МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Заведующий кафедрой
информационной безопасности
(наименование ф-та полностью)
М.О. Таныгин
(подпись, инициалы, фамилия)
« 29 » августа 2022 г.

ОЦЕНОЧНЫЕ СРЕДСТВА
для текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Безопасность распределенных баз данных
(наименование учебной дисциплины)

10.05.02 Информационная безопасность, направленность (профиль) «Защита информации в системах связи и управления»
(код и наименование ОПОП ВО)

Курск – 2022

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ УСТНОГО ОПРОСА

Тема 1. Понятия и определения безопасности распределенных баз данных

1. Что такое распределенная база данных?
2. Какие виды угроз безопасности могут возникать в распределенных базах данных?
3. Что такое шифрование данных и как оно может быть использовано для защиты распределенных баз данных?
4. Что такое контроль доступа и как он может быть использован для обеспечения безопасности распределенных баз данных?

Тема 2. Структура связи в распределенных базах данных

1. Какова основная цель распределения баз данных?
2. Какие существуют методы связи между узлами распределенной базы данных?
3. Какие преимущества имеет метод связи "сеть"?

Какой метод связи наиболее распространен в распределенных базах данных?

Тема 3. Современные ОС

1. Что такое операционная система и какие функции она выполняет?
2. Какие типы операционных систем существуют и как они отличаются друг от друга?
3. Что такое многозадачность и как ее реализуют в операционных системах?
4. Как происходит управление памятью в операционных системах?

Тема 4. Распределенные файловые системы

1. Что такое распределенная файловая система и как она отличается от локальной?
2. Какие основные проблемы решает распределенная файловая система?
3. Как обеспечивается целостность и безопасность данных в распределенных файловых системах?
4. Какие алгоритмы используются для балансировки нагрузки в распределенных файловых системах?

Тема 5. История безопасности распределенных баз данных

1. Какие основные проблемы безопасности распределенных баз данных возникали в прошлом?
2. Каким образом эволюционировала безопасность распределенных баз данных со временем?
3. Какие современные технологии используются для обеспечения безопасности распределенных баз данных?
4. Какие вызовы и проблемы стоят перед безопасностью распределенных баз данных в настоящее время?

Критерии оценки:

3-4 балла(или оценка «отлично») выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

2 балла (или оценка «хорошо») выставляется обучающемуся, если он владеет содержанием вопроса, но допускает некоторые недочеты при ответе; допускает незначительные неточности при определении основных понятий; недостаточно аргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свой ответ типовыми примерами.

1 балл (или оценка «удовлетворительно») выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов (или оценка «неудовлетворительно») выставляется обучающемуся, если он не владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основные определения; не может привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе на них грубые ошибки.

1.2 КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ЗАЩИТЫ ЛАБОРАТОРНЫХ РАБОТ

Лабораторная работа № 1 «Аппаратные и программные средства построения распределенных систем»

1. Какие аппаратные средства необходимы для построения распределенных систем?

2. Какие программные средства используются для построения распределенных систем?
3. Какую роль играют операционные системы в построении распределенных систем?
4. Какие алгоритмы используются для балансировки нагрузки в распределенных системах?

Лабораторная работа № 2«Файловая система NFS»

1. Что такое файловая система NFS?
2. Какие возможности предоставляет NFS?
3. Какие особенности управления доступом к файлам в NFS?
4. Какие альтернативы существуют для NFS и в каких случаях их применение может быть целесообразным?

Лабораторная работа №3«Определение параметров видеокарты с поддержкой технологии CUDA в среде Microsoft Visual Studio»

1. Что такое технология CUDA?
2. Какие настройки проекта необходимо задать для работы с технологией CUDA в Visual Studio?
3. Какие библиотеки необходимо подключить для работы с технологией CUDA в Visual Studio?
4. Какие методы оптимизации кода для работы с технологией CUDA можно использовать в Visual Studio?

Критерии оценки:

3-4 балла(или оценка «отлично») выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

2 балла (или оценка «хорошо») выставляется обучающемуся, если он владеет содержанием вопроса, но допускает некоторые недочеты при ответе; допускает незначительные неточности при определении основных понятий; недостаточно аргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свой ответ типовыми примерами.

1 балл (или оценка «удовлетворительно») выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов (или оценка «неудовлетворительно») выставляется обучающемуся, если он не владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основные определения; не может привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе на них грубые ошибки.

1.3 КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ЗАЩИТЫ ПРАКТИЧЕСКИХ РАБОТ

Практическая работа № 1 «Понятие СУБД, проектирование распределенных баз данных.»

1. Что такое СУБД?
2. Какие преимущества имеют распределенные базы данных перед централизованными?
3. Какие основные компоненты входят в архитектуру распределенной базы данных?
4. Какие модели данных используются при проектировании распределенных баз данных?
5. Какие методы фрагментации данных вы знаете? Как они используются при проектировании распределенных баз данных?

Практическая работа № 2«Организация защиты РБД»

1. Что такое РБД и какие типы РБД бывают?
2. Какие методы обеспечения конфиденциальности данных в РБД вы знаете?
3. Какие методы обеспечения целостности данных в РБД вы знаете?
4. Какие методы обеспечения доступности данных в РБД вы знаете?
5. Что такое аутентификация и авторизация пользователей в РБД?

Практическая работа № 3«Структура и синтаксис запросов.»

1. Что такое SQL?
2. Какие операторы SQL вы знаете?
3. Что такое SELECT, FROM, WHERE, GROUP BY, HAVING, ORDER BY?
4. Какой синтаксис использовать при написании запроса SELECT?
5. Какие типы соединений вы знаете?

Практическая работа №4«Резервное копирование РБД»

1. Что такое резервное копирование РБД?
2. Какие методы резервного копирования существуют?

3. Какой режим резервного копирования выбрать для различных типов РБД?

4. Как часто необходимо выполнять резервное копирование?

5. Что такое логическое и физическое восстановление РБД?

Критерии оценки:

3-4 балла(или оценка «отлично») выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

2 балла (или оценка «хорошо») выставляется обучающемуся, если он владеет содержанием вопроса, но допускает некоторые недочеты при ответе; допускает незначительные неточности при определении основных понятий; недостаточно аргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свой ответ типовыми примерами.

1 балл (или оценка «удовлетворительно») выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов (или оценка «неудовлетворительно») выставляется обучающемуся, если он не владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основные определения; не может привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе на них грубые ошибки.

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

2.1 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ

Задания в закрытой форме

1. Что отражает модель жизненного цикла информационной системы?

1) все события, происходящие с системой в процессе ее создания и использования

2) процесс создания системы

3) процессы, связанные с использованием системы

4) все события в системе во время ее эксплуатации

2. Для чего производится предварительное обследование объекта автоматизации?

1) для формирования концепции создания системы

2) для создания прототипа системы

3) для выяснения готовности предприятия к автоматизации

4) для формирования команды, которая будет работать над созданием системы

3. Укажите основную цель детального обследования объекта автоматизации.

1) формирование технического задания на систему

2) подбор исполнителя для создания системы

3) определение целей автоматизации

4) выбор технических и программных инструментов

4. Отметьте методы сбора информации при проведении обследования объекта автоматизации.

1) анкетирование

2) интервьюирование

3) метод аналогий

4) создание "фотографии рабочего дня"

5) метод проб и ошибок

6) метод Монте-Карло

5. Какие данные обрабатываются в фактографических информационных системах?

