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 распределённых систем

(наименование учебной дисциплины)

10.04.01 Информационная безопасность, направленность (профиль) «Защищённые информационные системы»

(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 систем

1. Что такое распределенная система и как она отличается от централизованной системы?
2. Какие угрозы могут возникнуть в распределенных системах и как их можно предотвратить?
3. Какие виды аутентификации используются в распределенных системах?
4. Какие методы обнаружения и защиты от атак DDoS используются в распределенных системах?

Тема 2. Структура связи в распределенных системах

1. Какие виды протоколов связи используются в распределенных системах?
2. Что такое маршрутизация и как она работает в распределенных системах?
3. Как обеспечивается надежность связи между узлами в распределенных системах?
4. Что такое транзакции и как они используются в распределенных системах для обеспечения целостности 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 систем

1. Когда появилась первая распределенная система и какие были проблемы безопасности?
2. Какие атаки на распределенные системы стали наиболее распространенными в первые годы их существования?
3. Как развивалась технология криптографии в контексте безопасности распределенных систем?
4. Какие протоколы и алгоритмы были разработаны для обеспечения безопасности в распределенных системах?

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«Средства защиты распределенных систем»

1. Какие методы шифрования используются для защиты данных в распределенных системах?
2. Какие методы аутентификации и авторизации используются для защиты доступа к распределенным системам?
3. Какие инструменты используются для обнаружения и предотвращения атак на распределенные системы?
4. Какие методы защиты от DDoS-атак используются в распределенных системах?

Лабораторная работа № 3«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 №4«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:

6-5 баллов (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.

4-3 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.

2-1 балла (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. Основные угрозы безопасности при работе с распределенными системами включают атаки на …
2. SSL/TLS - это протоколы шифрования, используемые для …
3. Атаки на отказ в обслуживании (DDoS) - это атаки, которые заключаются в …
4. Управление доступом - это процесс определения, кто имеет право на …
5. Блокчейн - это технология, которая позволяет создавать …
6. Распределенная система - это сеть компьютеров, которые работают…
7. Типы угроз, которые могут возникнуть при работе с распределенными системами, включают в себя…
8. Основные принципы криптографии включают в себя…
9. Методы аутентификации пользователей, которые могут быть использованы для защиты распределенных систем от несанкционированного доступа, включают в себя…
10. Атаки на отказ в обслуживании (DDoS) могут привести…
11. Технология блокчейн используется для обеспечения…
12. Использование виртуализации может увеличить уязвимости распределенных систем, но можно принять меры, такие как…
13. Система обнаружения вторжений (IDS) используется для защиты распределенных систем, путем…
14. Для защиты от атак на отказ в обслуживании (DDoS) используются различные инструменты и технологии, включая:…
15. Для защиты распределенных систем от несанкционированного доступа используются различные методы аутентификации пользователей, такие как…
16. Целостность данных играет важную роль в…
17. Использование виртуализации может повысить уязвимость распределенных систем, поскольку виртуальные среды…
18. Система баз данных-это…
19. Для защиты ИС от фишинга можно использовать различные методы, включая обучение сотрудников компании основам безопасности информации, использование…
20. Для защиты ИС от сетевых атак можно применять различные меры, включая использование механизмов защиты периметра, таких как …

Задания на установление соответствия

1. Установите соответствие между названием объекта операционной системы и его назначением

1	дескриптор сегмента	А	Вытесняется самая старая страница, к которой не было обращений в предыдущем временном интервале
2	указатель адреса	Б	Информация о размещении данных в памяти
3	дескриптор страницы	В	Информация о статусе области физической памяти фиксированного размера
4	i-узел	Г	Информация о логической структуре постоянной памяти

