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

Организация работ по обеспечению безопасности в информационных системах
(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. Кадровая политика в области информационной безопасности

1. Каким образом оценивается профессиональная компетентность и квалификация сотрудников в области информационной безопасности?
2. Каким образом осуществляется контроль за выполнением политики информационной безопасности среди сотрудников?
3. Какие критерии и требования устанавливаются при наборе персонала в области информационной безопасности?
4. Каким образом организация проводит проверку сотрудников на доступ к конфиденциальной информации и мониторит их действия в системах информационной безопасности?

Тема 2. Методы планирования работ по обеспечению информационной безопасности

1. Каким образом определяются уязвимости и риски в системах информационной безопасности организации, и как они учитываются в планах работ?
2. Какие инструменты или методики используются для анализа уязвимостей и оценки рисков информационной безопасности в вашей организации?
3. Как организация определяет ресурсы (бюджет, персонал, технические решения и т.д.), необходимые для реализации планов обеспечения информационной безопасности?
4. Каким образом взаимодействует отдел информационной безопасности с другими подразделениями организации в процессе планирования и реализации работ по обеспечению информационной безопасности?

Тема 3. Методы решения проблемных ситуаций в коллективе

1. Каким образом вы взаимодействуете с другими членами коллектива при решении проблемных ситуаций?
2. Какие организационные методы решения проблемных ситуаций в коллективе вам знакомы?
3. Какие технические методы могут быть использованы для решения проблемных ситуаций в коллективе?
4. Какие преимущества и недостатки Вы видите в применении организационных, инженерно-технических, технических и программно-аппаратных методов решения проблемных ситуаций в коллективе?

Тема 4. Применение нормативно-правовых актов при организации работ по защите информации

1. Какие нормативно-правовые акты регулируют организацию работ по защите информации?

2. Какие основные положения содержатся в этих нормативно-правовых актах?
3. Какие меры и документы необходимо разработать и применить в соответствии с нормативно-правовыми актами при организации работ по защите информации?
4. Какие меры предусмотрены в нормативно-правовых актах для обеспечения охраны секретных материалов и защиты информации?

Тема 5. Управление разработкой информационных систем

1. Какие этапы включает процесс управления разработкой информационных систем?
2. Каким образом определяются требования к разрабатываемым информационным системам и какие методы используются для их анализа и документирования?
3. Каким образом осуществляется тестирование, отладка и оптимизация информационных систем перед их внедрением?
4. Как осуществляется контроль над сроками, бюджетом и ресурсами проекта при управлении разработкой информационных систем? .

Тема 6. Формирование комплекса мер по обеспечению информационной безопасности

1. Что такое концепция безопасности и какие основные принципы она включает?
2. Какие организационные меры могут быть применены для обеспечения информационной безопасности на предприятии?
3. Каким образом оценивается эффективность мер по обеспечению информационной безопасности на предприятии?
4. Какие рекомендации можно предложить для организации комплекса мер по обеспечению информационной безопасности на предприятии?

Тема 7. Порядок разработки модели угроз при построении информационных систем

1. Какие этапы включает процесс разработки модели угроз?
2. Какие виды угроз могут быть включены в модель угроз информационных систем?
3. Какие методы можно использовать для выявления и анализа угроз безопасности информации и уязвимостей программного обеспечения?
4. Какие основные этапы процесса разработки модели угроз следует учесть?

Критерии оценки:

3 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 ПРАКТИЧЕСКИХ РАБОТ

Практическая работа № 1 «Система анализа рисков и проверки политики информационной безопасности предприятия»

1. Что такое система анализа рисков в контексте информационной безопасности предприятия?
2. Что такое политика информационной безопасности предприятия и зачем она необходима?
3. Каким образом проводится проверка политики информационной безопасности предприятия?
4. Какие меры могут быть предприняты для снижения выявленных рисков и улучшения политики информационной безопасности на предприятии?