1) структурированные данные в виде текстов и чисел

2) любые изображения

3) только числовые

4) исторические факты

6. Какая методология моделирования систем использует понятие "Прецедент"?

1) методология объектно-ориентированного моделирования

2) структурное моделирование

3) визуальное моделирование

4) функциональное моделирование

7. В основе архитектурного проектирования лежат понятия:

1) Проектирование – как средство достижения поставленного результата

2) Архитектура – как результат

3) Архитектура – как видение

4) Проектирование – как инструмент планирования разработки

8. Проектирование - это

1) вид активности направленный на создание уникального продукта (услуги), последовательность этапов реализации которого, будет определяться «внешними» факторами, и определять его конечные преимущества и недостатки

2) видение конечного результата реализации информационной системы

3) процесс формирования структуры проекта

4) анализ текущего состояния структуры компании и предложение идей об улучшении бизнес-процессов

9. Архитектурное проектирование - это

1) процесс реализации пожеланий Стэйкхолдеров

2) работы по подготовке структуры взаимодействия систем в организации

3) вид активности, который своей целью ставит создание архитектуры в процессе выполнения проекта

4) вид работ по определению границ проекта

10. Архитектурное проектирование программного обеспечения, одной из задач ставит

1) бесперебойное функционирование информационных систем компании

2) поддержку и развитие существующих процессов и информационных систем компании

3) формирование особого видения, всех участников проекта, на конечный продукт

4) создание артефакта (архитектуры), который должен обеспечить достижение результатов деятельности организаций, использующих программные продукты для реализации своих процессов

11. Программные продукты – это

1) исполняемые процедуры

2) реализация требований Спонсоров проекта

3) взаимосвязанные информационные сущности, выполняющие запросы Пользователей

4) основной элемент большинства современных высокотехнологичных доменов деятельности

12. Причиной развития темы архитектуры программного обеспечения является

1) рост издержек предприятий

2) развитие технологий

3) нарастающая конкуренция

4) требования к качеству информационных продуктов

13. Шаблоны проектирования (design patterns) представляет собой

1) руководство по реализации

2) универсальный свод информации

3) проектная документация на разработку

4) ограничения по реализации

14. Архитектурные решения - это

1) соглашения, учитывающие и удовлетворяющие различные точки зрения, «силы», принципы, как технического, так и не технического характера

2) соглашения, между Архитектором и Командой по реализации

3) тип используемых методик проектирования

4) видение конечного результата реализации

15. Выбор стиля использования шаблонов производится на основании

1) имеющихся ресурсов

2) конкурентной среды

3) политики организации

4) требований

16. Сложность обеспечения информационной безопасности является следствием:

1) злого умысла разработчиков информационных систем

2) объективных проблем современной технологии программирования

3) происков западных спецслужб, встраивающих "закладки" в аппаратуру и программы

17. Сложность обеспечения информационной безопасности является следствием:

1) невнимания широкой общественности к данной проблематике

2) все большей зависимости общества от информационных систем

3) быстрого прогресса информационных технологий, ведущего к постоянному изменению информационных систем и требований к ним

18. Что из перечисленного относится к числу основных аспектов информационной безопасности:

1) подотчетность - полнота регистрационной информации о действиях субъектов

2) приватность - сокрытие информации о личности пользователя

3) конфиденциальность - защита от несанкционированного ознакомления

19. Компьютерная преступность в мире:

1) остается на одном уровне

2) снижается

3) растет

20. Что из перечисленного не относится к числу основных аспектов информационной безопасности:

1) доступность

2) целостность

3) защита от копирования

4) конфиденциальность

21. Укажите, с какой целью строятся диаграммы для экспозиции (FEO).

1) для иллюстрации отдельных фрагментов модели

2) для иллюстрации альтернативной точки зрения

3) для иллюстрации специальных целей

4) для иллюстрации взаимосвязи между работами

22. Укажите, что показывает диаграмма дерева узлов.

1) иерархическую зависимость работ

2) взаимосвязи между работами

3) глубины детализации

23. Укажите, что входит в определение контекста модели.

1) определение субъекта моделирования

2) определение цели моделирования

3) определение точки зрения

4) определение количества уровней декомпозиции

24. Какие типы элементарных моделей используются для построения организационно-функциональной структуры?

1) древовидные модели (классификаторы)

2) процессные модели

3) матричные модели

25. Какая модель отвечает на вопросы: *зачем* компания занимается именно этим бизнесом, *почему* предполагает быть конкурентоспособной, *какие* цели и стратегии для этого необходимо реализовать?

1) стратегическая модель целеполагания

2) организационно-функциональная модель

3) функционально-технологическая модель

4) процессно-ролевая модель

5) модель структуры данных

26. Сформулируйте цель методологии проектирования ИС

1) регламентация процесса проектирования ИС и обеспечение управления этим процессом с тем, чтобы гарантировать выполнение требований как к самой ИС, так и к характеристикам процесса разработки

2) формирование требований, направленных на обеспечение возможности комплексного использования корпоративных данных в управлении и планировании деятельности предприятия

3) автоматизация ведения бухгалтерского аналитического учета и технологических процессов

27. Выделите утверждение, верное в отношении защиты сетей.

1) уровень защищенности сети определяется уровнем защищенности ее самого «сильного» звена

2) уровень защищенности сети определяется суммой уровней защищенности ее звеньев

3) уровень защищенности сети определяется уровнем защищенности ее самого «слабого» звена

4) уровень защищенности сети не зависит напрямую от защищенности ее отдельных звеньев

28. Как называется мера доверия, которая может быть оказана архитектуре, инфраструктуре, программно-аппаратной реализации системы и методам управления её конфигурацией и целостностью?

1) эффективность безопасности

2) гарантированность безопасности

3) непрерывность безопасности

4) надежность безопасности

29. Каким термином обозначается анализ регистрационной информации системы защиты?

1) мониторинг

2) аудит

3) аккредитация

4) сертификация

30. Какие компоненты присутствуют в модели системы защиты с полным перекрытием?

1) область угроз

2) область рисков

3) защищаемая область

4) система защиты

5) область безопасности

31. Как называется возможность осуществления угрозы T в отношении объекта O?

1) слабость

2) неполнота

3) уязвимость

4) риск

32. Что означает система защиты с полным перекрытием?

1) для половины (и более) уязвимостей есть устраняющие барьеры

2) для любой уязвимости есть устраняющий ее барьер

3) у любой уязвимости есть риск ее реализации

4) количество уязвимостей меньше, чем количество препятствующих им барьеров

33. Чем характеризуется степень сопротивляемости механизма защиты?

1) вероятностью его преодоления

2) количеством угроз, которым этот механизм препятствует

3) величиной потерь в случае успешного прохождения

4) стоимостью механизма защиты

34. При отсутствии в системе барьеров, «перекрывающих» выявленные уязвимости, степень сопротивляемости механизма защиты принимается равной...

1) 0

2) 1

35. Защищенность системы защиты определяется как величина…

1) обратная суммарному количеству рисков

2) обратная остаточному риску

3) обратная уязвимости

4) равная сумме всех уязвимостей

36. В чем заключается идеология открытых систем информационной безопасности?

1) в строгом соответствии систем информационной безопасности законодательству страны, котором они созданы

2) в строгом соблюдении совокупности профилей, протоколов и стандартов де-факто и де-юре

3) в открытости информации о стоимости реализации конкретной системы защиты

4) в открытости программных кодов средств защиты от производителей разных стран

37. Для чего в первую очередь нужна идеология открытых систем информационной безопасности?

