# ОСНОВНЫЕ НАПРАЛЕНИЯ АДМИНИСТРИРОВАНИЯ БАЗ ДАННЫХ И СЕРВЕРОВ

Соадминистрирование баз данных и серверов— это процесс управления и обслуживания баз данных и серверов в организации для обеспечения их бесперебойной работы, безопасности и производительности.

## Технические проблемы, возникающие в процессе эксплуатации баз данных

Этот пункт охватывает широкий спектр проблем, которые могут возникнуть в процессе работы с базами данных (БД). Важно понимать, что стабильность и надежность БД критически важны для многих бизнес-процессов. Вот некоторые примеры технических проблем:

Проблемы с производительностью:

* Медленные запросы: Запросы, которые выполняются слишком долго, могут быть вызваны неоптимизированными запросами, отсутствующими индексами, блокировками, недостаточными ресурсами сервера (CPU, RAM, дисковый ввод-вывод) или проблемами с сетевым подключением.
* Высокая загрузка CPU/RAM: Перегрузка сервера, на котором работает БД, может привести к замедлению работы и даже к сбоям. Это может быть вызвано большим количеством одновременных запросов, ресурсоемкими операциями или проблемами в коде приложения, обращающегося к БД.
* Проблемы с дисковым пространством: Недостаток свободного места на дисках, где хранятся данные и журналы БД, может привести к невозможности записи данных и остановке работы БД.
* Несогласованность данных: Неправильная работа транзакций или блокировок может привести к тому, что данные в разных таблицах БД будут противоречить друг другу.

Проблемы с доступностью:

* Сбои сервера: Аппаратные или программные сбои сервера, на котором работает БД, могут привести к недоступности БД для пользователей.
* Проблемы с сетью: Проблемы с сетевым подключением между клиентами и сервером БД могут привести к недоступности БД.
* Ошибки в конфигурации БД: Неправильная настройка параметров БД может привести к ее нестабильной работе и недоступности.

Проблемы с резервным копированием и восстановлением:

* Некорректные резервные копии: Если резервные копии БД создаются неправильно или не проверяются на работоспособность, то в случае сбоя восстановление данных может быть невозможным.
* Медленное восстановление: Процесс восстановления БД из резервной копии может занимать много времени, что приводит к длительному простою системы.

## Администрирование отдельных компонентов серверов

Ключевые компоненты и задачи администрирования включают:

Операционная система (ОС):

* Установка и настройка ОС: Выбор подходящей ОС (Windows Server, Linux и т.д.) и ее настройка для оптимальной работы с БД.
* Обновление и патчи безопасности: Регулярная установка обновлений ОС и патчей безопасности для защиты от уязвимостей.
* Управление пользователями и группами: Создание и управление учетными записями пользователей и групп, назначение прав доступа к ресурсам сервера.
* Мониторинг ресурсов ОС: Отслеживание загрузки CPU, RAM, дискового пространства и других ресурсов ОС для выявления проблем и оптимизации производительности.

Сетевые службы:

* Настройка сети: Настройка IP-адресов, DNS, маршрутизации и других сетевых параметров.
* Брандмауэр: Настройка брандмауэра для защиты сервера от несанкционированного доступа.
* Мониторинг сетевого трафика: Отслеживание сетевого трафика для выявления аномалий и проблем с сетью.

Система хранения данных:

* Настройка дисковых массивов (RAID): Настройка RAID-массивов для обеспечения отказоустойчивости и повышения производительности дисковой подсистемы.
* Управление дисковым пространством: Мониторинг и управление дисковым пространством, выделение места для БД и журналов.
* Оптимизация ввода-вывода: Настройка параметров дисковой подсистемы для оптимизации скорости чтения и записи данных.

Программное обеспечение сервера БД (СУБД):

* Установка и настройка СУБД: Установка и настройка СУБД (MySQL, PostgreSQL, Oracle, SQL Server и т.д.) в соответствии с требованиями приложения.
* Управление пользователями и правами доступа в СУБД: Создание и управление учетными записями пользователей и назначение прав доступа к базам данных и таблицам.
* Мониторинг производительности СУБД: Отслеживание производительности СУБД, выявление медленных запросов и проблем с блокировками.
* Настройка резервного копирования и восстановления СУБД: Настройка автоматического резервного копирования БД и процедур восстановления данных в случае сбоя.