2. Установить соответствие названия ОС её назначению

1	NetWare	А	Серверная операционная система для поддержки виртуальных машин, включая виртуальные машины на Linux.
2	LANtastic	Б	Серверная операционная система с объектно-ориентированный интерфейсом OS/2 для создания мощного набора графических средств администратора.
3	Windows Server 2019	В	Сетевая операционная система и набор сетевых протоколов для взаимодействия с компьютерами-клиентами, подключёнными к сети
4	LAN server	Г	Сетевая операционная система для DOS, Windows,OS/2 с поддержкой технологии Ethernet, ARCNET и Token Ring

3. Установить соответствие принципами распределения памяти и их недостатками и их достоинствами

1	эффективное использование памяти	А	С подвижными разделами является
2	простота реализации	Б	С динамическими границами.
3	большая гибкость	В	С фиксированными границами
4	малые временные затраты	Г	С фиксированными разделами

4. Установите соответствие между принципами распределения памяти и их недостатками

1	ограниченность уровней мультипрограммирования	А	С подвижными разделами является

2	отсутствие гибкости	Б	С динамическими границами.
3	значительные временные затраты	В	С фиксированными границами
4	фрагментация памяти	Г	С фиксированными разделами

5. Установите соответствие между названием метода вытеснения страниц и его описанием

1	WSClock	А	Вытесняется самая старая страница, к которой не было обращений в предыдущем временном интервале
2	LRU	Б	Вытесняется самая дальняя по списку страница
3	FIFO	В	Вытесняется страница с комбинацией критериев времени и очерёдности
4	«вторая попытка»	Г	Вытесняется страница, к которой не было обращений по крайней мере в течение одного тика системных часов

6. Установить соответствие топологии сети её характеристике

1	Общая шина	А	Каждая рабочая станция сети соединяется с несколькими другими рабочими станциями этой же сети
2	Звезда	Б	В данной топологии все рабочие станции соединены друг с другом с помощью центрального концентратора
3	Кольцо	В	В основе топологии лежит общий кабель (магистраль), к которому подсоединяются все рабочие станции
4	Комбинированные решения	Г	Топология, в которой каждая рабочая станция соединяется только с двумя соседними

7. Установите соответствие между типом операционной системы и её назначением

1	Реального времени	А	Наличие высоких требований по стабильности работы
2	Пакетной обработки	Б	Управление технологическими процессам
3	Многозадачная с вытесняющей многозадачностью	В	Работа с множеством пользователей
4	Многозадачная с невытесняющей многозадачностью	Г	Высокопроизводительные вычисления

8. Система защиты на Pentium поддерживает четыре уровня защиты, где уровень 0 является наиболее привилегированным, а уровень 3 — наименее привилегированным установите соответствие

1	Ядро	А	Уровень 3
2	Системные узлы	Б	Уровень 1
3	Библиотеки совместного доступа	В	Уровень 2
4	пользовательские программы	Г	Уровень 4

1. Установите соответствие между названием системных вызовов и их описанием

1	Create	А	Системный вызов позволяет системе прочитать в оперативную память атрибуты файла и список дисковых адресов для быстрого доступа к содержимому файла при последующих вызовах.
2	Read	Б	Когда все операции с файлом закончены, файл следует закрыть, чтобы освободить пространство во внутренней таблице системы.
3	Open	В	Этот системный вызов объ- являет о появлении нового файла и позволяет установить некоторые его атрибуты.
4	Close	Г	Чтение данных из файла.

2. Установите соответствие между названием объекта операционной системы и его назначением

1	Write	А	Операция устанавливает указатель текущей позиции на определенное место файла. Последующие данные будут считаны из этой позиции и записаны в нее.
2	Append	Б	Запись данных в файл, также в текущую позицию в файле. Если текущая позиция находится в конце файла, размер файла автоматически увеличивается.