1) для удешевления средств защиты информации

2) для минимизации рисков от реализации угроз

3) для совместимости компонент различных информационных систем

38. В чем заключается принцип минимизации привилегий?

1) выделение полных прав доступа только администраторам системы

2) выделение только тех прав, которые необходимы для реализации своих должностных обязанностей

3) выделение прав доступа в зависимости от величины возможного ущерба

39. В чем заключается принцип эшелонирования обороны?

1) в том, чтобы использовать максимально возможное количество защитных средств

2) в простоте и управляемости информационной системы

3) в усилении самого надежного защитного рубежа

4) в том, чтобы не полагаться на один защитный рубеж

40. Что из нижеперечисленного относится к оперативным методам повышения безопасности?

1) систематическое тестирование

2) предотвращение ошибок в CASE-технологиях

3) обязательная сертификация

4) программная избыточность

41. Что такое безопасность в распределенных системах?

1. Обеспечение целостности, конфиденциальности и доступности данных и ресурсов в распределенных системах.
2. Увеличение скорости передачи данных в распределенных системах.
3. Увеличение масштабируемости распределенных систем.

42. Какие проблемы могут возникнуть при обеспечении безопасности в распределенных системах?

1. Проблемы с целостностью и конфиденциальностью данных.
2. Проблемы с доступностью данных.
3. Проблемы с авторизацией и аутентификацией пользователей.

43. Что такое аутентификация?

1.Проверка подлинности пользователя.
2.Проверка целостности данных.
3.Проверка доступности данных.

44. Что такое авторизация?

1. Проверка правильности доступа пользователя к данным.
2. Проверка целостности данных.
3. Проверка доступности данных.

45. Какие меры безопасности могут быть применены для обеспечения безопасности в распределенных системах?

1. Шифрование данных.
2. Аутентификация пользователей.
3. Авторизация пользователей.
4. Межсетевые экраны.
5. Все перечисленные меры безопасности.

46. Что такое SSL (Secure Sockets Layer)?

1. Протокол, который обеспечивает безопасность передачи данных по сети.
2. Программный продукт, который обеспечивает безопасность хранения данных.
3. Протокол, который обеспечивает быстрое соединение по сети.

47. Какой тип угроз наиболее часто встречается в распределенных системах?

1. Угрозы со стороны злоумышленников.
2. Неудачи оборудования.
3. Неудачи программного обеспечения.

48. Что такое DoS-атака?

1. Атака, направленная на привлечение внимания к определенной проблеме.
2. Атака, направленная на отказ в обслуживании сервиса.
3. Атака, направленная на получение конфиденциальной информации.

49. Транзакция - это:

1) хранимые процедуры, обеспечивающие соблюдение условий ссылочной целостности

2) поименованная совокупность таблиц, экранных форм, отчетов, запросов, относящихся к определенной предметной области

3) создание копий базы данных (реплик), которые могут обмениваться обновляемыми данными или реплицированными формами, отчетами или другими объектами в результате выполнения процесса синхронизации

4) поименованная совокупность структурированных данных, относящихся к определенной предметной области

5) изменение информации в базе в результате выполнения одной операции или их последовательности, которое должно быть выполнено полностью или не выполнено вообще

50. Концептуальная модель предметной области

1) отображает информационные объекты и их свойства без указания способов физического хранения информации

2) отражает все свойства (атрибуты) информационных объектов базы и связи между ними с учетом способа их хранения – используемой СУБД

3) база данных, соответствующая определенной логической модели

4) некоторая часть реально существующей системы, функционирующая как самостоятельная единица

51. Последовательность этапов разработки информационной системы:

1) анализ системы - проектирование - реализация проекта - внедрение - сопровождение

2) проектирование - анализ системы - реализация проекта - внедрение - сопровождение

3) реализация проекта - проектирование - анализ системы - внедрение - сопровождение

4) сопровождение - проектирование - реализация проекта - внедрение - анализ системы

5) внедрение - сопровождение - анализ системы - проектирование - реализация проекта

52. Логическая единица работы в базе данных - это:
1) транзакция

2) трансляция

3) трансформация

53. При фиксации изменений в базе данных может быть гарантировано сохранение:

1) нескольких изменений

2) последнего изменения

3) всех изменений

4) ни одного изменения

54. Транзакции базы данных обладают свойствами, сокращенно называемыми ACID, а именно:

1) неделимость

2) согласованность

3) стабильность

4) изолированность

5) защищенность

6) продолжительность

55. Неделимость транзакции означает, что:

1) транзакция либо выполняется полностью, либо не выполняется

2) транзакция переводит базу данных из одного согласованного состояния в другое

3) результаты транзакции становятся доступны для других транзакций только после ее фиксации

4) после фиксации транзакции изменения становятся постоянными

56. Согласованность транзакции означает, что:

1) транзакция либо выполняется полностью, либо не выполняется

2) транзакция переводит базу данных из одного согласованного состояния в другое

3) результаты транзакции становятся доступны для других транзакций только после ее фиксации

4) после фиксации транзакции изменения становятся постоянными

57. Изолированность транзакции означает, что:

1) транзакция либо выполняется полностью, либо не выполняется

2) транзакция переводит базу данных из одного согласованного состояния в другое

3) результаты транзакции становятся доступны для других транзакций только после ее фиксации

4) после фиксации транзакции изменения становятся постоянными

58. Продолжительность транзакции означает, что:

1) транзакция либо выполняется полностью, либо не выполняется

2) транзакция переводит базу данных из одного согласованного состояния в другое

3) результаты транзакции становятся доступны для других транзакций только после ее фиксации

4) после фиксации транзакции изменения становятся постоянными

59. Свойство транзакции, характеризующееся тем, что транзакция либо выполняется, либо не выполняется, называется:

1) неделимость

2) согласованность

3) изолированность

4) продолжительность

60. Свойство транзакции, характеризующееся тем, что транзакция переводит базу данных из одного согласованного состояния в другое, называется:

1) неделимость

2) согласованность

3) изолированность

4) продолжительность

61. Свойство транзакции, характеризующееся тем, что после фиксации транзакции изменения становятся постоянными, называется:

1) неделимость

2) согласованность

3) изолированность

4) продолжительность

62. Транзакции могут быть:

1) явные

2) неявные

3) специальные

63. Явная транзакция характеризуется следующим:

1) по умолчанию каждая команда выполняется как отдельная транзакция; пользователь может объединить несколько команд в одну транзакцию, указав ее начало и конец

2) не существует оператора начала транзакции; транзакция начинается с началом сеанса работы с БД и завершается по одному из событий (явно выполненный оператор завершения транзакции - rollback или commit, оператор DDL или завершение сеанса)

64. Неявная транзакция характеризуется следующим:

1) по умолчанию каждая команда выполняется как отдельная транзакция; пользователь может объединить несколько команд в одну транзакцию, указав ее начало и конец

2) не существует оператора начала транзакции; транзакция начинается с началом сеанса работы с БД и завершается по одному из событий (явно выполненный оператор завершения транзакции - rollback или commit, оператор DDL или завершение сеанса)

65. Возможны следующие сценарии взаимовлияния нескольких транзакций с точки зрения обработки одних и тех же данных:

1) грязное чтение

2) неповторяемость при чтении

3) несохраняемость при записи

4) чтение фантомов

66. Грязное чтение означает, что:

1) допускается чтение незафиксированных данных; при этом нарушается как целостность данных, так и требования внешнего ключа, а требования уникальности игнорируются

2) если строка читается в момент времени T1, а затем перечитывается в момент времени T2, то за этот период она может измениться; строка может исчезнуть, может быть обновлена и так далее

3) если выполнить запрос в момент времени T1, а затем выполнить его повторно в момент времени T2, в базе данных могут появиться дополнительные строки, влияющие на результаты; при этом прочитанные данные не изменились, но критериям запроса стало удовлетворять больше данных, чем прежде

67. Неповторяемость при чтении означает, что:

1) допускается чтение незафиксированных данных; при этом нарушается как целостность данных, так и требования внешнего ключа, а требования уникальности игнорируются

2) если строка читается в момент времени T1, а затем перечитывается в момент времени T2, то за этот период она может измениться; строка может исчезнуть, может быть обновлена и так далее

3) если выполнить запрос в момент времени T1, а затем выполнить его повторно в момент времени T2, в базе данных могут появиться дополнительные строки, влияющие на результаты; при этом прочитанные данные не изменились, но критериям запроса стало удовлетворять больше данных, чем прежде

68. Чтение фантомов означает, что:

1) допускается чтение незафиксированных данных; при этом нарушается как целостность данных, так и требования внешнего ключа, а требования уникальности игнорируются

2) если строка читается в момент времени T1, а затем перечитывается в момент времени T2, то за этот период она может измениться; строка может исчезнуть, может быть обновлена и так далее

3) если выполнить запрос в момент времени T1, а затем выполнить его повторно в момент времени T2, в базе данных могут появиться дополнительные строки, влияющие на результаты; при этом прочитанные данные не изменились, но критериям запроса стало удовлетворять больше данных, чем прежде

69. Оператор управления транзакциями SAVEPOINT:

1) позволяет устанавливать атрибуты транзакции

2) позволяет откатить транзакцию до указанной точки сохранения, не отменяя все сделанные до нее изменения

3) позволяет создать в транзакции "метку", или точку сохранения

70. Что такое аутентификация в контексте безопасности распределённых систем?

1) процесс проверки подлинности идентификационных данных пользователя
2) процесс шифрования данных, передаваемых между узлами сети
3) процесс фильтрации сетевого трафика
4) процесс сканирования сети на наличие уязвимостей

Ответ: а

71. Какое из перечисленных не является методом обеспечения конфиденциальности в распределённых системах?
1) шифрование данных
2) аутентификация пользователей
3) установка межсетевых экранов (firewalls)
4) обеспечение безопасности физического доступа к серверам
72. Что такое DDOS-атака?
1) атака на один конкретный узел сети
2) атака на сетевой протокол
3) атака на сетевую архитектуру
4) атака, целью которой является перегрузка сети путём отправки большого количества запросов
73. Что такое SSL?
1) протокол безопасности
2) язык программирования
3) база данных
4) аппаратный ключ

74. Что такое фильтрация трафика?
1) процесс шифрования данных, передаваемых между узлами сети
2) процесс аутентификации пользователей
3) процесс обнаружения и блокировки трафика, нарушающего правила сетевой безопасности
4) процесс защиты от DDOS-атак

75. Что такое аутентификация в контексте безопасности распределённых систем?
1) процесс проверки подлинности идентификационных данных пользователя
2) процесс шифрования данных, передаваемых между узлами сети
3) процесс фильтрации сетевого трафика
4) процесс сканирования сети на наличие уязвимостей

76. Какое из перечисленных не является методом обеспечения конфиденциальности в распределённых системах?

1) шифрование данных
2) аутентификация пользователей
3) установка межсетевых экранов (firewalls)
4) обеспечение безопасности физического доступа к серверам

77. Что такое DDOS-атака?
1) атака на один конкретный узел сети
2) атака на сетевой протокол
3) атака на сетевую архитектуру

4) атака, целью которой является перегрузка сети путём отправки большого количества запросов

78. Что такое SSL?

1) протокол безопасности
2) язык программирования
3) база данных
4) аппаратный ключ

79. Что такое фильтрация трафика?

1) процесс шифрования данных, передаваемых между узлами сети
2) процесс аутентификации пользователей
3) процесс обнаружения и блокировки трафика, нарушающего правила сетевой безопасности
4) процесс защиты от DDOS-атак

80. Что такое распределенная система?

1) Система, состоящая из нескольких компьютеров, которые работают независимо друг от друга;
2) Система, состоящая из нескольких компьютеров, которые работают вместе для решения общей задачи;
3) Система, состоящая из одного компьютера, который выполняет несколько задач одновременно.

81. Какие виды угроз могут возникать в распределенных системах?

1) Несанкционированный доступ к данным;
2) Нарушение целостности данных;
3) Отказ в обслуживании (DoS) и распределенный отказ в обслуживании (DDoS);
4) Все перечисленные варианты.

82. Что такое аутентификация?

1) Процесс проверки подлинности пользователя;
2) Процесс шифрования данных для защиты их от несанкционированного доступа;
3) Процесс установления защищенного соединения между клиентом и сервером.

83. Что такое шифрование?

1) Процесс проверки подлинности пользователя;
2) Процесс установления защищенного соединения между клиентом и сервером;
3) Процесс преобразования данных в такой вид, который не может быть понят или прочитан без специального ключа.

84. Что такое брандмауэр?

1) Средство для аутентификации пользователей;

2) Средство для шифрования данных;
3) Средство для защиты от несанкционированного доступа.

85. Какой из перечисленных методов шифрования является асимметричным?

1) AES
2) RSA
3) DES
4) Blowfish

86. Какой из перечисленных атак является целенаправленной нарушительской атакой?

1) Атака переполнения буфера

2) Атака отказа в обслуживании
3) Фишинг
4) Все перечисленные

87. Что означает аббревиатура IDS?

1) Информационная система документооборота
2) Система обнаружения вторжений
3) Система управления базами данных
4) Система контроля доступа

88. Какой из перечисленных видов аутентификации основан на знании определенной информации, такой как пароль?

1) Биометрическая аутентификация
2) Аутентификация по IP-адресу
3) Аутентификация на основе сертификатов
4) Аутентификация на основе знаний

89. Что означает аббревиатура SSL?

1) Secure Socket Layer
2) Secure System Login
3) Security Service Layer
4) Secure Site Lock

90. Какие из перечисленных ниже могут быть уязвимостями распределенной системы?

1. Недостатки в алгоритмах шифрования
2. Неправильная конфигурация сетевых устройств
3. Отсутствие бэкапов данных
4. Использование сетевых протоколов с ограниченной поддержкой шифрования
5. Все перечисленное

91. Что такое привилегированный доступ в распределенных системах?

1. Доступ к файлам и папкам без авторизации
2. Доступ с повышенными правами, чем у обычных пользователей
3. Доступ к защищенной информации других пользователей
4. Доступ к удаленному управлению сервером

92. Что такое атака «отказ в обслуживании» (DoS)?

1. Атака на файловую систему, цель которой — изменить содержимое файлов или получить несанкционированный доступ
2. Атака, направленная на использование уязвимости с целью получения повышенных привилегий
3. Атака на сеть, направленная на перегрузку системы или сервиса, что приводит к отказу в обслуживании
4. Атака, при которой злоумышленник устанавливает скрытый канал связи между компьютерами

93. Что такое SSL?