Практическая работа № 2«Моделирование объектов защиты»

1. Какие основные цели и задачи моделирования объектов защиты?
2. Какие методы и техники могут быть применены при моделировании объектов защиты?
3. Каким образом моделирование объектов защиты может быть использовано в анализе рисков информационной безопасности?
4. Какие преимущества и ограничения может иметь моделирование объектов защиты в контексте оценки информационных рисков?

Практическая работа № 3«Организационная культура и управление конфликтами»

1. Что такое организационная культура и почему она важна для управления коллективом?

2. Какие основные элементы организационной культуры можно выделить?

3. Как организационная культура может влиять на эффективность работы коллектива?

4. Какие меры можно предпринять для профилактики конфликтов в организации и создания благоприятной организационной культуры?

Практическая работа №4«Работа с нормативно-правовыми документами»

1. Какие нормативно-правовые документы регулируют деятельность организации в области информационной безопасности?

2. Как должно быть организовано хранение и обновление нормативно-правовых документов в организации?

3. Какие меры принимаются для контроля соответствия действий сотрудников нормативно-правовым требованиям в области информационной безопасности?

4. Какие проблемы и трудности могут возникнуть при работе с нормативно-правовыми документами в организации и как они решаются?

Практическая работа №5«Разработка организационных и технических мер по инженерно-технической защите информации»

1. Какие принципы следует учитывать при разработке организационных и технических мер по инженерно-технической защите информации?

2. Какие методы могут использоваться при разработке технических мер по инженерно-технической защите информации?

3. Какие факторы следует учитывать при анализе эффективности организационных и технических мер по инженерно-технической защите информации?

4. Какие меры безопасности могут быть реализованы на техническом уровне для защиты информации в организации?

Практическая работа №6«Оценка показателей качества функционирования комплексной системы защиты информации на предприятии: физическое проникновение»

1. Что такое физическое проникновение в контексте оценки показателей качества функционирования комплексной системы защиты информации на предприятии?

2. Какие меры обеспечения физической безопасности могут быть применены для предотвращения физического проникновения на предприятие?

3. Каким образом оценивается эффективность мер по предотвращению физического проникновения на предприятие?

4. Какие технические и организационные меры могут быть использованы для обнаружения физического проникновения на предприятие?

Практическая работа №7«Разработка модели угроз информационной безопасности»

1. Что такое модель угроз информационной безопасности?

2. Какие основные принципы следует учитывать при разработке модели угроз информационной безопасности?

3. Каким образом осуществляется идентификация и классификация угроз в модели угроз информационной безопасности?

4. Какие меры могут быть предприняты на основе модели угроз для снижения рисков информационной безопасности?

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)К правовым методам, обеспечивающим информационную безопасность, относятся:

1. Разработка аппаратных средств обеспечения правовых данных
2. Разработка и установка во всех компьютерных правовых сетях журналов учета действий

3. Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2)Основными источниками угроз информационной безопасности являются все указанное в списке:

1. Хищение жестких дисков, подключение к сети, инсайдерство
2. Перехват данных, хищение данных, изменение архитектуры системы
3. Хищение данных, подкуп системных администраторов, нарушение регламента работы

3)Виды информационной безопасности:

1. Персональная, корпоративная, государственная
2. Клиентская, серверная, сетевая
3. Локальная, глобальная, смешанная

4)Цели информационной безопасности – своевременное обнаружение, предупреждение:

1. несанкционированного доступа, воздействия в сети
2. инсайдерства в организации
3. чрезвычайных ситуаций

5)Основные объекты информационной безопасности:

1. Компьютерные сети, базы данных
2. Информационные системы, психологическое состояние пользователей
3. Бизнес-ориентированные, коммерческие системы

6)Основными рисками информационной безопасности являются:

1. Искажение, уменьшение объема, перекодировка информации
2. Техническое вмешательство, выведение из строя оборудования сети
3. Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:

1. Экономической эффективности системы безопасности
2. Многоплатформенной реализации системы
3. Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:

1. руководители, менеджеры, администраторы компаний
2. органы права, государства, бизнеса
3. сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:

1. Установление регламента, аудит системы, выявление рисков
2. Установка новых офисных приложений, смена хостинг-компании
3. Внедрение аутентификации, проверки контактных данных пользователей