## Требования, предъявляемые к конфигурации локальных компьютерных сетей и серверного оборудования

Требования к локальной сети (LAN):

* Пропускная способность: Сеть должна обеспечивать достаточную пропускную способность для передачи данных между клиентами и сервером БД. Необходимо учитывать пиковые нагрузки и потенциальный рост трафика.
* Задержка (Latency): Задержка в сети должна быть минимальной, особенно для критически важных приложений, работающих с БД. Высокая задержка может привести к замедлению работы приложений.
* Надежность: Сеть должна быть надежной и отказоустойчивой, чтобы обеспечить постоянный доступ к БД. Необходимо использовать резервные каналы связи и оборудование.
* Безопасность: Сеть должна быть защищена от несанкционированного доступа и сетевых атак. Необходимо использовать брандмауэры, системы обнаружения вторжений (IDS) и другие средства защиты.

Требования к серверному оборудованию:

* Процессор (CPU): Сервер должен быть оснащен мощным процессором, способным обрабатывать большое количество запросов к БД. Количество ядер и тактовая частота процессора должны соответствовать требованиям СУБД и приложения.
* Оперативная память (RAM): Сервер должен иметь достаточно оперативной памяти для хранения данных, индексов и кешей СУБД. Недостаток RAM может привести к замедлению работы БД и использованию дискового пространства для подкачки данных (swap).
* Дисковая подсистема: Дисковая подсистема должна обеспечивать высокую скорость чтения и записи данных. Рекомендуется использовать быстрые SSD-накопители или RAID-массивы для повышения производительности и отказоустойчивости.
* Сетевая карта (NIC): Сервер должен быть оснащен сетевой картой с высокой пропускной способностью (например, 10 Gbps) для обеспечения быстрой передачи данных по сети.
* Охлаждение: Система охлаждения сервера должна обеспечивать поддержание оптимальной температуры компонентов для предотвращения перегрева и сбоев.

## Аудит систем безопасности БД и серверов

Аудит БД:

* Аудит прав доступа: Проверка прав доступа пользователей и ролей к базам данных, таблицам и другим объектам БД. Убедиться, что у пользователей есть только необходимые права для выполнения своих задач.
* Аудит конфигурации СУБД: Проверка настроек СУБД на предмет соответствия рекомендациям по безопасности. Например, проверка парольной политики, настроек аудита, шифрования и других параметров.
* Аудит резервного копирования и восстановления: Проверка процедур резервного копирования и восстановления БД на предмет их работоспособности и соответствия требованиям по времени восстановления (RTO) и точке восстановления (RPO).

Аудит серверов:

* Аудит ОС: Проверка конфигурации ОС на предмет соответствия стандартам безопасности. Например, проверка парольной политики, настроек брандмауэра, аудита, обновлений безопасности и других параметров.
* Аудит сетевых служб: Проверка конфигурации сетевых служб (например, SSH, RDP, HTTP) на предмет соответствия рекомендациям по безопасности.
* Аудит физической безопасности: Проверка физической безопасности серверов, например, контроль доступа в серверную комнату, наличие систем видеонаблюдения и пожарной сигнализации.
* Аудит управления уязвимостями: Проверка наличия процессов сканирования уязвимостей и установки патчей безопасности.

## Регламенты по защите информации баз данных

Общие положения:

* Цель и область применения: Определение цели и области применения регламента, указание на то, какие базы данных и системы он охватывает.
* Определения и термины: Определение используемых терминов и сокращений.
* Ответственность: Определение ответственных лиц за выполнение требований регламента (например, администраторы БД, администраторы серверов, специалисты по безопасности).

Политика доступа:

* Принципы минимальных привилегий: Предоставление пользователям только тех прав доступа, которые необходимы для выполнения их задач.
* Процедура предоставления и отзыва прав доступа: Описание процедуры запроса, утверждения и предоставления прав доступа к БД.
* Регулярный пересмотр прав доступа: Проведение регулярного пересмотра прав доступа пользователей для выявления и устранения избыточных прав.
* Использование ролей: Использование ролей для упрощения управления правами доступа и обеспечения единообразия.

Аудит и мониторинг:

* Настройка аудита СУБД: Определение событий, которые должны быть зафиксированы в журналах аудита.
* Мониторинг журналов аудита: Регулярный мониторинг журналов аудита для выявления подозрительной активности.
* Реагирование на инциденты безопасности: Описание процедуры реагирования на инциденты безопасности, такие как несанкционированный доступ, попытки взлома и т.д.

Резервное копирование и восстановление:

* Периодичность резервного копирования: Определение периодичности создания резервных копий БД.
* Типы резервных копий: Определение типов резервных копий (полные, инкрементные, дифференциальные).
* Место хранения резервных копий: Определение безопасного места хранения резервных копий.
* Процедура восстановления: Описание процедуры восстановления БД из резервной копии.

Шифрование данных:

* Шифрование данных при хранении: Использование шифрования данных на дисках для защиты от несанкционированного доступа в случае физической кражи или компрометации носителей.
* Шифрование данных при передаче: Использование шифрования данных при передаче по сети (например, SSL/TLS) для защиты от перехвата трафика.