1. Протокол, обеспечивающий безопасную передачу данных между сервером и клиентом
2. Протокол, обеспечивающий защиту локальных файлов на компьютере
3. Протокол, обеспечивающий защиту передачи данных в локальной сети
4. Протокол, обеспечивающий безопасность работы с операционной системой

94. Какие из перечисленных ниже могут быть уязвимостями распределенной системы?

1. Недостатки в алгоритмах шифрования
2. Неправильная конфигурация сетевых устройств
3. Отсутствие бэкапов данных
4. Использование сетевых протоколов с ограниченной поддержкой шифрования
5. Все перечисленное

95. Что такое привилегированный доступ в распределенных системах?

1. Доступ к файлам и папкам без авторизации
2. Доступ с повышенными правами, чем у обычных пользователей
3. Доступ к защищенной информации других пользователей
4. Доступ к удаленному управлению сервером

96. Что такое атака «отказ в обслуживании» (DoS)?

1. Атака на файловую систему, цель которой — изменить содержимое файлов или получить несанкционированный доступ

2. Атака, направленная на использование уязвимости с целью получения повышенных привилегий
3. Атака на сеть, направленная на перегрузку системы или сервиса, что приводит к отказу в обслуживании
4. Атака, при которой злоумышленник устанавливает скрытый канал связи между компьютерами

97. Что такое SSL?

1. Протокол, обеспечивающий безопасную передачу данных между сервером и клиентом

2. Протокол, обеспечивающий защиту локальных файлов на компьютере
3. Протокол, обеспечивающий защиту передачи данных в локальной сети
4. Протокол, обеспечивающий безопасность работы с операционной системой

98. Что такое аутентификация в контексте безопасности распределенных систем?

1) Процесс подтверждения личности пользователя или устройства
2) Процесс шифрования данных для их безопасной передачи по сети
3) Процесс установления соединения между двумя узлами в сети
4) Процесс контроля доступа к ресурсам в распределенной системе

99. Какой тип атаки на безопасность распределенных систем заключается в перехвате и чтении информации, передаваемой по сети?

1) Атака межсетевого экрана
2) Атака на отказ в обслуживании
3) Атака переполнения буфера
4) Атака перехвата трафика

100. Какие меры могут быть предприняты для защиты распределенной системы от атак на отказ в обслуживании?

1) Использование криптографических алгоритмов для защиты данных
2) Разработка сетевой инфраструктуры с большой пропускной способностью
3) Использование технологии виртуализации для разделения вычислительных ресурсов
4) Установка ограничений на количество запросов к серверу от одного устройства за единицу времени

Задания в открытой форме

1. Распределенная база данных (distributed database) - это совокупность связанных баз данных, которые…
2. Основные проблемы безопасности в распределенных базах данных могут включать несанкционированный доступ к…
3. Методы защиты данных в распределенных базах данных могут включать…
4. Протоколы безопасности в распределенных базах данных обеспечивают защиту данных при…
5. Резервное копирование распределенной базы данных может осуществляться…
6. Проблема обеспечения целостности данных в распределенных базах данных возникает из-за того, что данные могут находиться на…
7. Репликация данных в распределенных базах данных осуществляется путем создания нескольких копий…
8. Обеспечение конфиденциальности данных в распределенных базах данных: Конфиденциальность данных в распределенных базах данных может быть обеспечена путем…
9. Для обеспечения безопасности в распределенных базах данных используются методы…
10. Аудит безопасности в распределенных базах данных позволяет выявить и анализировать нарушения…
11. Проблема обеспечения целостности данных в распределенных базах данных возникает из-за того, что данные…
12. Резервное копирование распределенной базы данных происходит путем создания резервных копий данных на различных…
13. Аутентификация и авторизация: для обеспечения безопасности доступа к данным используются методы аутентификации и авторизации, которые позволяют проверять подлинность…
14. Протоколы безопасности в распределенных базах данных обеспечивают защиту данных путем…
15. Основные проблемы безопасности при использовании распределенных баз данных могут включать…
16. Протоколы безопасности в распределенных базах данных могут включать…
17. Одной из основных проблем безопасности при использовании распределенных баз данных является…
18. Обеспечение целостности данных в распределенных базах данных - это процесс поддержания правильности и точности данных, хранящихся в…
19. Аудит безопасности в распределенных базах данных - это процесс мониторинга и анализа действий пользователей в…
20. Чтобы защитить данные от несанкционированного доступа, в распределенных базах данных используются различные методы защиты. Например, могут быть установлены…

Задания на установление соответствия

1. Установить соответствие

1	Домен -	А	это информация о связи между таблиц базы данных, которая описывает сколько рядов в одной таблице соответствуют рядам в другой
2	Кардинальность-	Б	это определенный выбор минимального набора атрибутов (столбцов), которые однозначно определяют кортеж (строку) в отношении (таблице)
3	Первичный ключ-	В	это онлайн-адрес сайта, место его размещения в интернете
4	Отношение-	Г	это определенный выбор минимального набора атрибутов (столбцов), которые однозначно определяют кортеж (строку) в отношении (таблице)

2. Установить соответствие

1	Правило информации	А	описание базы данных на логическом уровне должно быть представлено в том же виде, что и основные данные, чтобы пользователи, обладающие соответствующими правами, могли работать с ним с помощью того же реляционного языка, который они применяют для работы с основными данными
2	Правило гарантированного доступа	Б	В реляционной базе данных должна быть реализована поддержка недействительных значений, которые отличаются от строки символов нулевой длины, строки пробельных символов, от нуля или любого другого числа и используются для представления отсутствующих данных независимо от типа этих данных
3	Правило поддержки недействительных значений	В	Вся информация в базе данных должна быть предоставлена исключительно на логическом уровне и только одним способом - в виде значений, содержащихся в таблицах
4	Правило динамического каталога	Г	Логический доступ ко всем и каждому элементу данных (атомарному значению) в реляционной базе данных должен обеспечиваться путем использования комбинации имени таблицы, первичного ключа и имени столбца

3. Установить соответствие

1	Простой ключ-	А	сложный ключ, с большим числом столбцов, не удовлетворяющий свойству минимальности
2	Сложный (составной) ключ-	Б	ключ, содержащий только один атрибут
3	Суперключ-	В	ключ, состоящий из нескольких атрибутов
4	Искусственный или суррогатны й ключ-	Г	Искусственный или суррогатный ключ

4. Установите соответствие

1	База данных-	А	это система, в которой в одно и то же время к БД может получить доступ несколько пользователей
2	Система баз данных (СБД)-	Б	это система, в которой в одно и то же время к БД может получить доступ не более одного пользователя
3	Однопользовательская система-	В	поименованная совокупность структурированных данных относящихся к некоторой предметной области
4	Многопользовательская система-	Г	это компьютеризированная система хранения структурированных данных, основная цель которой - хранить информацию и предоставлять ее по требованию

5. Установите соответствие

1	Инфологические (семантические) модели данных	А	самые простые, широко использовались раньше
2	Даталогические модели данных	Б	используются на ранних стадиях проектирования БД.

