

Отказоустойчивость

1. **Отказ информационной системы:** поведение информационной системы, не удовлетворяющее ее спецификации.
2. **Отказы:**
 - проходные отказы - однократные;
 - перемежающиеся отказы - появляются, пропадают и снова появляются с непредсказуемой периодичностью;
 - постоянные отказы - появился и существует, пока не исправят.
3. **Ошибка информационной системы:** состояние информационной системы, которое может привести к отказу.
4. **Маскирование ошибок:** сокрытие ошибок в процессе от других процессов распределенной системы. Основным методом - применение избыточности: информационная избыточность, временная избыточность, физическая избыточность.
5. **Маскирование ошибок информационной избыточностью:** помехоустойчивое кодирование данных.
6. **Маскирование ошибок временной избыточностью:** повторение действия в случае ошибки.
7. **Маскирование ошибок физической избыточностью:** резервирование элементов системы (резервирование в авиации, кластеры - резервирование в информационных системах).
8. **Особенности отказа распределенной системы:** отказ в распределенной системе может быть частичным, отдельные ее компоненты могут утратить свою работоспособность, в то время, как другие могут полностью сохранить свою функциональность.
9. **Типы отказов в распределенной системе:**
 - поломка - сервер перестал работать; остановка сервера; зависание ОС, требующее перезагрузки;

- пропуск данных - сервер неправильно реагирует на входные запросы (например, переполнение буферов соединений или данных, превышение timeout и пр.);
- ошибка синхронизации - реакция сервера происходит не в определенный интервал времени (например, на сервере взаимная блокировка процессов);
- ошибка отклика - в ответе сервера ошибка;
- произвольная ошибка сервера - сервер отправляет непредсказуемые сообщения в непредсказуемые моменты времени;

10. **Отказоустойчивость информационной системы:** свойство технической системы сохранять свою работоспособность после отказа одного или нескольких составных компонентов.

11. **Надежность информационной системы:**

- доступность (availability);
- безотказность (reliability);
- безопасность (safety);
- ремонтпригодность (maintainability).

12. **Доступность:** свойство системы находится в состоянии готовности к работе. Система с высокой степенью доступности - это система, которая в произвольный момент времени, вероятнее всего, находится в работоспособном состоянии.

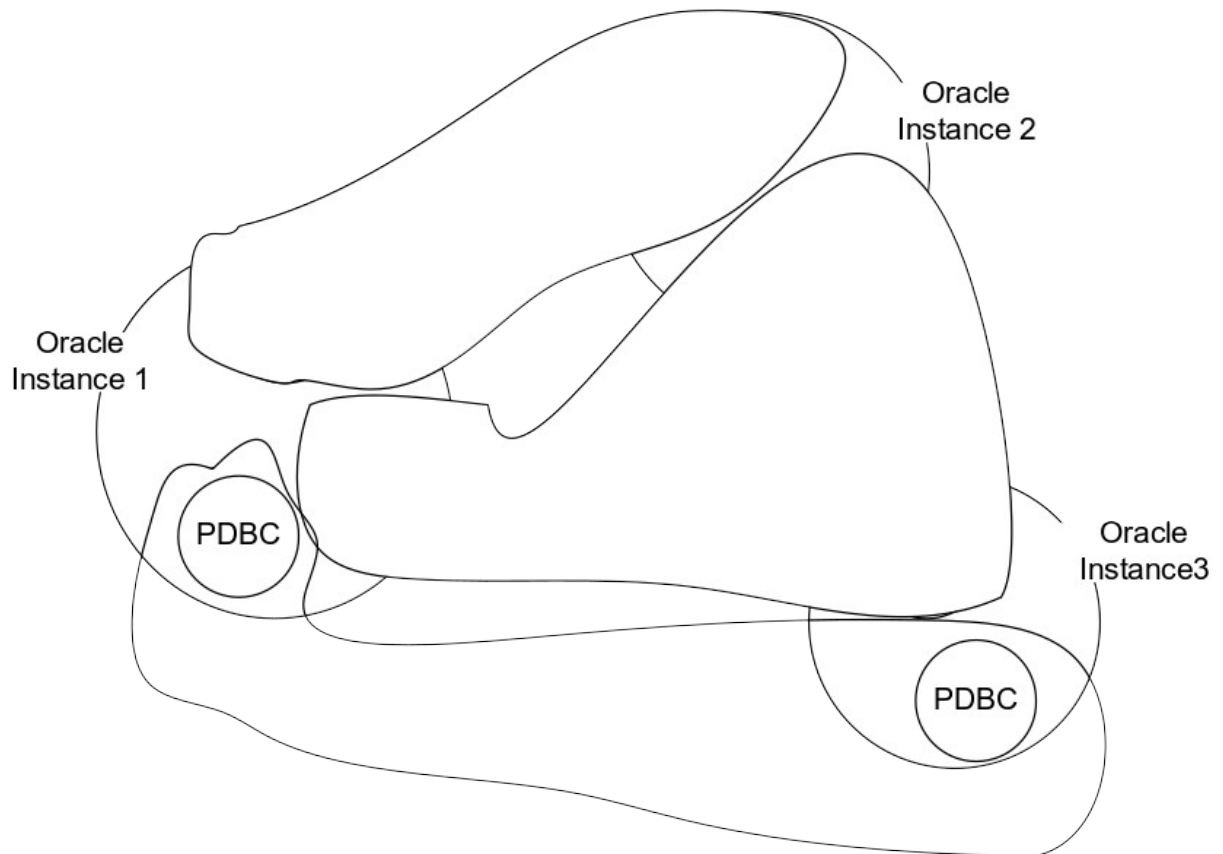
13. **Безотказность:** свойство системы длительное время работать без отказов. Системы с высокой безотказностью - это системы, которая вероятнее всего, будет непрерывно работать в течении относительно (зависит от системы, авиационные пушки живут 3-4 секунды) долгого времени. Система может иметь высокую безотказность, но низкую доступность (снабжение горячей водой, редко отказывает, но отключают на длительное время на ремонт).

