


Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Сахалинский государственный университет»

Кафедра информатики

УТВЕРЖДЕН
на заседании кафедры
«19» марта 2024 г, протокол № 8
Исполняющий обязанности
заведующего кафедрой

 Осипов Г.С.

**ФОНД
ОЦЕНОЧНЫХ СРЕДСТВ
ПО ДИСЦИПЛИНЕ (МОДУЛЮ)**

Б1.О.32 Администрирование информационных систем

Направление подготовки

10.03.01 Информационная безопасность

профиль

Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)

Уровень высшего образования

БАКАЛАВРИАТ

Южно-Сахалинск
2024 г.

1. Формируемые компетенции и индикаторы их достижения по дисциплине (модулю)

Код компетенции	Содержание компетенции	Код и наименование индикатора достижения компетенции
ОПК-4.2	Способен администрировать операционные системы, системы управления базами данных, вычислительные сети;	ОПК-4.2.1 Знать теоретические основы администрирования информационных систем, функции управления и поддержки программного обеспечения информационных систем ОПК-4.2.2 Уметь устанавливать, настраивать и обслуживать программные средства в ходе внедрения информационных систем и технологий в промышленную эксплуатацию. ОПК-4.2.3 Владеть навыками администрирования информационных систем, а также обеспечивать эффективную их работу, обслуживание и последующую модернизацию.
ОПК-4.3	Способен выполнять работы по установке, настройке, администрированию, обслуживанию и проверке работоспособности отдельных программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации автоматизированных систем;	ОПК-4.3.1 Знать теоретические основы функционирования и сопровождения информационных систем, функции по установке, настройке, администрированию, обслуживанию и проверке работоспособности программного обеспечения; ОПК-4.3.2 Уметь выполнять установку, настройку, администрирование, обслуживание и проверку работоспособности программного обеспечения информационных систем. ОПК-4.3.3 Владеть способностью выполнять работы и управлять работами по созданию (модификации) и сопровождению информационных систем, автоматизирующих бизнес-процессы в организациях различной форм собственности.

2. Паспорт фонда оценочных средств по дисциплине (модулю)

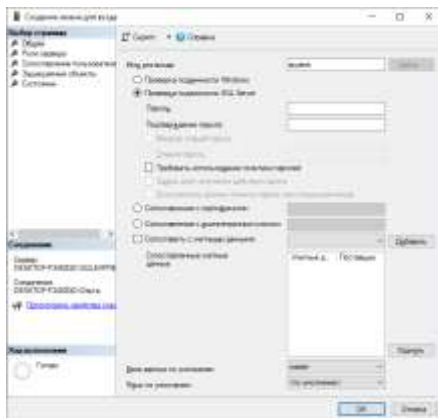
№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	Тема 1. Основы функционирования и сопровождения информационных систем	ОПК-4.2 ОПК-4.3	Лабораторный практикум, контрольные вопросы, тестирование, вопросы к зачету
2	Тема 2 Системное и сетевое администрирование	ОПК-4.2 ОПК-4.3	Лабораторный практикум, контрольные вопросы, тестирование, вопросы к зачету

3	Тема 3 Администрирование баз данных	ОПК-4.2 ОПК-4.3	Лабораторный практикум, контрольные вопросы, тестирование, вопросы к зачету
4	Тема 4 Аппаратно-программные платформы администрирования информационных систем	ОПК-4.2 ОПК-4.3	Лабораторный практикум, контрольные вопросы, тестирование, вопросы к зачету
5	Тема 5 Эксплуатация и сопровождение информационных систем	ОПК-4.2 ОПК-4.3	Лабораторный практикум, контрольные вопросы, тестирование, вопросы к зачету
6	Тема 6 Управление эксплуатацией и сопровождением информационных систем	ОПК-4.2 ОПК-4.3	Лабораторный практикум, контрольные вопросы, тестирование, вопросы к зачету