10) Принципом информационной безопасности является принцип недопущения:

1. Неоправданных ограничений при работе в сети (системе)
2. Рисков безопасности сети, системы
3. Презумпции секретности

11) Принципом политики информационной безопасности является принцип:

1. Невозможности миновать защитные средства сети (системы)
2. Усиления основного звена сети, системы
3. Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:

1. Усиления защищенности самого незащищенного звена сети (системы)
2. Перехода в безопасное состояние работы сети, системы
3. Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:

1. Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
2. Одноуровневой защиты сети, системы
3. Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:

1. Компьютерный сбой
2. Логические закладки («мины»)
3. Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:

1. Прочитать приложение, если оно не содержит ничего ценного – удалить
2. Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
3. Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:

1. Секретность ключа определена секретностью открытого сообщения
2. Секретность информации определена скоростью передачи данных
3. Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:

1. Электронно-цифровой преобразователь
2. Электронно-цифровая подпись
3. Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:

1. Покупка нелицензионного ПО

2. Ошибки эксплуатации и неумышленного изменения режима работы системы
3. Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:
1. Распределенный доступ клиент, отказ оборудования
2. Моральный износ сети, инсайдерство
3. Сбой (отказ) оборудования, нелегальное копирование данных

20) Наиболее распространены средства воздействия на сеть офиса:
1. Слабый трафик, информационный обман, вирусы в интернет
2. Вирусы в сети, логические мины (закладки), информационный перехват
3. Компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризуемая:
1. Потерей данных в системе
2. Изменением формы информации
3. Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
1. Целостность
2. Доступность
3. Актуальностьl

23) Угроза информационной системе (компьютерной сети) – это:
1. Вероятное событие
2. Детерминированное (всегда определенное) событие
3. Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
1. Регламентированной
2. Правовой
3. Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:
1. Программные, технические, организационные, технологические
2. Серверные, клиентские, спутниковые, наземные
3. Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:
1. Владелец сети
2. Администратор сети
3. Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:

1. Руководств, требований обеспечения необходимого уровня безопасности
2. Инструкций, алгоритмов поведения пользователя в сети
3. Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:

1. Аудит, анализ затрат на проведение защитных мер
2. Аудит, анализ безопасности
3. Аудит, анализ уязвимостей, риск-ситуаций

29) Что такое ИС?

1. Интернет-система
2. Информационная система
3. Информационный сервер
4. Информационное хранилище

30) Что включает в себя организация работ по обеспечению безопасности в ИС?

1. Определение уровня доступа пользователей
2. Установка антивирусного программного обеспечения
3. Аудит безопасности системы
4. Все вышеперечисленное

31) Что такое аутентификация в ИС?

1. Процесс определения подлинности пользователя
2. Процесс шифрования данных
3. Процесс резервного копирования данных
4. Процесс удаления данных

32) Что такое многофакторная аутентификация?

1. Процесс проверки подлинности пользователя с использованием нескольких различных методов
2. Процесс резервного копирования данных на нескольких устройствах
3. Процесс шифрования данных с использованием нескольких алгоритмов
4. Процесс удаления данных с нескольких устройств

33) Что такое физическая безопасность ИС?

1. Защита данных с помощью физических барьеров, таких как замки, ограждения и видеонаблюдение
2. Защита данных с помощью антивирусного программного обеспечения
3. Защита данных с помощью шифрования
4. Защита данных с помощью паролей

34) Что такое социальная инженерия?

1. Метод хакерской атаки на информационную систему

2. Процесс аутентификации пользователя
3. Метод обеспечения физической безопасности информационной системы
4. Метод межсетевого экрана

35) Какой метод обеспечивает защиту данных с помощью физических барьеров, таких как замки, ограждения и видеонаблюдение?

1. Физическая безопасность
2. Аутентификация
3. Шифрование
4. Пароли

36) Какой процесс определяет уровень доступа пользователей в информационной системе?

1. Аутентификация
2. Физическая безопасность с
3. Шифрование
4. Резервное копирование данных

37) Какой процесс включает установку антивирусного программного обеспечения?