3	Документальные модели данных	В	уже поддерживаются конкретной СУБД
4	Дескрипторные модели данных	Г	соответствуют слабоструктурированной информации, ориентированной на свободные форматы документов на естественном языке

6. Установите соответствие

1	Идентифицирующие и описательные атрибуты	А	атрибут состоит из одного компонента, его значение неделимо
2	Простые атрибуты	Б	имеют уникальное значение для сущностей данного типа и являются потенциальными ключами
3	Однозначные и многозначные атрибуты	В	вычисляется на основе значений других атрибутов
4	Производные атрибуты	Г	могут иметь соответственно одно или много значений для каждого экземпляра сущности

7. Установите соответствие

1	Реляционная алгебра-	А	сокращение (Restriction), или выборка (Selection), проекция (Projection), соединение (Join) и деление (Division) Эти операции можно разделить на базовые (выборка, проекция, декартово произведение, объединение и разность) и дополнительные (соединение, пересечение и деление).
2	Специальные реляционные	Б	это коллекция операций,

	операции-		которые принимают отношения в качестве операндов и возвращают отношение в качестве результата.
3	Унарная операция-	В	математическая операция, принимающая два аргумента и возвращающая один результат
4	Бинарная операция-	Г	это операция только с одним операндом, то есть с одним входом.

8. Установите соответствие

1	Фактографический тип БД	А	БД, разные части которой хранятся на различных серверах, объединенных в сеть
2	Документальный тип БД	Б	для данных, находящихся на одном сервере
3	Распределенный тип БД	В	включены документы или файлы разного типа: текстовые, графические, звуковые, мультимедийные
4	Централизованный тип БД	Г	сюда вносят краткую описательную информацию об объектах некоторой системы в точно определенном формате

9. Установите соответствие

1	Атомарность-	А	транзакция выполняется без обмена информацией с другими транзакциями
2	Изолированность-	Б	если результаты транзакции зафиксированы, то они хранятся в базе данных сколь угодно долго
3	Долговечность -	В	транзакция рассматривается как единое целое

10. Установите соответствие

1	Список содержимого папки	А	предоставляет все возможности для работы с папкой и вложенными файлами, включая изменение разрешений
2	Чтение и выполнение	Б	предоставляет возможность просмотра файлов и папок в текущем каталоге
3	Запись	В	предоставляет возможность открывать в данном каталоге все файлы
4	Полный доступ	Г	предоставляет возможность добавления файлов в папку без права на доступ к вложенным в него объектам, в том числе на просмотр содержимого каталога

11. Установите соответствие

1	Фильтрация	А	устанавливает кнопки скрытых списков (кнопки со стрелками) непосредственно в строку с именами столбцов
2	Критерии вычисления	Б	выделение из БД данных, отвечающих некоторому критерию
3	Критерии сравнения	В	это критерии, которые являются результатом вычисления формулы
4	Автофильтр	Г	это набор условий для поиска, используемый для извлечения данных при запросах по примеру

12. Установите соответствие

1	Проектирование внешней модели	А	собственно данные, расположенные в файлах или в страничных

			структурах, расположенных на внешних носителях информации.
2	Проектирование концептуальной модели	Б	самый верхний уровень, где каждая модель имеет свое «видение» данных
3	Проектирование внутренней модели	В	центральное управляющее звено, здесь база данных представлена в наиболее общем виде, который объединяет данные, используемые всеми приложениями, работающими с данной базой данных

13. Установите последовательность

1	Инфологическое проектирование	А	этап, который полностью связан с конкретной СУБД, рассматривает логические связи между элементами системы и физическое хранение данных
2	Датологическое проектирование	Б	сбор информации, определение парадигмы (концепции) информационной модели - способ представления, характер использования информации
3	Системный анализ программной области	В	представление БД на диске в конкретной СУБД
4	Физическое проектирование	Г	это этап, который предполагает формальное описание будущей системы и не связан с конкретной СУБД

14. Установите соответствие

1	Ограничения целостности домена	А	представляют собой ограничения, накладываемые на допустимые значения атрибута

			вследствие того, что атрибут основан на каком-либо домене
2	Ограничение целостности атрибута	Б	представляют собой ограничения, накладываемые только на допустимые значения домена
3	Ограничения целостности кортежа	В	представляют ограничения, накладываемые только на допустимые значения отдельного отношения, и не являющиеся ограничением целостности
4	Ограничения целостности отношения	Г	представляют собой ограничения, накладываемые на допустимые значения отдельного кортежа отношения, и не являющиеся ограничением целостности атрибута

15. Установите соответствие

1	DEFAULT Constraint	А	используется для быстрого создания данных базы данных
2	UNIQUE Constraint	Б	уникальная идентификация каждой строки/записи в таблице базы данных
3	PRIMARY Key	В	задает значение по умолчанию для столбца, если оно не указано
4	INDEX	Г	все значения в столбце должны быть разными

16. Установите соответствие

1	No Action	А	при удалении строки из родительской таблицы во всех ссылающихся на неё строках дочерней таблицы в атрибутах внешнего ключа записывается пустое значение
2	Cascade (каскадное взаимодействие)	Б	удаление строки из родительской таблицы запрещено, если в дочерней

			таблице есть хотя бы одна ссылающаяся на неё строка
3	Set Null	В	при удалении строки из родительской таблицы никаких действий по сохранению ссылочной целостности не предпринимается
4	No Check	Г	при удалении строки из родительской таблицы автоматически удаляются все ссылающиеся на нее строки дочерней таблицы

17. Установите соответствие

1	Прерывание	А	необратимое изменение информации, например стирание данных с диска
2	Кража, или раскрытие	Б	прекращение нормальной обработки информации, например, вследствие разрушения вычислительных средств.
3	Разрушение	В	чтение или копирование информации с целью получения данных, которые могут быть использованы либо злоумышленником, либо третьей стороной

18. Установите соответствие

1	Простой пароль	А	Пользователю выдается список из N паролей, которые хранятся в памяти компьютера в зашифрованном виде
2	Пароль однократного использования	Б	Пользователь должен дать правильные ответы на набор вопросов, хранящихся в памяти компьютера и управляемых операционной системой
3	Пароль на основе выборки	В	Пользователь вводит такой

	символов		пароль с клавиатуры после запроса, а компьютерная программа (или специальная микросхема) кодирует его и сравнивает с хранящимся в памяти эталоном
4	Метод «запрос-ответ»	Г	Пользователь выводит из пароля отдельные символы, позиции которых задаются с помощью преобразования случайных чисел или генератора псевдослучайных чисел

19. Установите соответствие

1	Конфиденциальность	А	информация и соответствующие информационные службы должны быть доступны, готовы к обслуживанию всегда, когда в этом возникает необходимость
2	Готовность	Б	(информация, на основе которой принимаются важные решения, должна быть достоверной и точной и должна быть защищена от возможных непреднамеренных и злоумышленных искажений
3	Целостность	В	засекреченная информация должна быть доступна только тому, кому она предназначена

20. Установите соответствие

1	Симметричное шифрование	А	наиболее простой вид преобразований, заключающийся в замене символов исходного текста на другие (того же алфавита)

			по более или менее сложному правилу
2	Моно- и многоалфавитные подстановки	Б	несложный метод криптографического преобразования, используемый, как правило, в сочетании с другими методами
3	Перестановки	В	метод, который заключается в наложении на открытые данные некоторой псевдослучайной последовательности, генерируемой на основе ключа
4	Гаммирование	Г	Применяется в классической криптографии, предполагает использование одной секретной единицы - ключа, который позволяет отправителю зашифровать сообщение, а получателю расшифровать его

Задания на установление правильной последовательности

1. Установите правильную последовательность шагов для защиты распределенной базы данных:
   1. Определение угроз и уязвимостей;
   2. Разработка плана защиты;
   3. Установка системы мониторинга и анализа безопасности;
   4. Реализация технических мер защиты; е. Проведение аудита безопасности.