Лабораторный практикум

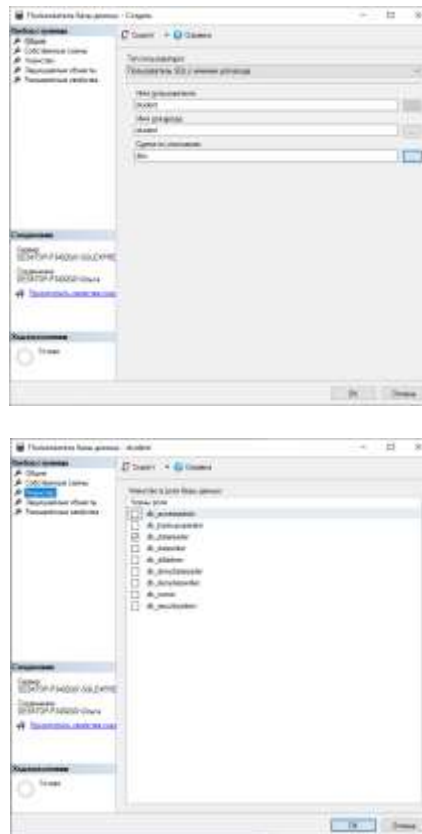
Задание: войти в SSMS с правами администратора (запустить MS SQL Server). Создать новое имя для входа в SSMS - *student* (без пароля). Не выходя из MS SQL Server (с правами администратора) создайте новую БД TEST и дайте пользователю *student* разрешение только на чтение данных (роль базы данных db_datareader).

1. Создать новое имя для входа в SSMS - *student* (без пароля). Безопасность / Имена для входа / Создать имя для входа.



2. Не выходя из MS SQL Server (с правами администратора) создайте новую БД TEST (таблица Клиенты (Код, ФИО), введите одну запись).

3. Для только что созданной БД TEST создать нового пользователя – *student*. Базы данных / TEST / Безопасность / Пользователи / Создать пользователя. Заполнить только 2 вкладки: Общие и Членство, как показано на рисунке ниже.



4. Перезагрузить SSMS, войти под пользователем *student* и проверить, можно ли вводить изменения в БД TEST. Система должна выдать ошибку о невозможности вносить изменения в БД TEST, так как пользователь *student* не имеет на это прав.

Перечень контрольных вопросов

1. Комплекс программно-технических средств и административных мер по обеспечению надежности и информационной безопасности компьютерной сети предприятия.
2. Технологии построения виртуальной частной сети.
3. Классификация операционных систем.
4. Сетевые операционные системы: структура, назначение, функции
5. Администрирование почтовых и Internet серверов
6. Маршрутизация в сетях TCP/IP.
7. Стек протоколов TCP/IP.
8. Протоколы удаленного доступа.
9. Администрирование локальных вычислительных сетей.
10. Администрирование операционных систем.
11. Администрирование баз данных.
12. Управление конфигурацией ИС.
13. Аутентификация в распределенных системах.
14. Инструменты администрирования пользователей.
15. Типы архитектур распределенных информационных систем.
16. Распределенные информационные системы.
17. Средства обеспечения защиты информации.
18. По каким трем основным уровням распределяются специальные методы и средства обеспечения надежности и информационной безопасности?
19. Надежность и безопасность информационных систем.

20. Аппаратно-программные платформы администрирования локальных сетей.
21. Аппаратно-программные платформы администрирования баз данных.
22. Принципы построения и администрирования информационных систем.
23. Программные средства автоматизации администрирования.
24. Аппаратные средства автоматизации администрирования.
25. Сопровождение информационных систем.
26. Эксплуатация информационных систем.
27. Мероприятия по обеспечения безопасности информационных систем.
28. Средства обеспечения безопасности.
29. Виды угроз безопасности информационных систем.
30. Домены. Основные задачи администрирования доменных сетей.
31. Права и разрешения. Группы безопасности и управление разрешениями.
32. Виды ресурсов информационных систем и задачи управления ими.
33. Информационные системы и основные задачи их администрирования
34. Способы аутентификации, многофакторная аутентификация

Тестовые задания

1. Сколько выделенных серверов может одновременно работать в сети?
 - 1)Нет специальных ограничений
 - 2)В зависимости от занятости оперативной памяти
 - 3)Только один сервер
 - 4)По числу требуемых в сети служб: для каждой сетевой службы отдельный выделенный сервер
2. Какого типа адреса могут быть одинаковыми в разных процессах?
 - 1)Виртуальные
 - 2)Физические
 - 3)Реальные
 - 4)сегментные
3. Для управления безопасностью на уровне строк в СУБД используют:
 - 1)Запросы
 - 2)Типы данных,
 - 3)Представления,
 - 4)Триггеры,
 - 5)Функции, возвращающие таблицы
4. Безопасность информации это:
 - 1)Когда информация безопасна
 - 2)Отсутствие ущерба от информации
 - 3)Учтены все аспекты обеспечения безопасности
 - 4)Когда информация защищена
 - 5)Состояние защищенности информации.
5. Состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право называется:
 - 1)Целостность
 - 2)Доступность
 - 3)Неотказуемость
 - 4)Подотчетность

5) Конфиденциальность.