1. Определение уровня доступа пользователей
2. Аутентификация
3. Аудит безопасности системы
4. Организация работ по обеспечению безопасности

38) Что такое многофакторная аутентификация?

1. Процесс проверки подлинности пользователя с использованием нескольких различных методов
2. Процесс резервного копирования данных на нескольких устройствах
3. Процесс шифрования данных с использованием нескольких алгоритмов
4. Процесс удаления данных с нескольких устройств

39) Что такое аудит безопасности системы?

1. Процесс определения уровня доступа пользователей
2. Процесс резервного копирования данных
3. Процесс проверки системы на наличие уязвимостей и неправомерных действий
4. Процесс удаления данных

40) Что такое регулярное обновление программного обеспечения в ИС?

1. Процесс резервного копирования данных
2. Процесс удаления данных
3. Процесс установки обновлений и патчей для программного обеспечения системы
4. Процесс определения уровня доступа пользователей

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

1. неделимость
2. согласованность
3. изолированность
4. продолжительность

42) Свойство транзакции, характеризующееся тем, что после фиксации транзакции изменения становятся постоянными, называется:

1. неделимость
2. согласованность
3. изолированность
4. продолжительность

43) Транзакции могут быть:

1. явные
2. неявные
3. специальные

44) 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)

45) 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)

46) 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

47) 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

48) 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

49) 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

50) 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

51)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

52)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

53) 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

54)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

55)Какие данные обрабатываются в фактографических информационных системах?

1. структурированные данные в виде текстов и чисел
2. любые изображения
3. только числовые
4. исторические факты

56)Какая методология моделирования систем использует понятие "Прецедент"?

1. методология объектно-ориентированного моделирования
2. структурное моделирование
3. визуальное моделирование
4. функциональное моделирование

57)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

58)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

59)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

60)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

61)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

62) Причиной развития темы архитектуры программного обеспечения является

1. рост издержек предприятий
2. развитие технологий
3. нарастающая конкуренция
4. требования к качеству информационных продуктов

63)Шаблоны проектирования (design patterns) представляет собой

1. руководство по реализации
2. универсальный свод информации
3. проектная документация на разработку
4. ограничения по реализации

64)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

65) Выбор стиля использования шаблонов производится на основании

1. имеющихся ресурсов
2. конкурентной среды
3. политики организации
4. требований

66) 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

67) 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

68) 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

69) Компьютерная преступность в мире:

1. остается на одном уровне

2. снижается

3. растет

70) Что из перечисленного не относится к числу основных аспектов информационной безопасности:

1. доступность

2. целостность

3. защита от копирования

4. конфиденциальность

71) 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

72) Укажите, что показывает диаграмма дерева узлов.

1. иерархическую зависимость работ
2. взаимосвязи между работами
3. глубины детализации

73) Укажите, что входит в определение контекста модели.

1. определение субъекта моделирования
2. определение цели моделирования
3. определение точки зрения
4. определение количества уровней декомпозиции

74) Какие типы элементарных моделей используются для построения организационно-функциональной структуры?

1. древовидные модели (классификаторы)
2. процессные модели
3. матричные модели

75) 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

76) 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

77)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

78) 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

79) Каким термином обозначается анализ регистрационной информации системы защиты?

1. мониторинг
2. аудит
3. аккредитация
4. сертификация

80) 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

81) Как называется возможность осуществления угрозы T в отношении объекта O?

1. слабость
2. неполнота
3. уязвимость
4. риск

81) 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

83) 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

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

1. 0
2. 1

85) Защищенность системы защиты определяется как величина…

1. обратная суммарному количеству рисков
2. обратная остаточному риску
3. обратная уязвимости
4. равная сумме всех уязвимостей

86) 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

87) 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

88) 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

89) 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

90) Что из нижеперечисленного относится к оперативным методам повышения безопасности?

1. систематическое тестирование
2. предотвращение ошибок в CASE-технологиях
3. обязательная сертификация
4. программная избыточность

91. то из нижеперечисленного относится к мерам предотвращения угроз безопасности?