3	Seek	В	Некоторые атрибуты файла могут устанавливаться пользователем после создания файла. Этот системный вызов предоставляет такую возможность.
4	Set attributes	Г	Этот системный вызов представляет собой усеченную форму вызова write. Он может только добавлять данные к концу файла. Данный вызов в операционных системах может отсутствовать

3. Установите соответствие с названием разделяемой памятью системных вызовов и их описанием

1	shmget	А	Служит для управления разнообразными параметрами, связанными с существующим сегментом
2	shmat	Б	Создает новый сегмент разделяемой памяти или находит существующий сегмент с тем же ключом
3	shmdt	В	Отключает от виртуальной памяти ранее подключенный к ней сегмент с указанным виртуальным адресом начала
4	shmctl	Г	Подключает сегмент с указанным дескриптором к виртуальной памяти обращающегося процесса

4. Установите соответствие между названием видов памяти и его описанием

1	Оперативная память	А	Это промежуточное запоминающее устройство, используемое для ускорения обмена между процессором и RAM. В современных процессорах используется несколько уровней кэш-памяти.
2	Регистры	Б	Это электронная память предназначена для длительного сохранения программы и данных. Используется оно для чтения данных. Как правило, эта информация записывается при изготовлении компьютера и служит для начальной загрузки оперативной системы, проверки работоспособности компьютера.
3	Кэш-память	В	Это устройства, где размещены данные, который процессор обрабатывает в определенный промежуток времени.
4	Постоянная память	Г	Это сверхскоростная память процессора. Они сохраняют адрес команды, саму команду, данные для её выполнения и результат.

5. Установите соответствие между названием объекта операционной системы и его назначением

1	UFS	А	Это абстрактный уровень поверх более конкретной файловой системы
2	VFS	Б	Описание способов взаимодействия одной компьютерной программы с другими
3	API	В	Название файловой системы, использовавшейся в SCO Unix, System V и некоторых других ранних вариантах Unix.

6. Установите соответствие между названием задач алгоритма планирования и его описание

1	Равноправие	А	Минимизация времени, затрачиваемого на ожидание обслуживания и обработку задачи
2	Использование процессора	Б	Поддержка постоянной занятости процессора
3	Время отклика	В	Предоставление каждому процессу справедливой доли процессорного времени
4	Оборотное время	Г	Быстрая реакция на запросы

7. Установите соответствие между названием условий и его описание

1	Условие взаимного исключения	А	можно исключить, позволяя ОС отнимать у процесса ресурсы
2	Условие ожидания	Б	можно подавить путем разрешения неограниченного разделения ресурсов
3	Условие отсутствия перераспределения	В	можно исключить, предотвращая образование цепи запросов
4	Условие кругового ожидания	Г	можно подавить, предварительно выделяя ресурсы

8. Установите соответствие между названием фреймов и их описанием

1	page frame	А	Диспетчер виртуальной памяти может быстро и относительно легко удовлетворить программные прерывания
2	page fault	Б	Виртуальная страница памяти, отображаемая на физическую страницу
3	Pagefile	В	Содержит объекты, которые могут быть при необходимости выгружены на диск
4	paged pool	Г	Это файл подкачки операционной системы Windows. При нехватке оперативной памяти Windows резервирует определенное место на жестком диске и использует его для увеличения своих возможностей.

9. Установите соответствие между названием реализаций файлов и их описанием

1	Неразрывные файлы	А	Метод отслеживания принадлежности блоков диска файлам заключался в связывании с каждым файлом структуры данных
2	Списки	Б	Простейшей схемой выделения файлам определенных блоков на диске является система, в которой файлы представляют собой наборы последовательных соседних блоков диска
3	Список с индексацией	В	Метод размещения файлов состоит в представлении каждого файла в виде однонаправленного списка блоков диска
4	I-узлы	Г	Оба недостатка предыдущей схемы организации файлов в виде списков могут быть устранены, если указатели на следующие блоки хранить не прямо в блоках, а в отдельной таблице, загружаемой в память, элементы которой хранят ссылку на физический блок диска и на элемент таблицы, соответствующий очередному блоку файла