2. Установите правильную последовательность действий для обеспечения безопасности при резервном копировании распределенной базы данных:
   1. Зашифровать резервную копию;
   2. Выбрать метод резервного копирования;
   3. Проверить целостность резервной копии;
   4. Удалить старую резервную копию;
   5. Определить частоту резервного копирования.

3. Установите правильную последовательность шагов для обеспечения безопасности при репликации распределенной базы данных:

1. Настройка системы репликации;
2. Аутентификация и авторизация доступа к реплицируемым данным;
3. Защита данных перед передачей;
4. Ограничение доступа к каналу передачи данных;
5. Мониторинг безопасности репликации.

4. Расположите следующие шаги в правильной последовательности для обеспечения безопасности распределенных баз данных:
1. Шифрование данных при передаче;
2. Использование многофакторной аутентификации;
3. Регулярные проверки на наличие уязвимостей и мониторинг безопасности;
4. Резервное копирование и восстановление данных;
5. Ограничение доступа к данным на основе ролей и прав доступа.

5. Расположите следующие шаги в правильной последовательности для защиты распределенных баз данных от кибератак:
1. Использование средств мониторинга и регистрации событий;
2. Установка и обновление программного обеспечения на всех устройствах;
3. Установка и настройка брандмауэра;
4. Ограничение доступа к системам на основе принципа "необходимый доступ";
5. Организация регулярных тренингов для персонала по безопасности информации.

6. Расположите следующие шаги в правильной последовательности для обеспечения безопасности распределенных баз данных в облачной среде:
1. Использование механизмов шифрования на уровне приложений и баз данных;
2. Определение и управление ролями и правами доступа;
3. Резервное копирование и восстановление данных;
4. Регулярная проверка на наличие уязвимостей;
5. Мониторинг облачной среды и анализ журналов событий.

7. Расположите следующие шаги в правильной последовательности для обеспечения безопасности распределенных баз данных в сети Интернет:
1. Использование средств мониторинга и обнаружения инцидентов безопасности;
2. Использование шифрования при передаче данных;
3. Ограничение доступа к базам данных через сеть Интернет;
4. Регулярные аудиты безопасности и исправление обнаруженных уязвимостей;
5. Использование механизмов аутентификации и авторизации.

8. Расположите следующие шаги в правильной последовательности для обеспечения безопасности распределенной базы данных:

1. Определить требования к безопасности базы данных.
2. Разработать план защиты данных, основываясь на требованиях к безопасности.
3. Установить доступные меры безопасности в соответствии с планом.
4. Проводить регулярную проверку на уязвимости и улучшение безопасности в соответствии с новыми требованиями.

9. Поместите следующие шаги в правильной последовательности для установления безопасной связи между клиентом и распределенной базой данных:

1. Клиент отправляет запрос на сервер с использованием безопасного протокола связи, такого как HTTPS.
2. Сервер отправляет обратно сертификат безопасности для клиента.
3. Клиент проверяет сертификат, чтобы убедиться, что он действительный и соответствует серверу.
4. Клиент и сервер обмениваются ключами шифрования, которые будут использоваться для безопасной связи.
5. Клиент и сервер начинают защищенную связь, используя ключи шифрования для зашифровки и расшифровки сообщений.

10. Расположите следующие шаги в правильной последовательности для создания безопасной копии распределенной базы данных:

1. Определить необходимые требования для создания безопасной копии, такие как время создания, место хранения и формат файла.
2. Остановить работу базы данных и начать процесс создания копии.
3. Защитить копию данных от несанкционированного доступа, используя механизмы шифрования или физические меры безопасности.
4. Восстановить работу базы данных с использованием созданной копии в случае необходимости.
5. Провести проверку целостности данных, чтобы убедиться, что копия была создана без ошибок и является полной.

11. Порядок действий при обнаружении утечки данных в распределенной базе данных:

1. Оповещение ответственных лиц
2. Проверка источника утечки
3. Оценка масштаба утечки и ее последствий
4. Принятие мер по предотвращению дальнейшей утечки
5. Восстановление утраченных данных

12. Порядок действий при аутентификации пользователей в распределенной базе данных:

1. Ввод логина и пароля

2. Проверка логина на наличие в базе данных
3. Проверка соответствия введенного пароля хэш-значению в базе данных
4. Предоставление доступа к базе данных
5. Запись лога входа пользователя

13. Порядок действий при установке защиты распределенной базы данных:
1. Оценка уровня защиты, необходимого для базы данных
2. Выбор механизмов защиты, включая шифрование, контроль доступа и мониторинг безопасности
3. Разработка стратегии резервного копирования и восстановления данных
4. Установка и настройка выбранных механизмов защиты
5. Проведение тестовых испытаний и анализ результатов

14. Установите правильную последовательность для создания безопасной распределенной базы данных:
1. Защита физического уровня (физическая безопасность серверов, кабелей и т.д.)
2. Защита логического уровня (доступ к данным, шифрование и т.д.)
3. Разработка безопасной архитектуры (сетевые настройки, управление правами доступа)
4. Резервное копирование и восстановление данных

15. Поместите следующие шаги в правильной последовательности для обеспечения безопасности распределенной базы данных:
1. Аудит безопасности и устранение уязвимостей
2. Управление правами доступа и авторизация пользователей
3. Защита данных с помощью шифрования
4. Мониторинг и журналирование событий

16. Определите правильную последовательность шагов для обеспечения безопасности при репликации данных в распределенной базе данных:
1. Защита каналов связи для передачи данных между серверами
2. Управление правами доступа на уровне базы данных и таблиц
3. Шифрование данных при передаче между серверами
4. Проверка целостности данных на каждом сервере после репликации

17. Расставьте следующие шаги в правильной последовательности для обеспечения безопасности распределенной базы данных при использовании облачных сервисов:
1. Определение требований к безопасности и выбор облачного провайдера с соответствующими сертификатами и стандартами безопасности
2. Защита данных с помощью шифрования

3. Управление правами доступа к данным и обеспечение авторизации пользователей
4. Регулярный мониторинг безопасности и устранение уязвимостей

18. Установите правильную последовательность шагов для создания безопасной распределенной базы данных в общедоступной сети:
1. Сегментация сети и настройка брандмауэра для защиты серверов базы данных
2. Защита данных с помощью шифрования
3. Управление правами доступа на уровне базы данных и таблиц
4. Мониторинг и журналирование событий для обнаружения потенциальных угроз

19. Поставьте следующие этапы в правильной последовательности для обеспечения безопасности распределенной базы данных:
1. Аутентификация пользователей
2. Шифрование данных
3. Контроль доступа
4. Резервное копирование данных
5. Мониторинг системы безопасности

20. Установите правильную последовательность следующих этапов, необходимых для защиты распределенной базы данных:
1. Оценка рисков безопасности
2. Создание политики безопасности
3. Разработка плана безопасности
4. Реализация мер безопасности
5. Оценка эффективности мер безопасности

Шкала оценивания результатов тестирования: в соответствии с действующей в университете балльно-рейтинговой системой оценивание результатов промежуточной аттестации обучающихся осуществляется в рамках 100-балльной шкалы, при этом максимальный балл по промежуточной аттестации обучающихся по очной форме обучения составляет 36 баллов, по очно-заочной и заочной формам обучения – 60 баллов (установлено положением П 02.016).

Максимальный балл за тестирование представляет собой разность двух чисел: максимального балла по промежуточной аттестации для данной формы обучения (36) и максимального балла за решение компетентностно-ориентированной задачи (6).

