

Курс «Базы данных»

Тема. Управление ролями

Барабанщиков
Игорь Витальевич

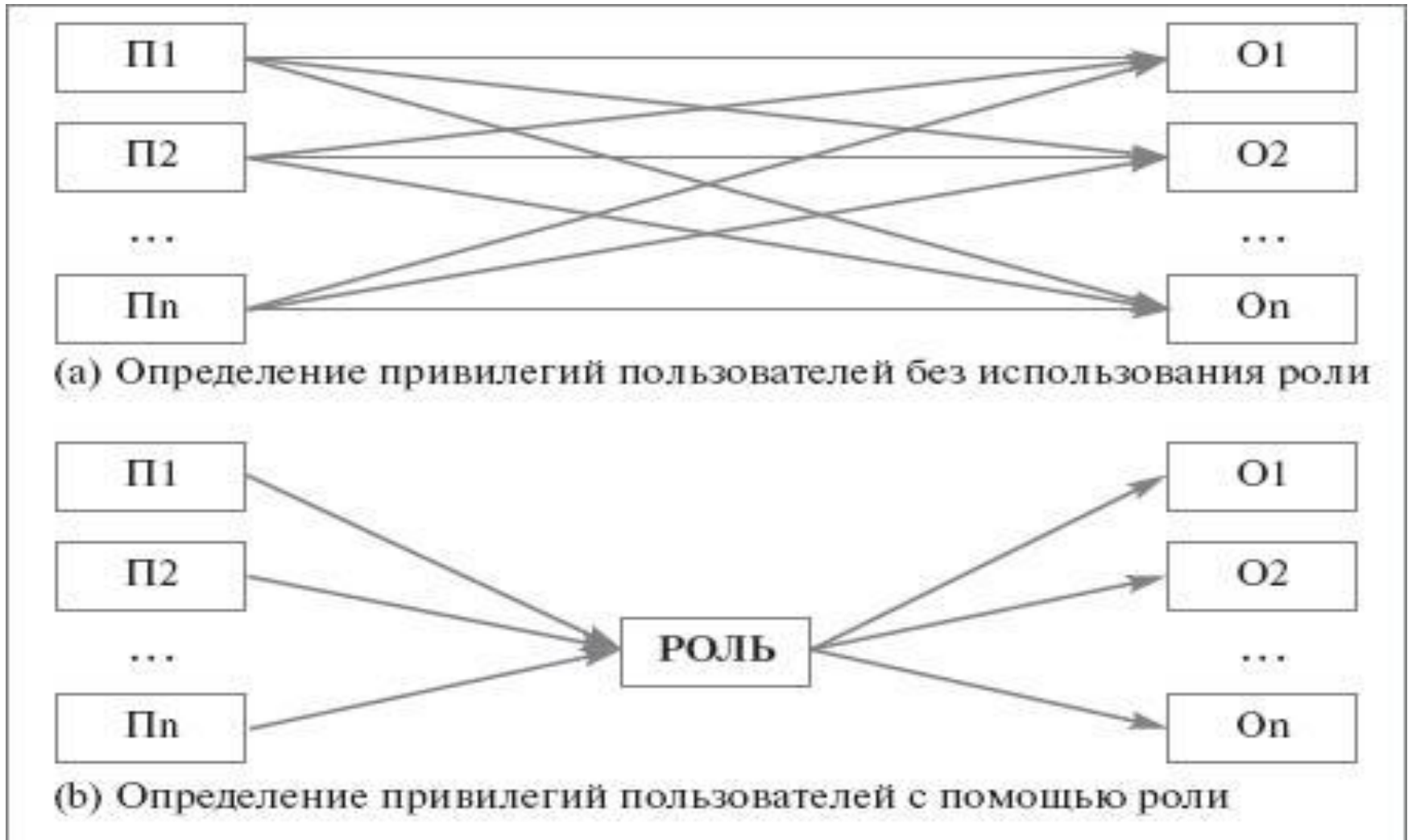
План лекции

- Проблемы сопровождения привилегий.
- Использование ролей для упрощения сопровождения модели безопасности БД.
- Предоставление привилегий ролям.
- Проверка привилегий, доступных ролям.

Проблема сопровождения привилегий

- Когда в БД много пользователей и много привилегий, которые надо им выдавать, то **задача сопровождения привилегий становится слишком сложной.**
- Эту задачу можно существенно упростить, если использовать **механизм ролей.**

Упрощение сопровождения привилегий



Роль

- **Роль** - это именованная совокупность *взаимосвязанных* привилегий, которые могут быть предоставлены пользователю.
- Роли *упрощают* предоставление и сопровождение привилегий.
- Пользователь может иметь доступ к *нескольким* ролям.
- Одна и та же роль может быть назначена *нескольким* пользователям.
- Обычно роли создаются для приложения БД.