10. Установите соответствие между названием регистров и их описанием

1	Регистр данных	А	Использовался для указания номера цилиндра, с которого необходимо выполнить предкомпенсацию
2	Регистр ошибок	Б	Содержит количество секторов для операции записи или считывания
3	Регистр предкомпенсации	В	Используется при выполнении операций чтения или записи сектора в программном режиме ввода/вывода
4	Регистр счетчика секторов	Г	Определяет состояние НЖМД после выполнения операции

11. Установите соответствие между названием методов скрытия дефектов и их описанием

1	Метод резервного сектора	А	При этом методе дорожка содержащая дефект считается нерабочей и "не замечается" контроллером диска
2	Метод резервной дорожки	Б	Суть метода заключается в том, что на каждой дорожке накопителя размещается дополнительный, недоступный в обычном режиме работы, сектор и при обнаружении дефекта в каком-либо рабочем секторе дорожки, вместо него включается резервный
3	Метод пропуска дефектной дорожки	В	Такой метод позволяет исключить всю дорожку при обнаружении на ней дефектов
4	Метод пропуска дефектного сектора	Г	Этот метод применим только к накопителям, использующих режим трансляции физических параметров в логические

12. Установите соответствие между названием системных вызовов и их описанием

1	semget	А	для манипулирования значениями семафоров
2	semop	Б	для выполнения разнообразных управляющих операций над набором семафоров
3	semctl	В	для создания и получения доступа к набору семафоров

13. Установить соответствие технических каналов утечки информации:

1. Прямой акустический (окна, двери, щели, проемы)	a. Электронные устройства перехвата речевой информации с датчиками микрофонного типа при условии неконтролируемого доступа к ним посторонних лиц
2. Акусто-оптический (через оконные стекла)	b. Лазерные акустические локационные системы, находящиеся за пределами КЗ
3. Акусто-электрический (через соединительные линии ВТСС)	c. Специальные низкочастотные усилители, подсоединенные к соединительным линиям ВТСС, обладающие «микрофонным» эффектом
4. Акусто-электромагнитный (параметрический)	d. Прослушивание разговоров, ведущихся в помещении без применения технических средств посторонними лицами

14. Установить соответствие дальности подавления диктофонов:

1. Аналоговые диктофоны	a. 5–6 м.
2. Цифровые диктофоны	b. Не более 1,5 м
3. Аналоговые диктофоны в металлическом корпусе	c. 4–5 м
4. Современные цифровые диктофоны в металлическом корпусе	d. Практически не подавляются

15. Установить соответствие

1. I группа	a. Блокираторы представляют собой генераторы помех с ручным управлением, обеспечивающие подстановку заградительной помехи в диапазоне частот работы базовых станций соответствующего стандарта (т.е. в диапазоне рабочих частот приемников телефонов сотовой связи). Помеха приводит к срыву управления сотовым телефоном базовой станции (потеря сети) и следовательно невозможности установления связи и передачи информации.
2. II группа	b. В своем составе кроме передатчика помех имеют еще специальный приемник, обеспечивающий прием сигналов в диапазонах частот работы передатчиков телефонных аппаратов соответствующего стандарта. Учитывая, что вся система сотовой связи работает в дуплексном режиме, специальный приемник используется как средство автоматического управления передатчиком помех. При обнаружении сигнала в одном из диапазонов частот приемник выдает сигнал управления на включения передатчика заградительных помех соответствующего диапазона частот. При пропадании сигнала приемник выдает сигнал управления на выключение сигнала помех соответствующего диапазона.
3. III группа	c. Так называемые «интеллектуальные блокираторы связи». На примере GSM: приемник блокиратора в течение короткого времени (примерно 300 мкс) обнаруживает в КЗ излучение входящего в связь мобильного телефона, вычисляет номер частотного канала и временной слот, выделяемый данному телефону.

