**Перечень вопросов для итогового контроля студентов 4 курса по предмету «Безопасностъ базa данных».**

**Осенний семестр 2023/2024 учебного года**

1. Понятие базы данных?
2. Роль базы данных в УАИС.
3. Важность безопасности базы данных.
4. Основные угрозы безопасности баз данных в УАИС.
5. Методы идентификации и аутентификации пользователей.
6. Понятия идентификации и аутентификации и их отличия.
7. Системы управления доступом и их роль в обеспечении безопасности
8. Виды управления доступом. Их схожести и отличия.
9. Шифрование и защита данных в базах данных УАИС
10. Виды шифрования.
11. Резервное копирование и восстановление данных. Определение и виды
12. Мониторинг и аудит действий пользователей в базе данных.
13. Что такое система управления базами данных (СУБД), и какие основные виды СУБД существуют?
14. Какие механизмы обеспечивают целостность данных в СУБД?
15. Объясните различия между реляционными, документоориентированными и объектно-ориентированными СУБД.
16. Каково назначение первичного ключа в таблице базы данных?
17. Что такое внешние ключи, и как они обеспечивают целостность данных?
18. Какие ограничения существуют для обеспечения целостности данных в СУБД?
19. Какие основные методы обеспечения информационной безопасности в базах данных существуют?
20. Опишите механизм шифрования данных в базе данных.
21. Чем отличаются методы предотвращения несанкционированного доступа от методов обнаружения атак?
22. В чем состоит различие между физической и логической защитой данных?
23. Как технологии виртуализации могут повлиять на безопасность базы данных?
24. Какие риски связаны с доступом к базе данных через сеть?
25. Опишите основные модели безопасности для баз данных (например, мандатная, дискреционная и ролевая модели).
26. Как реализуется ограничение доступа к данным в мандатной модели безопасности?
27. Какие особенности есть у многоуровневой модели безопасности?
28. Какую роль играет политика доступа в модели дискреционного управления?
29. В чем преимущества многоуровневой модели безопасности?
30. Как реализуется управление доступом в модели RBAC (Role-Based Access Control)?
31. Что такое ролевая модель защиты данных, и в чем ее преимущества?
32. Как создать и настроить роли в реляционной СУБД?
33. В чем отличие роли от привилегии в базе данных?
34. Какие действия можно ограничивать с помощью ролей в базе данных?
35. Как изменяется безопасность системы при использовании ролей вместо индивидуальных разрешений?
36. Приведите пример настройки роли для администратора базы данных.
37. Какие риски возникают при работе с распределенными базами данных?
38. Опишите концепцию обеспечения информационной безопасности в распределенных СУБД.
39. Как обеспечивается защита данных при их передаче между узлами распределенной базы данных?
40. Какие дополнительные меры безопасности необходимы для шифрования данных в распределенной системе?
41. Как защищаются данные при использовании репликации в распределенных базах данных?
42. Какие механизмы используются для предотвращения консистентнос данных в распределенных системах?
43. Что такое транзакция, и каковы ее основные свойства (ACID)?
44. Для чего используются мониторы транзакций в СУБД?
45. Объясните процесс репликации данных и ее виды (синхронная и асинхронная).
46. Почему важно использовать механизмы блокировок при работе с транзакциями?
47. Какие проблемы могут возникнуть при параллельном выполнении транзакций?
48. Объясните различие между активным и пассивным монитором транзакций.
49. Почему важно использовать политику паролей для защиты СУБД?
50. Какие требования обычно предъявляются к надежным паролям в СУБД?
51. Истечение срока действия пароля
52. Защита соединения с базой данных
53. Запрещенные слова и шаблоны
54. Как настроить автоматическую проверку паролей в СУБД?
55. Какие методы предотвращают повторное использование старых паролей?
56. Что такое двухфакторная аутентификация, и как она используется для защиты СУБД?
57. Какие требования предъявляются к хранению паролей в СУБД?
58. Что такое аудит базы данных, и для чего он используется?
59. Задачи аудита безопасности БД
60. Основные компоненты аудита безопасности
61. Идентификация и анализ угроз безопасности
62. Методы аудита привилегий пользователей и ролей
63. Проверка конфигурации и настроек безопасности
64. Мониторинг событий и журналов безопасности
65. Выявление попыток несанкционированного доступа
66. Какие инструменты используются для мониторинга безопасности базы данных?
67. Объясните, как настроить журналирование событий в базе данных.
68. Какую информацию можно получить с помощью аудита базы данных?
69. Какие события должны обязательно регистрироваться в рамках мониторинга?
70. Какие инструменты позволяют анализировать журналы безопасности базы данных?
71. Какие типы резервного копирования существуют в СУБД?
72. Объясните процесс восстановления базы данных после сбоя.
73. Какую роль играют журналы транзакций при восстановлении базы данных?
74. Какие стратегии резервного копирования существуют для крупных баз данных?
75. Что такое инкрементное резервное копирование, и в чем его преимущества?
76. Как осуществляется проверка целостности резервной копии?
77. Какие основные компоненты системы безопасности имеются в СУБД?
78. Как архитектура базы данных влияет на ее защиту?
79. Опишите принципы работы системы контроля доступа в базе данных.
80. Какую роль играет модуль аутентификации в системе безопасности базы данных?
81. Какие компоненты отвечают за контроль целостности данных?
82. В чем особенности работы систем защиты на уровне сетевого доступа?
83. Какие международные стандарты регламентируют информационную безопасность баз данных?
84. Какую роль играет стандарт ISO/IEC 27001 в безопасности баз данных?
85. Приведите примеры технических условий для защиты данных в СУБД.
86. Какие стандарты регламентируют шифрование данных в базах данных?
87. Как стандарты безопасности влияют на проектирование базы данных?
88. Какие обязательные требования могут быть прописаны в технических условиях безопасности?
89. Какие угрозы характерны для баз данных в облаке?
90. Какие методы защиты используются для шифрования данных в облаке?
91. Объясните концепцию разграничения обязанностей в облачных базах данных.
92. Какие особенности защиты данных облачных технологий отличают их от локальных баз данных?
93. Как осуществляется защита доступа к базам данных в облачной инфраструктуре?
94. Какие дополнительные меры безопасности необходимо применять для мультиарендных баз данных?
95. Какие инструменты Oracle предоставляют для обеспечения безопасности баз данных?
96. Объясните принцип работы Virtual Private Database (VPD) в Oracle.
97. Как настроить шифрование данных в Oracle Database?
98. Какие функции предоставляет Oracle Data Redaction для защиты данных?
99. Как работает механизм Transparent Data Encryption (TDE) в Oracle?
100. Какие политики безопасности можно настроить с помощью Oracle Label Security?