Проблемы безопасности в БД

- СУБД не должны решать проблем безопасности файлового и сетевого уровня
- Безопасность в БД обеспечивается для метаданных и информации

Firebird

- База данных пользователей
  - security.fdb
  - security2.fdb (Для версии выше 2.0)
- Суперпользователь
  - SYSDBA
- Работа с базой данных пользователей
  - Утилита gsec

gsec

- Таблицы
  - USERS
  - RDB$USERS
- Разные права у SYSDBA и простого пользователя

gsec

- Интерактивный режим

gsec –user SYSDBA –password masterkey

GSEC>

- Команды
  - добавление нового пользователя

    add <имя> -pw <пароль> [<параметры>]
  - удаление пользователя

    delete <имя>

gsec

- вывод информации обо всех зарегистрированных пользователях, пароли не показываются

  display

- вывод информации только об одном пользователе

  display <имя>

- изменение информации о пользователе, включая пароль

  modify <имя> <параметр> [<параметры>]

- справка по командам

  help или ?

- выход из интерактивного режима

  quit

Пример

gseq>add newuser –pw password

con> –fname User –lname First;

Права пользователей

- доступ и работа с объектами базы данных, если этот пользователь является владельцем этих объектов
- предать права работы с объектами другому пользователю
- работать с чужими объектами, права на которые выданы этому пользователю владельцем объекта или администратором SYSDBA

Выдача прав (разрешений)

GRANT <привилегия>
[ON <объект>]
TO {<пользователь>|
<список пользователей>|PUBLIC|
<роль>|
<триггер>|<хранимая процедура>}
[{WITH GRANT OPTION|
WITH ADMIN OPTION]};

Привилегии

- SELECT, INSERT, UPDATE, DELETE
- ALL
- EXECUTE
- REFERENCES
- ROLE (без фразы ON)

- UPDATE и REFERENCES могут быть ограничены отдельными столбцами

Отмена разрешений

REVOKE <привилегия>
  ON <объект>
  FROM {<пользователь>|<роль>}

REVOKE GRANT OPTION
FOR <привилегия>
  ON <объект>
  FROM <пользователь>

Предоставление привилегий через роли

- Роль – объект схемы БД
- Создание роли
  - CREATE ROLE <имя роли>
    [WITH ADMIN OPTION];
- Удаление роли
  - DROP ROLE <имя роли>;

Предоставление привилегий роли

GRANT <привилегия>

[ON <объект>]

TO <имя роли>;

Предоставление роли пользователю

GRANT <имя роли>

TO {<пользователь>|

<список пользователей>|PUBLIC

[WITH ADMIN OPTION];

Доступ пользователя к БД через роль

CONNECT <путь доступа к базе данных>

USER <имя пользователя>

ROLE <имя роли>

PASSWORD <пароль>;