Балл, полученный обучающимся за тестирование, суммируется с баллом, выставленным ему за решение компетентностно-ориентированной задачи.

Общий балл по промежуточной аттестации суммируется с баллами, полученными обучающимся по результатам текущего контроля успеваемости

в течение семестра; сумма баллов переводится в оценку по 5-балльной шкале следующим образом:

Соответствие 100-балльной и 5-балльной шкал

Сумма баллов по 100-балльной шкале	Оценка по 5-балльной шкале
100-85	отлично
84-70	хорошо
69-50	удовлетворительно
49 и менее	неудовлетворительно

2.2 КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ЗАДАЧИ

1. Разработайте план обеспечения безопасности распределенной базы данных. Какие меры защиты вы предпримете, чтобы обезопасить хранящуюся информацию?
2. На основе сценария угрозы для распределенной базы данных, разработайте план действий для предотвращения и реагирования на инциденты.
3. Какие меры защиты могут быть предприняты при сетевом взаимодействии между узлами распределенной базы данных? Разработайте схему безопасного сетевого взаимодействия между узлами.
4. Разработайте политику доступа к распределенной базе данных. Какие типы доступа и права пользователей должны быть определены? Как вы будете управлять доступом к базе данных?
5. Разработайте план резервного копирования и восстановления для распределенной базы данных. Какие меры вы предпримете для защиты резервных копий и предотвращения потери данных?
6. Какие меры безопасности могут быть приняты при использовании облачных технологий для хранения распределенных баз данных? Какие риски могут возникнуть, и как их можно снизить?
7. Разработайте план мониторинга безопасности распределенной базы данных. Какие инструменты вы будете использовать для мониторинга и анализа безопасности базы данных? Как часто вы будете проводить мониторинг и анализ? Какие действия будут предприняты в случае выявления нарушений безопасности?
8. Какие меры защиты могут быть предприняты при передаче данных между узлами распределенной базы данных? Разработайте план защиты данных при передаче.
9. Какие уязвимости могут быть связаны с использованием распределенных баз данных, и как их можно предотвратить? Разработайте план управления уязвимостями для распределенной базы данных.
10. Разработайте план обучения пользователей по безопасности использования распределенной базы данных. Какие основные принципы

безопасности должны быть изучены пользователями, и как вы будете проверять их знания и соблюдение правил безопасности?

11. Задача на управление доступом: Вы являетесь администратором распределенной базы данных. Один из пользователей запросил доступ к конкретной таблице. Какие шаги вы выполните, чтобы обеспечить безопасность базы данных и предоставить пользователю необходимые права доступа?

12. Задача на аутентификацию и авторизацию: Вас попросили настроить безопасность для распределенной базы данных, которая будет использоваться несколькими пользователями. Как вы убедитесь, что только авторизованные пользователи имеют доступ к базе данных, и как вы будете проверять подлинность пользователей?

13. Задача на управление конфиденциальностью: Вы администрируете распределенную базу данных, которая содержит конфиденциальную информацию. Как вы обеспечите безопасность этой информации и защитите ее от несанкционированного доступа?

14. Задача на управление целостностью данных: Как администратор базы данных вы обнаружили, что данные в одной из таблиц были повреждены. Какие шаги вы выполните, чтобы восстановить целостность данных и предотвратить повторное нарушение безопасности?

15. Задача на управление резервными копиями: Как вы будете резервировать данные в распределенной базе данных для обеспечения безопасности и восстановления данных в случае возникновения проблем? Какие шаги вы выполните, чтобы убедиться, что резервные копии базы данных сохранены в безопасном месте и доступны для восстановления?

16. Представьте, что вы администратор базы данных. Ваша задача - настроить механизм шифрования данных на распределенной базе данных. Опишите процесс установки и настройки шифрования на каждом узле базы данных.

17. Ваша компания использует распределенную базу данных для хранения конфиденциальных данных клиентов. Однако вы обнаружили, что один из узлов базы данных был скомпрометирован. Как вы бы реагировали на эту ситуацию? Какие меры бы вы приняли, чтобы защитить данные на других узлах базы данных?

18. Ваша компания хранит большое количество конфиденциальных данных на распределенной базе данных. Как бы вы обеспечили целостность и конфиденциальность этих данных? Опишите меры, которые вы бы предприняли, чтобы защитить данные от несанкционированного доступа и модификации.

19. Представьте, что вы являетесь ответственным за резервное копирование распределенной базы данных. Как бы вы убедились в том, что все узлы базы данных регулярно резервируются и сохраняются на безопасном сервере? Опишите процесс резервного копирования и восстановления данных.

20. Ваша компания использует распределенную базу данных для хранения критически важных данных. Однако вы заметили, что некоторые узлы

базы данных работают медленно или периодически недоступны. Как бы вы решали эту проблему? Как бы вы убедились в том, что данные остаются доступными и целостность не нарушается?

Шкала оценивания решения компетентностно-ориентированной задачи: в соответствии с действующей в университете балльно-рейтинговой системой оценивание результатов промежуточной аттестации обучающихся осуществляется в рамках 100-балльной шкалы, при этом максимальный балл по промежуточной аттестации обучающихся по очной форме обучения составляет 36 баллов, по очно-заочной и заочной формам обучения – 60 (установлено положением П 02.016).

Максимальное количество баллов за решение компетентностно-ориентированной задачи – 6 баллов.

Балл, полученный обучающимся за решение компетентностно-ориентированной задачи, суммируется с баллом, выставленным ему по результатам тестирования. Общий балл промежуточной аттестации суммируется с баллами, полученными обучающимся по результатам текущего контроля успеваемости в течение семестра; сумма баллов переводится в оценку по 5-балльной шкале следующим образом:

Соответствие 100-балльной и 5-балльной шкал

Сумма баллов по 100-балльной шкале	Оценка по 5-балльной шкале
100-85	отлично
84-70	хорошо
69-50	удовлетворительно
49 и менее	неудовлетворительно

Критерии оценивания решения компетентностно-ориентированной задачи (нижеследующие критерии оценки являются примерными и могут корректироваться):

6-5 баллов выставляется обучающемуся, если решение задачи демонстрирует глубокое понимание обучающимся предложенной проблемы и разностороннее ее рассмотрение; свободно конструируемая работа представляет собой логичное, ясное и при этом краткое, точное описание хода решения задачи (последовательности (или выполнения) необходимых трудовых действий) и формулировку доказанного, правильного вывода (ответа); при этом обучающимся предложено несколько вариантов решения или оригинальное, нестандартное решение (или наиболее эффективное, или наиболее рациональное, или оптимальное, или единственно правильное решение); задача решена в установленное преподавателем время или с опережением времени.

4-3 балла выставляется обучающемуся, если решение задачи демонстрирует понимание обучающимся предложенной проблемы; задача решена типовым способом в установленное преподавателем время; имеют

место общие фразы и (или) несущественные недочеты в описании хода решения и (или) вывода (ответа).

2-1 балла выставляется обучающемуся, если решение задачи демонстрирует поверхностное понимание обучающимся предложенной проблемы; осуществлена попытка шаблонного решения задачи, но при ее решении допущены ошибки и (или) превышено установленное преподавателем время.

0 баллов выставляется обучающемуся, если решение задачи демонстрирует непонимание обучающимся предложенной проблемы, и (или) значительное место занимают общие фразы и голословные рассуждения, и (или) задача не решена.