

## **Вопросы для промежуточной аттестации по дисциплине «Хранение и защита информации в базах данных информационных систем»**

1. Специфика защиты в базах данных. Инференция и агрегирование
2. Специфика защиты в базах данных. Комбинация разрешенных запросов для получения закрытых данных;
3. Специфика защиты в базах данных. Организация скрытых каналов передачи информации (Covert Channels);
4. Специфика защиты в базах данных. SQL инъекции (SQL Injection);
5. Специфика защиты в базах данных. Программные закладки, отладочный код (Backdoors, Trapdoors)
6. Специфика защиты в базах данных. Троянские кони (Trojan Horses).
7. Принципы управление доступом к данным и функции защиты.
8. Дискреционное разграничение доступа в БД, достоинства и недостатки
9. Модель Харрисона-Руззо-Ульмана.
10. Операторы SQL предоставления и отмены привилегий.
11. Мандатное разграничение доступа, достоинства и недостатки
12. Ролевое разграничение доступа, достоинства и недостатки
13. Обеспечение целостности данных, основные положения и определения
14. Принципы обеспечения целостности данных
15. Модель Кларка-Вильсона
16. Модель Биба
17. Совместное использование моделей безопасности Белла-Лападулы и Биба
18. Операторы языка SQL задания ограничений целостности
19. Восстановление целостного состояния БД. Понятие транзакции
20. Принципы восстановления данных в БД
21. Методы восстановления БД
22. Организация восстановления данных в СУБД MS SQL Server
23. Защита данных с помощью представлений, сохраненных процедур, функций и триггеров, основные определения
24. Преимущества и недостатки представлений в СУБД
25. Transact-SQL
26. Понятие хранимой процедуры
27. Типы хранимых процедур
28. Выполнение хранимой процедуры
29. Понятие функции пользователя
30. Определение триггера в стандарте языка SQL
31. Система защиты Microsoft Access на уровне пользователя
32. Методы противодействия взлому защиты Access
33. Архитектура системы безопасности SQL Server
34. Система безопасности уровня сервера
35. Аутентификация Windows