16. Установить соответствие:

1. Косвенные каналы	a. связанные с доступом к элементам АСОД, но не требующие изменения компонентов системы.
2. Прямые каналы	b. не связанные с физическим доступом к элементам АСОД.
3. Прямые каналы	c. связанные с доступом к элементам АСОД и изменением структуры компонентов АСОД.

17. Установить соответствие:

1. Нарушитель	a. намеренно идущий на нарушение из корыстных побуждений.
2. Злоумышленник	b. лицо, предпринявшее попытку выполнения запрещенных действий по ошибке, незнанию или осознанно со злым умыслом или без такового, и использующее для этого различные возможности, методы и средства.
3. взломщик	c. Лицо, которое с корыстными целями осуществляет несанкционированный доступ к данным или программам.

18. Установить соответствие нарушителей по уровням знания АСОД:

1. 1 уровень	a. Обладает высоким уровнем знаний и опытом работы с техническими средствами системы и ее обслуживания.
2. 2 уровень	b. Знает функциональные особенности АСОД, основные закономерности формирования в нестандартных массивах данных и потоков запросов к ним. Умеет пользоваться штатными средствами.
3. 3 уровень	4. Знает структуру, функции и механизмы действия средств защиты, их слабые и сильные стороны.
5. 4 уровень	6. Обладает уровнем знаний в области программирования и вычислительных технологий, проектирования и эксплуатации АСОД.

19. Установить соответствие нарушителей по времени действия:

1. 3 уровень	a. В период неактивности компонентов системы (нерабочее время, перерывы, ремонт и т.п.).
2. 2 уровень	b. Во время функционирования АСОД (во время работы компонентов системы).
3. 1 уровень	c. Как в процессе функционирования АСОД, так и в период неактивности системы.

20. Установить соответствие нарушителей по уровням возможностей (используемым методам и вопросам):

1. 1 уровень	a. Применяющие пассивные средства (технические средства перехвата без модификации компонентов системы).
2. 2 уровень	b. Применяющие только агентурные методы получения сведений
3. 3 уровень	c. Использующие только штатные средства и недостатки системы защиты, их сильные и слабые стороны.
4. 4 уровень	d. Применяющие методы и действия активного воздействия (модификация и подключение дополнительных технических устройств).

Задания на установление правильной последовательности

1. Установите правильную последовательность этапов оценки рисков в распределенных системах:

a) Идентификация активов и уязвимостей;

b) Оценка уровня угрозы;

c) Оценка вероятности наступления угрозы;

d) Оценка возможных последствий угрозы;

e) Оценка уровня риска;

f) Разработка и реализация мер по управлению рисками.

2. Установите правильную последовательность этапов реализации контроля доступа в распределенных системах:

a) Идентификация пользователей и ресурсов;

b) Аутентификация пользователей и авторизация доступа к ресурсам;

c) Установка прав доступа;

d) Мониторинг доступа;

e) Аудит доступа.

3. Установите правильную последовательность этапов реализации защиты информации в распределенных системах:

a) Оценка уровня угрозы и риска;

b) Разработка и реализация мер по управлению рисками;

c) Использование шифрования данных;

d) Установка мер защиты на уровне операционной системы;

e) Установка мер защиты на уровне приложений.

4. Установите правильную последовательность этапов процесса резервного копирования данных в распределенных системах:

a) Определение частоты создания резервных копий;

b) Определение места хранения резервных копий;

c) Выбор метода резервного копирования;

d) Создание резервных копий;

e) Проверка целостности и доступности резервных копий.

5. Установите правильную последовательность этапов реализации мер по обеспечению физической безопасности в распределенных системах:

a) Идентификация критических зон;

b) Установка систем видеонаблюдения и контроля доступа;

c) Установка физических барьеров;

d) Определение места расположения серверных комнат;

e) Определение места расположения резервных источников питания.

