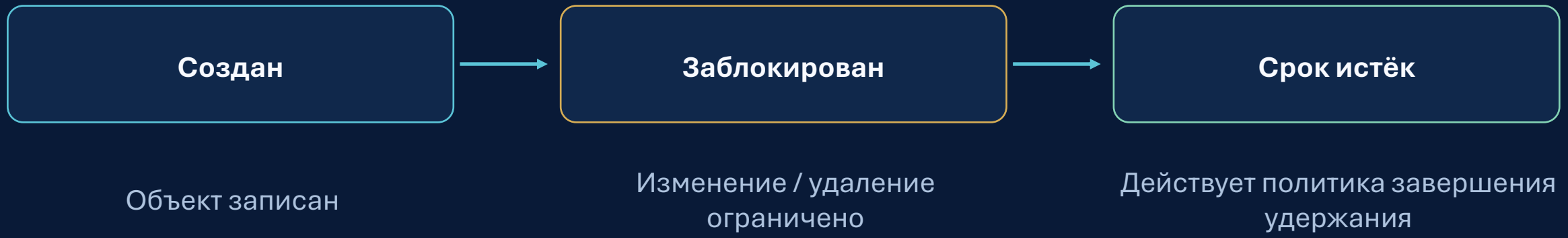
Частые точки требуют контроля объёма изменённых данных и свободного места.

Группы согласованности и управление версиями



Несовпадение времени снимков связанных LUN может сделать базу логически несогласованной.

WORM и HyperLock: защита от изменений



Часы соответствия помогают предотвращать обход срока удержания изменением системного времени.

Защита копий от преднамеренного удаления

Разделение полномочий

Отдельные административные роли и минимальные права.

Изолированная копия

Другой домен управления или физическое отделение.

Неизменяемость

Политики удержания для резервных данных.

Проверка восстановления

Регулярное тестирование целостности и пригодности копий.

Аварийное восстановление: выбор механизма

Удалён один документ	→ Snapshot / версия файла
Повреждён том	→ Клон либо backup
Утрачен основной массив	→ Независимая копия на другом оборудовании

После возврата сервиса проверяют целостность, права, зависимости и фактические RPO/RTO.

Итоги и контрольные вопросы

- Доступность СХД и восстановимость данных - разные характеристики.
- HyperSnap обеспечивает точки времени; HyperClone создаёт рабочую копию.
- HyperCDP уменьшает интервал между защищёнными состояниями.
- WORM защищает от изменения, но не заменяет независимые копии.
- Тест восстановления подтверждает работоспособность всей стратегии.

Вопрос: как выбрать защиту для базы данных, файлового ресурса и архива?