Пример. Создание роли и предоставление ей привилегий

- **Создание роли**

```
CREATE ROLE developer;
```

- **Предоставление роли привилегий**

```
GRANT create table TO developer;
```

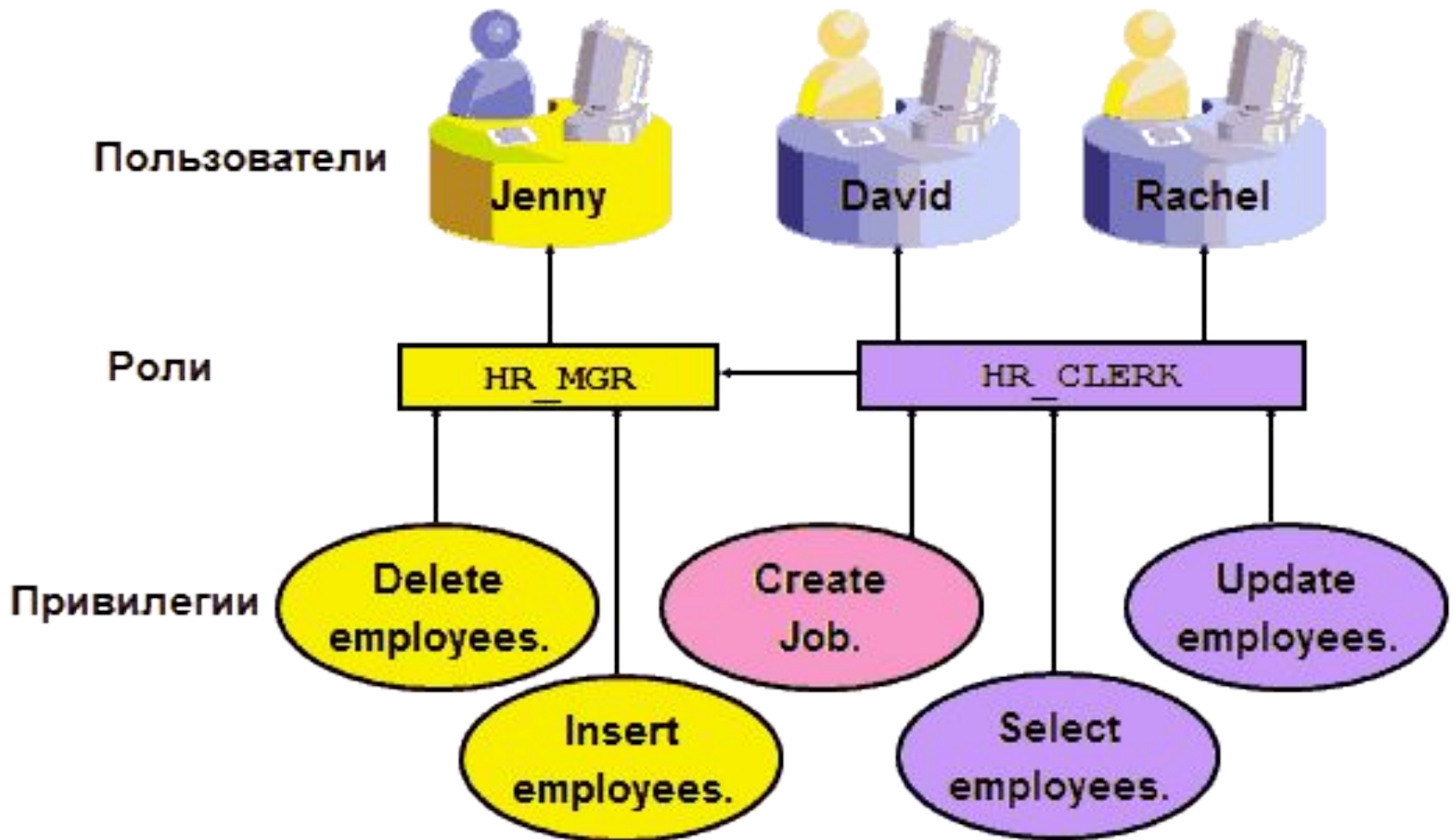
- **Назначение роли пользователям БД**

```
GRANT developer TO ivan, petr
```

Характеристики ролей

- Привилегии выдаются и отбираются у ролей с помощью команд **GRANT** и **REVOKE**.
- Роли могут состоять как из системных, так и объектных привилегий.
- **Роль можно включать и выключать** для пользователя, кому она предоставлена.
- Для включения роли может требоваться **пароль**.
- **Роли никому не принадлежат**, они не находятся ни в чьей схеме.

Пример. Наследование ролей



Предопределенные роли

Сразу после создания БД

Oracle в ней есть роли:

- **CONNECT** – create session
- **RESOURCE** – create table, create sequence, create type, create procedure ...
- **DBA** – большинство системных привилегий
- **SELECT_CATALOG_ROLE** – привилегии доступа к словарю данных



Безопасность БД

- Администратор БД обеспечивает начальную степень безопасности БД – он создает учетные записи пользователей.
- С помощью команды CREATE ROLE администратор БД может создавать роли.
- Ролям выдаются необходимые привилегии (системные и объектные).
- Роли назначаются пользователям БД.

SQL-команды, используемые для настройки безопасности БД

Команда	Описание
CREATE USER	Позволяет АБД создавать пользователей БД.
GRANT	Позволяет предоставлять пользователю системные, объектные привилегии и роли.
CREATE ROLE	Позволяет АБД создавать роли – именованные наборы привилегий.
ALTER USER	Позволяет пользователям менять свои пароли
REVOKE	Отменяет выданные ранее пользователю привилегии и роли.

Обзоры словаря БД

Информацию о ролях и доступных им привилегиях можно получить из словаря базы данных.

Обзоры словаря БД	Описание
ROLE_SYS_PRIVS	Системные привилегии, предоставленные ролям
ROLE_TAB_PRIVS	Привилегии на таблицы, предоставленные ролям
DBA_ROLES	Список всех ролей, имеющих в БД
USER_ROLE_PRIVS	Роли, доступные пользователю

ИТОГИ

- Роли позволяют сделать процессы предоставления и отмены привилегий более простыми.
- В процессе разработки приложения программист должен реализовать механизм разграничения прав доступа на основе ролей.