1. систематическое тестирование

2. предотвращение ошибок в CASE-технологиях

3. обязательная сертификация

4. программная избыточность

92) Выделите внутренние по отношению к объекту уязвимости дестабилизирующие факторы и угрозы безопасности:

1. ошибки персонала при эксплуатации

2. ошибки программирования

3. сбой и отказы аппаратуры ЭВМ

4. ошибки алгоритмизации задач

93) На каких принципах должна строиться архитектура ИС?

1. проектирование на принципе закрытых систем

2. проектирование на принципе открытых систем

3. усиление самого сильного звена

4. усиление самого слабого звена

5. эшелонирование обороны

94)Какие органы исполнительной власти являются ключевыми в области технической защиты информации?

1. ФСТЭК России

2. ФСБ России

3. СВР России

4. МВД России

5. Роскомнадзор

95) Какой орган государственной власти осуществляет контроль и надзор за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных?

1. ФСТЭК России
2. ФСБ России
3. СВР России
4. МВД России
5. Роскомнадзор

96)Какой орган исполнительной власти осуществляет контроль в области криптографической защиты информации?

1. ФСТЭК России
2. ФСБ России
3. МВД России
4. Роскомнадзор

97)Какой орган исполнительной власти осуществляет сертификацию средств защиты информации, систем и комплексов телекоммуникаций, технических средств, используемых для выявления электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах?

1. ФСТЭК России
2. ФСБ России
3. МВД России
4. Роскомнадзор

98)Какой орган исполнительной власти в настоящее время выполняет функции Гостехкомиссиии России в области технической защиты информации?

1. ФСТЭК России

2. ФСБ России

3. МВД России

4. Роскомнадзор

99)Какой орган исполнительной власти реализует контрольные функции в области обеспечения защиты (некриптографическими методами) информации?

1. ФСТЭК России

2. ФСБ России

3. МВД России

4. Роскомнадзор

100) Какой орган исполнительной власти проводит лицензирование деятельности по оказанию услуг в области защиты государственной тайны в части, касающейся противодействия техническим разведкам и/или технической защиты информации?

1. ФСТЭК России
2. ФСБ России
3. МВД России
4. Роскомнадзор

Задания в открытой форме

1. Информационная система (ИС) - это совокупность программных, аппаратных, организационных и технических средств, предназначенных для…
2. Организация работ по обеспечению безопасности в информационных системах включает следующие этапы: ….
3. Аутентификация - это процесс проверки подлинности пользователя или устройства, чтобы установить, имеет ли оно право на доступ к …
4. Методы аутентификации могут включать…
5. Физическая безопасность информационных систем - это меры, предпринимаемые для защиты физических ресурсов, таких как …
6. Социальная инженерия - это метод атак на информационные системы, при котором злоумышленник использует манипуляции социальными навыками и манипуляцией информацией для …
7. Методы аутентификации бывают…
8. В ИС используются различные методы шифрования данных, включая…
9. Социальная инженерия - это метод атаки на ИС, включающий…
10. Процесс аудита безопасности ИС включает в себя ряд задач, таких как: …

11. Меры физической безопасности, которые могут быть применены для защиты ИС, включают: …
12. Для защиты ИС от угроз, связанных с вредоносным ПО, можно применять следующие меры: …
13. Меры, которые могут быть предприняты для защиты ИС от атак по перехвату данных, включают: использование шифрования …
14. Регулярное обновление программного обеспечения ИС важно для…
15. Основными задачами по обеспечению безопасности являются…
16. Для повышения степени безопасности БД часто используются…
17. Внешний ключ-это…
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. 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 суррогатный 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 операции-	Б	это коллекция операций, 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 символов	В	Пользователь вводит такой 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 действий для создания безопасного пароля:

1. Написать любое слово, которое легко запомнить
2. Добавить к слову цифры и знаки препинания
3. Использовать пароль для нескольких учетных записей
4. Не использовать словарные слова
5. Периодически менять пароль

2. Установите правильную последовательность шагов при обнаружении утечки конфиденциальных данных:

1. Определить, какие данные были скомпрометированы
2. Сообщить о случившемся ответственным лицам
3. Оценить масштаб утечки
4. Принять меры по обезвреживанию утечки
5. Провести расследование и выяснить причину утечки

3. Установите правильную последовательность действий при подозрении на заражение вредоносным ПО:

1. Изолировать устройство от сети
2. Сканировать систему антивирусным ПО

3. Переустановить операционную систему
4. Удалить вредоносное ПО
5. Изменить пароли на всех учетных записях

4. Установите правильную последовательность действий для выполнения аудита безопасности ИС:

1. Определить цели и задачи аудита
2. Собрать информацию о системе и ее настройках
3. Определить риски и угрозы для системы
4. Оценить эффективность системы защиты
5. Разработать план мероприятий по устранению обнаруженных уязвимостей

5. Установите правильную последовательность действий при подозрении на атаку хакера:

1. Определить вид атаки и место ее происхождения
2. Изменить пароли на всех учетных записях
3. Сообщить о случившемся ответственным лицам
4. Изолировать устройство от сети
5. Провести анализ логов системы для выявления следов атаки

6. Расположите следующие действия в правильной последовательности для обеспечения физической безопасности ИС в офисе:

9. Установите систему видеонаблюдения
    1. Ограничьте доступ к помещению с серверами
    2. Запретите посторонним лицам нахождение в офисе без разрешения
    3. Установите систему контроля доступа к помещению с серверами
    4. Закройте окна и двери на ночь

7. Расположите следующие действия в правильной последовательности для защиты ИС от вредоносных программ:
    1. Установите антивирусное программное обеспечение
    2. Регулярно обновляйте антивирусную базу данных
    3. Установите программное обеспечение для брандмауэра
    4. Не открывайте вложения от незнакомых отправителей
    5. Не загружайте и не устанавливайте программное обеспечение из ненадежных источников

8. Расположите следующие действия в правильной последовательности для обеспечения аутентификации пользователей в ИС:
    1. Запросите у пользователя уникальное имя пользователя и пароль
    2. Проверьте, есть ли у данного пользователя права доступа к системе
    3. Проверьте правильность введенных данных
    4. Предоставьте пользователю доступ к системе, если все данные верны
    5. Запишите факт входа пользователя в систему в журнал

9. Расположите следующие действия в правильной последовательности для обеспечения безопасности ИС при удаленной работе:

1. Используйте защищенное соединение VPN при удаленном доступе к ИС
2. Регулярно обновляйте программное обеспечение на удаленных устройствах
3. Защитите устройства от вирусов и других угроз с помощью антивирусного программного обеспечения
4. Проводите обучение сотрудников по безопасному использованию удаленного доступа к ИС
5. Ограничьте доступ к ИС только уполномоченным сотрудникам с помощью механизмов аутентификации и авторизации

10. Установите правильную последовательность действий для выполнения резервного копирования данных:
    1. Определить, какие данные нужно скопировать
    2. Выбрать тип и носитель для копирования
    3. Запустить программу резервного копирования
    4. Проверить, что копирование прошло успешно
11. Установите правильную последовательность действий для проведения тестирования на проникновение:
    1. Подготовить тестовое окружение и выбрать методы тестирования
    2. Запустить тестирование и собирать данные о найденных уязвимостях
    3. Оценить найденные уязвимости и их потенциальные последствия
    4. Подготовить отчет о результатах тестирования и предложить меры по устранению уязвимостей
12. Установите правильную последовательность действий при обнаружении уязвимостей в ИС:
    1. Оценить уровень серьезности уязвимости и ее потенциальные последствия
    2. Подготовить отчет о найденной уязвимости и ее описании
    3. Сообщить ответственным лицам и предложить меры по устранению уязвимости
    4. Проверить, что уязвимость устранена и отслеживать изменения в системе
13. Установите правильную последовательность действий при инциденте в ИС:
    1. Оценить уровень серьезности инцидента и его потенциальные последствия
    2. Принять меры по ограничению ущерба и восстановлению работоспособности системы
    3. Сообщить ответственным лицам и органам об инциденте
    4. Провести анализ причин инцидента и принять меры по предотвращению подобных случаев в будущем
14. Установите правильную последовательность действий для проведения аудита безопасности ИС:

1. Определить цели аудита и выбрать методы и инструменты для проведения аудита
2. Подготовить план и программу аудита, определить сроки и ответственных за проведение аудита
3. Провести аудит, собрать данные и провести их анализ
4. Подготовить отчет о результатах аудита и предложить меры по устранению выявленных недостатков в безопасности ИС.