6. Установите правильную последовательность шагов для установки и настройки брандмауэра на сервере, чтобы обеспечить безопасность распределенной системы:

- Скачать и установить необходимое ПО
- Настроить правила брандмауэра
- Запустить брандмауэр и добавить его в автозапуск
- Протестировать брандмауэр, используя уязвимости, известные для вашей системы
- Создать резервную копию настроек брандмауэра

7. Установите правильную последовательность действий для защиты распределенной системы от атак, использующих уязвимости веб-приложений:

a) Сканирование веб-приложений на уязвимости

b) Исправление найденных уязвимостей

c) Определение правильных настроек фаервола для предотвращения атак

d) Установка системы обнаружения вторжений

e) Регулярное обновление программного обеспечения системы

8. Установите правильную последовательность действий для обеспечения безопасности данных, передаваемых между узлами распределенной системы:

a) Выбор протокола безопасности передачи данных

b) Установка и настройка сертификатов безопасности

c) Защита паролей и логинов

d) Реализация защиты от атак межсетевого экрана

e) Настройка шифрования данных

9. Установите правильную последовательность действий для защиты распределенной системы от атак на уровне приложений:

a) Сканирование приложений на уязвимости

b) Установка системы обнаружения вторжений

c) Исправление найденных уязвимостей

d) Проверка наличия несанкционированных сценариев веб-приложений

e) Регулярное обновление программного обеспечения системы

10. Установите правильную последовательность действий для обеспечения безопасности распределенной системы при использовании облачных сервисов:

a) Определение рисков использования облачных сервисов
b) Выбор надежного облачного провайдера
c) Настройка управления доступом к данным
d) Настройка механизма резервного копирования
e) Регулярный мониторинг безопасности системы

11. Расставьте действия по установлению безопасной связи между клиентом и сервером:
a) Клиент посылает запрос на подключение к серверу
b) Сервер отправляет клиенту сертификат безопасности
c) Клиент проверяет подлинность сертификата
d) Клиент и сервер обмениваются сеансовым ключом
e) Клиент и сервер начинают обмен данными с использованием сеансового ключа

12. Расставьте действия по обеспечению безопасности данных в распределенной системе:
a) Зашифровать передаваемые данные
b) Аутентифицировать пользователей
c) Ограничить доступ к ресурсам системы на основе ролей и прав
d) Установить межсетевые экраны для блокировки нежелательного трафика
e) Установить обновления безопасности для программного обеспечения системы

13. Расставьте действия по противодействию атаке DDoS на распределенную систему:
a) Определить источник атаки и заблокировать его IP-адрес
b) Установить межсетевые экраны для блокировки входящего трафика
c) Использовать средства для фильтрации трафика и отбраковки подозрительных пакетов
d) Использовать технологии балансировки нагрузки для равномерного распределения трафика по серверам
e) Повысить пропускную способность сети, чтобы выдержать большой объем трафика

14. Установите правильную последовательность действий для обеспечения безопасности в процессе аутентификации пользователей в распределенной системе:
a. Пользователь вводит логин и пароль
b) Система проверяет правильность логина и пароля
c) Система выдает токен для доступа к ресурсам
d) Пользователь получает доступ к ресурсам с помощью токена

15. Установите правильную последовательность действий для защиты данных в распределенной системе:
a) Данные шифруются с помощью алгоритма шифрования
b) Зашифрованные данные передаются по сети
c) Получатель расшифровывает данные с помощью ключа

d) Данные сохраняются в зашифрованном виде на диске

16. Установите правильную последовательность действий для предотвращения атак на распределенную систему:

a) Идентифицирование потенциальных уязвимостей в системе
b) Разработка плана мер по устранению уязвимостей
c) Реализация мер безопасности в системе
d) Мониторинг и обновление мер безопасности в системе

17. Установите правильную последовательность действий для обеспечения физической безопасности распределенной системы:

a) Ограничение доступа к серверной комнате
b) Установка системы видеонаблюдения и контроля доступа
c) Резервное копирование данных
d) Регулярная проверка оборудования и устройств на наличие уязвимостей

18. Установите правильную последовательность действий для обеспечения защиты от внешних атак на распределенную систему:

a. Установка брандмауэра для контроля входящего и исходящего трафика
c. Установка программного обеспечения для обнаружения вредоносных программ
d. Установка системы обнаружения вторжений
e. Регулярное обновление программного обеспечения и операционной системы.

