Безопасность и аудит

Для безопасности хранилища нужно организовать ролевую модель.

Транснациональная передача данных

152 ФЗ — Хранение и передача персональных данных

Группировать можно не только пользователей, но и привилегии;

Группа привилегий — роль;

Роль можно назначать другой роли (многоуровневая структура);

Циклические роли создать нельзя;

В Oracle, в отличие от Postgres, под каждого пользователя создаётся своя схема, в которую он может писать, т. е. в БД нельзя просто „сходить почитать";

Мандатная модель: объекты наследуют метки пользователей (субъектов), создавших их;

Мандаты до сих пор исп. в ОС в файловых системах;

SE Linux – расширение Postgres

Атрибутивная (характерна для модели звёздочки) модель упр-я доступом относительно легко автоматизируются; (распр-е ролей)

Политику можно один раз выработать и переносить из компании в компанию; (наследование)

В хранилище нельзя делать DELETE!

А в приложении всё по-другому организуется;

Также важна архитектура приложения (монолит/микросервисы);

В данном контексте политика – набор нормативных правил
- атрибутивная модель упр-я доступом