15. Установите правильную последовательность действий при обнаружении угрозы в ИС:
1. Оценка угрозы
2. Идентификация уязвимости
3. Планирование мер по устранению уязвимости
4. Принятие мер по устранению уязвимости
5. Мониторинг состояния ИС после принятия мер

16. Установите правильную последовательность действий при разработке плана восстановления ИС:
1. Оценка рисков и угроз
2. Идентификация критических систем и данных
3. Разработка сценариев возможных катастроф
4. Разработка плана восстановления
5. Тестирование плана восстановления

17.Установите правильную последовательность действий при аудите безопасности ИС:
1. Определение целей аудита
2. Сбор информации об ИС
3. Оценка рисков ИС
4. Проверка соответствия ИС требованиям безопасности
5. Составление отчета по результатам аудита

18.Установите правильную последовательность действий при разработке политики безопасности ИС:
1. Оценка рисков и угроз
2. Определение требований к безопасности ИС
3. Разработка политики безопасности ИС
4. Утверждение и внедрение политики безопасности ИС
5. Обучение пользователей ИС правилам безопасности

19.Установите правильную последовательность действий при проведении тестирования на проникновение:
1. Оценка уязвимостей ИС
2. Планирование тестирования
3. Проведение тестирования на проникновение
4. Анализ результатов тестирования
5. Разработка рекомендаций по устранению уязвимостей

20. Установите правильную последовательность процесса управления доступом к информационным ресурсам:

1. Определение прав доступа на основе ролей и обязанностей пользователей
2. Аутентификация и авторизация пользователей
3. Установление политик и процедур управления доступом
4. Назначение ответственных лиц за управление доступом
5. Регулярный мониторинг и анализ журналов доступа

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 обнаружила, что ее ИС была скомпрометирована. Какие конкретные действия вы бы предприняли, чтобы расследовать инцидент и вернуть ИС в рабочее состояние? Какие меры безопасности вы предпринимаете, чтобы предотвратить подобные инциденты в будущем?
2. Как бы вы провели аудит безопасности ИС в компании Y? Какие инструменты и методы вы бы использовали для обнаружения потенциальных уязвимостей в ИС? Как бы вы определили критические уязвимости и разработали план мероприятий по устранению этих уязвимостей?
3. Компания Z планирует перевести свою ИС на облачную платформу. Какие меры безопасности вы бы рекомендовали принять компании Z перед переносом данных в облако? Как бы вы оценили безопасность выбранного облачного провайдера и как бы вы защитили данные, хранящиеся в облаке, от потенциальных угроз?
4. Ваша компания получила угрозу распространения вредоносного ПО. Как бы вы организовали обучение сотрудников по безопасности ИС и какие меры безопасности вы бы рекомендовали принять, чтобы предотвратить распространение вредоносного ПО? Как бы вы оценили эффективность ваших мер безопасности?
5. Как бы вы разработали и реализовали план управления рисками безопасности ИС в компании? Как бы вы определили потенциальные угрозы и оценили их влияние на бизнес компании? Как бы вы определили наиболее критические области ИС и как бы вы защитили их от угроз?
6. Компания А решила провести реструктуризацию своих информационных систем для повышения безопасности данных. Какие компетенции необходимо иметь у специалистов, занимающихся этим проектом?
7. Сотрудник компании Б обнаружил утечку конфиденциальной информации. Какие компетенции он должен проявить, чтобы правильно и своевременно сообщить об этом инциденте и помочь минимизировать его последствия?
8. Компания В решила перевести свои информационные системы на облачные платформы. Какие компетенции должны иметь сотрудники, которые будут заниматься реализацией этого проекта, чтобы обеспечить максимальную безопасность данных?