14. **Безопасность:** свойство системы, определяющее последствие отказа (отказ авиационной техники, отказ почтового сервера общего назначения).

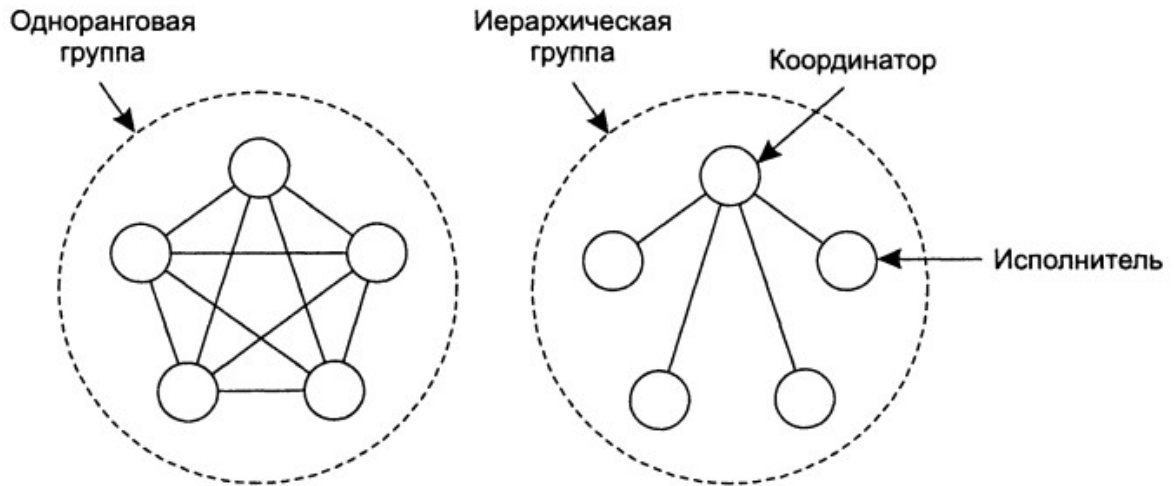
15. **Ремонтпригодность:** свойство системы, определяющее сложность (продолжительность) восстановления работоспособности системы. Большинство отказов -

монотонные процессы. Системы с обслуживанием по состоянию, системы с обслуживанием по регламенту.

16. **Отказоустойчивость процессов:** достигается объединением нескольких идентичных процессов в группу (кластер). Сообщение получают все члены группы, если один из процессов перестает работать, то его место занимает другой. Группы могут быть динамическими и статическими, один и тот же процесс может входить в несколько групп одновременно.



17. **Отказоустойчивость процессов: группы процессов** – одноранговые, иерархические. В иерархических группах присутствует координатор распределяющий запросы (во многих системах называется балансировщиком), в случае отказа координатора – выбирается другой координатор из исполнителей.



18. **Отказоустойчивость процессов: группы процессов:** при централизованном управлении группами, требуется специальный сервер – сервер групп, следящий за членством процессов входящих в группы. Такой подход прост в реализации, но уменьшает надежность – отказ сервера групп, приведет к отказу всей группы.
19. **Отказоустойчивость процессов: группы процессов:** при распределенном управлении, все процессы хранят список членов группы; требуется надежная групповая рассылка (широкополосная); процесс извещает все процессы группы о своем желании вступить в группу или покинуть ее; нужен механизм позволяющий определить аварийный отказ одного из членов группы (постоянный опрос друг друга); при включении в группу необходим механизм синхронизации (реплицирования) нового члена группы с другими членами (пример, grid Oracle).
20. **Отказоустойчивость процессов: группы процессов:** группа процессов позволяет замаскировать отказы одного или более процессов; другими словами можно реплицировать процессы, заменяя одиночный процесс **отказоустойчивой группой (failover group/cluster** – понятие в Microsoft, в Oracle и др.)
21. **Отказоустойчивость процессов: группы процессов:** соглашения в системах с ошибками; процесс посылающий, какое-то уведомление другому процессу не знает точно

дошло ли сообщение до адресата; при подтверждении получения запроса, не ясно дошло ли подтверждение, ..., дошло ли подтверждение на подтверждение; требуется специальные протоколы.