19. Установите последовательность действий для обеспечения безопасности данных в распределенной системе:

a) Разработка политики безопасности
b) Разработка механизмов шифрования данных
c) Установка мер безопасности на всех уровнях системы
d) Создание резервных копий данных
e) Оценка эффективности мер безопасности
f) Регулярное обновление и патчинг системы
g) Обучение пользователей правилам безопасности

20. Установите правильную последовательность действий для мониторинга безопасности в распределенной системе:

a) Разработка политики мониторинга безопасности
b) Установка мониторинговых инструментов на всех уровнях системы
c) Определение критических ресурсов для мониторинга
d) Определение пороговых значений для оповещений о нарушениях безопасности
e) Регулярный анализ и интерпретация данных мониторинга
f) Принятие мер по предотвращению нарушений 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. Компания X разрабатывает приложение для хранения и обработки конфиденциальных данных своих клиентов. Какие меры безопасности должны быть предприняты для защиты этих данных? Какие риски могут возникнуть при неправильной реализации мер безопасности?
2. Компания Y использует облачное хранилище для хранения своих данных. Какие меры безопасности должны быть предприняты для защиты данных в облаке? Какие риски могут возникнуть при неправильной реализации мер безопасности?
3. Компания Z использует открытый Wi-Fi для своих сотрудников во время командировок. Какие меры безопасности должны быть предприняты для защиты конфиденциальной информации компании? Какие риски могут возникнуть при неправильной реализации мер безопасности?
4. Компания A рассматривает возможность использования биометрической аутентификации для входа в свою систему. Какие

риски могут возникнуть при использовании такого метода аутентификации? Какие меры безопасности должны быть предприняты для защиты данных при использовании биометрической аутентификации?

5. Компания В использует систему виртуальных машин для своих сотрудников. Какие меры безопасности должны быть предприняты для защиты данных в виртуальных машинах? Какие риски могут возникнуть при неправильной реализации мер безопасности?
6. Вы работаете в крупной компании, которая использует распределенную систему для хранения и обработки данных. Один из ваших коллег сообщил вам о том, что он получил письмо от неизвестного отправителя, в котором говорится о возможной утечке конфиденциальной информации из вашей компании. Что вы сделаете в первую очередь, чтобы убедиться в безопасности системы?
7. Ваша компания использует распределенную систему для хранения и обработки данных клиентов. Однако, вы заметили, что произошла утечка некоторой конфиденциальной информации. В результате, несколько клиентов потеряли доверие к вашей компании. Какие меры вы предпримете, чтобы восстановить доверие клиентов и защитить данные в будущем?
8. Вы работаете в команде, которая отвечает за безопасность распределенной системы вашей компании. Один из ваших коллег предложил изменить пароли для всех пользователей системы раз в месяц. Однако, другой коллега считает, что это неэффективно и может негативно повлиять на производительность. Как вы решите эту ситуацию и какие меры безопасности вы предложите вместо изменения паролей?
9. Ваша компания решила использовать облачные технологии для хранения и обработки данных. Какие меры безопасности вы предложите для защиты данных и обеспечения безопасности в облаке?
10. Ваша компания использует распределенную систему для обработки крупных объемов данных. Какие меры безопасности вы предложите для защиты от DDoS-атак и других угроз, связанных с доступом к системе?
11. Задача на анализ рисков: Вам поручено провести анализ рисков для распределенной системы, состоящей из нескольких серверов, на которых хранится конфиденциальная информация. Какие шаги вы будете предпринимать для выполнения этого задания?
12. Задача на выбор метода шифрования: Вы разрабатываете распределенную систему, которая будет использоваться для передачи конфиденциальной информации. Какой метод шифрования вы выберете и почему?
13. Задача на оценку угроз: Ваша компания использует распределенную систему для хранения и обработки конфиденциальной информации. Какие угрозы могут возникнуть для безопасности этой системы и как можно защититься от них?