6. Состояние информации, при котором её изменение осуществляется только преднамеренно субъектами, имеющими на него право называется:

- 1) Доступность
- 2) Неотказуемость
- 3) Подотчетность
- 4) Конфиденциальность
- 5) Целостность

7. Проверка принадлежности субъекту доступа предъявленного им идентификатора называется:

- 1) Авторизация
- 2) Идентификация
- 3) Инициализация
- 4) Субъективизация
- 5) Аутентификация

8. Совокупность правил, регламентирующих права субъектов доступа к объектам доступа.

- 1) Правила поведения пользователя
- 2) Санкционированный доступ
- 3) Несанкционированный доступ
- 4) Идентификация
- 5) Правила разграничения доступа

9. Объектом доступа в СУБД может выступать:

- 1) Компьютер
- 2) Папка
- 3) Файл
- 4) Пользователь
- 5) Таблица
- 6) Столбец таблицы
- 7) Процедура

10. Модель разграничения доступа, основанная на объединении пользователей в группы, называется:

- 1) дискреционной
- 2) мандатной
- 3) групповой
- 4) ролевой

11. Модель разграничения доступа между поименованными субъектами и поименованными объектами это:

- 1) Ролевая модель
- 2) Сетевая модель
- 3) Мандатная модель
- 4) Иерархическая модель
- 5) Дискреционная модель

12. Выберите виды информационных систем по степени автоматизации:

- 1) Вычислительные
- 2) Стратегические

- 3) Ручные
- 4) Автоматизированные
- 5) Автоматические.

Примерный перечень вопросов к зачету (8 семестр)

1. Функции и процедуры администрирования информационных систем.
2. Управление конфигурацией информационных систем, выявление и контроль сбойных и ошибочных ситуаций.
3. Управление системой безопасности информационных систем.
4. Управление общим доступом в информационных системах.
5. Объекты и методы администрирования информационных систем.
6. Администрирование операционных систем, локально-вычислительных сетей и баз данных
7. Основы управления пользователями.
8. Понятие домена и рабочей группы.
9. Права доступа к файлам и каталогам.
10. Политики учетных записей.
11. Принципы резервного копирования.
12. Устройства, используемые для резервного копирования.
13. Архивирование и восстановление при модификации системы.
14. Ведение локальной документации.
15. Слежение за безопасностью системы.
16. Стратегия и методика администрирования.
17. Система NAT.
18. Трансляция адресов.
19. Сетевые службы.
20. Совместное использование файлов.
21. Взаимодействие операционных систем.
22. Организация электронной почты.
23. Сетевая безопасность.
24. Аутентификация.
25. Инструментальные средства защиты информационных систем.
26. Системы криптографической защиты в информационных системах.
27. Принципы построения информационных систем.
28. Программирование в системах администрирования.
29. Сценарии регистрации и скрипты администрирования.
30. Примеры систем администрирования с использованием Windows Script Host.
31. Служба каталогов Active Directory для операционных систем семейства Windows Server.
32. Средства администрирования ЛВС на примере домена Windows Server.
33. Защита информационных систем от угроз безопасности.
34. Виды угроз безопасности информационных систем.
35. Средства, мероприятия и нормы обеспечения безопасности.
36. Обычные меры организационной защиты для борьбы с преднамеренными угрозами.
37. Аппаратные средства защиты информационных систем.
38. Программные ограничения, препятствующие угрозам.
39. Организационные мероприятия по обеспечению безопасности.
40. Политика безопасности магистрального уровня.
41. Политика безопасности уровня распределения.

- 42. Политика безопасности на уровне доступа
- 43. Работы по внедрению компонентов ИС в эксплуатацию.
- 44. Обеспечение эксплуатационной документацией.
- 45. Проведение обучения персонала.
- 46. Модификация ИС в рамках установленного регламента, подготовка предложений по совершенствованию, развитию и модернизации системы.

Составитель
«12» марта 2024 г.



к.п.н., доцент Корнева О.С.