?????????? ??.

???? ? ?????????????

- Доступ к БД только через приватную сеть или VPN
- Firewall: открыт только порт СУБД
- БД не должна быть напрямую в интернете

????? ? ??

- Права доступа на уровне ОС для файлов БД
- Регулярные обновления безопасности ОС
- Шифрование диска (LUKS/BitLocker/TPM) для защиты данных «на физическом носителе»

???????????? ? ???????

- Принцип минимальных прав (Least Privilege)
- Только нужные права: SELECT / INSERT / UPDATE / DELETE
- Не использовать root / postgres в приложениях
- Не хранить пароли в коде

????? ? ???????????

- Аудит: кто, когда, что делал, с какими объектами
- Логирование: подключения, ошибки, подозрительная активность
- Профайлер / планы запросов: выявление тяжёлых запросов → предотвращение DoS или неправильного доступа

SQL-????????

- П араметризованные запросы / prepared statements

??????

- Цель: ошибки пользователей, сбои, атаки
- Типы бэкапов:
  1. Полный — вся база
  2. Инкрементальный — изменения с последнего бэкапа
  3. Дифференциальный — изменения с последнего полного бэкапа
- Методы:
  - SQL-дампы — перенос структуры и данных
  - Файловый — точная копия файлов
  - Стриминг (WAL) — откат к любому моменту времени
  - Практика: хранить отдельно, шифровать, проверять восстановление

??????

- Разделение сред: dev / stage / prod
- 2FA для админов
- Отключить пользователей и базы по умолчанию
- Отключить анонимные подключения
- SSL / TLS: шифрование трафика (пароли и PII)

> Безопасность БД = сеть + доступы + шифрование + аудит + бэкапы + защита данных + ограничения ресурсов

Revision #1
Created 2026-01-15 15:46:45 UTC by Fedmog1lnkv
Updated 2026-01-17 02:00:13 UTC by Fedmog1lnkv