14. Задача на выбор аутентификационного метода: Вы разрабатываете распределенную систему, которая будет использоваться несколькими пользователями. Какой метод аутентификации вы выберете и почему?
15. Задача на планирование реагирования на инциденты: Ваша компания использует распределенную систему, которая хранит и обрабатывает конфиденциальную информацию. Как вы спланируете реагирование на возможные инциденты, такие как взлом системы или утечка данных? Какие шаги вы предпримете, чтобы свести к минимуму потенциальный ущерб?
16. Компания X использует распределенную систему для обработки своих данных. Однако, некоторые сотрудники компании заметили, что их персональные данные также обрабатываются в этой системе. Какие меры безопасности необходимо принять для защиты персональных данных при использовании распределенных систем?
17. Компания Y использует распределенную систему для обработки своих финансовых данных. Однако, некоторые сотрудники компании украли логин и пароль от учетной записи администратора, имеющей доступ к этой системе. Какие меры безопасности необходимо принять для предотвращения таких инцидентов?
18. Компания Z использует распределенную систему для хранения и обработки своих клиентских данных. Однако, система была атакована злоумышленниками, которые украли большое количество этих данных. Какие меры безопасности необходимо принять, чтобы избежать подобных инцидентов в будущем?
19. Компания A использует распределенную систему для обработки своих данных. Однако, некоторые сотрудники компании заметили, что их персональные данные также обрабатываются в этой системе. Какие законодательные нормы необходимо учитывать при обработке персональных данных в распределенных системах?
20. Компания B использует распределенную систему для хранения и обработки своих финансовых данных. Однако, некоторые сотрудники компании заметили, что данные на серверах, находящихся в другой стране, не зашифрованы. Какие меры безопасности необходимо принять для защиты данных при использовании распределенных систем в других странах?
21. Компания решила перевести свою ИТ-инфраструктуру в облако. Какие меры безопасности необходимо принять для защиты данных компании?
22. Разработчик написал код для распределенной системы, однако забыл установить защиту от DDoS-атак. Что следует сделать, чтобы избежать таких атак?
23. Компания хочет сократить расходы на безопасность распределенной системы. Какие меры безопасности можно опустить, чтобы сэкономить деньги, и какие меры необходимо сохранить в любом случае?

24. В компании имеется несколько серверов, расположенных в разных странах. Какие меры безопасности необходимо принять, чтобы защитить данные, хранящиеся на этих серверах?
25. Разработчик написал код для распределенной системы, однако забыл установить защиту от внедрения вредоносного кода. Что следует сделать, чтобы избежать такой угрозы?
26. Компания хочет использовать блокчейн-технологии для хранения данных. Какие меры безопасности необходимо принять, чтобы защитить данные, хранящиеся на блокчейн-платформе?
27. Разработчик написал код для распределенной системы, однако забыл установить защиту от SQL-инъекций. Что следует сделать, чтобы избежать такой угрозы?
28. Компания использует открытый исходный код для своей распределенной системы. Какие меры безопасности необходимо принять, чтобы защитить систему от уязвимостей в коде с открытым исходным кодом?
29. Разработчик написал код для распределенной системы, однако забыл установить защиту от фишинг-атак. Что следует сделать, чтобы избежать такой угрозы?
30. Компания хочет использовать мультифакторную аутентификацию для своей распределенной системы. Какие меры безопасности необходимо принять, чтобы защитить данные, используемые для мультифакторной аутентификации?

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.