9. Специалист по информационной безопасности в компании Г заметил некоторые аномальные действия в системе и подозревает, что произошла атака хакеров. Какие компетенции ему необходимо проявить, чтобы быстро и эффективно реагировать на инцидент и предотвратить утечку конфиденциальной информации?
10. Компания Д решила создать отдел по информационной безопасности. Какие компетенции должны быть у новых сотрудников, чтобы эффективно защищать ИС компании и принимать меры по предотвращению угроз?
11. Ваша компания переживает серьезный инцидент безопасности, который привел к утечке конфиденциальной информации. Вам поручено возглавить расследование и принять меры для предотвращения подобных инцидентов в будущем. Какие конкретные действия вы будете предпринимать, чтобы выполнить это задание и продемонстрировать свою компетентность в области безопасности информационных систем?
12. Ваша компания готовится к запуску нового веб-приложения. Ваша задача - убедиться, что приложение безопасно и не подвержено риску взлома или кражи данных. Какие шаги вы будете предпринимать, чтобы проверить безопасность приложения и дать рекомендации по усовершенствованию его безопасности?
13. Ваша компания рассматривает возможность перехода на облачные технологии. Ваша задача - провести анализ рисков и предложить конкретные меры для обеспечения безопасности данных и приложений в облачной среде. Какие действия вы будете предпринимать, чтобы выполнить это задание и продемонстрировать свою компетентность в области облачных технологий и безопасности информационных систем?
14. Ваша компания недавно была атакована злоумышленниками, которые украли данные и вымогали выкуп. Ваша задача - разработать стратегию обеспечения безопасности информационных систем компании, чтобы избежать подобных инцидентов в будущем. Какие действия вы будете предпринимать, чтобы выполнить это задание и продемонстрировать свою компетентность в области безопасности информационных систем и управления рисками?
15. Вы работаете в отделе информационной безопасности крупной компании. Ваша задача - разработать и реализовать программу обучения по безопасности информационных систем для всех сотрудников компании. Какие методы обучения и материалы вы будете использовать, чтобы обеспечить эффективность программы обучения и

продемонстрировать свою компетентность в области обучения и безопасности информационных систем?

16. Компания решила провести обучение сотрудников по безопасности информации. Какие компетенции должны быть развиты у сотрудников, чтобы они смогли эффективно обеспечивать безопасность информации в организации?
17. Ваш друг попросил помочь ему настроить парольную защиту на своем устройстве. Опишите ему, какие принципы и методы должны быть использованы для создания безопасного пароля.
18. Вы были назначены ответственным за обеспечение безопасности информации в вашей компании. Какие компетенции вы должны иметь, чтобы успешно выполнять свою работу?
19. Какие компетенции необходимы для проведения аудита безопасности информации в организации?
20. Какие компетенции необходимы для защиты информации в рамках работы в удаленном режиме?
21. Вы работаете в IT-компании и заметили, что ваш коллега часто делает ошибки в своих проектах. Вы хотите помочь ему, но боитесь, что ваше предложение может обидеть его. Как вы можете подойти к этой ситуации таким образом, чтобы помочь своему коллеге и не ущемить его самооценку?
22. Вы работаете в отделе разработки программного обеспечения и ваша команда столкнулась с проблемой в проекте. Вам нужно придумать новое решение, которое поможет вам продвинуться в работе. Как вы можете использовать свою творческую мысль, чтобы найти новый подход к решению проблемы?
23. Вы являетесь руководителем отдела информационной безопасности и обнаружили нарушение в безопасности данных вашей компании. Как вы можете использовать свои лидерские навыки, чтобы предотвратить дальнейшие угрозы для компании и защитить данные?

24. Вы работаете в отделе разработки программного обеспечения и столкнулись с проблемой в работе вашей программы. Вы не знаете, какой именно код вызывает проблему. Как вы можете использовать свои аналитические навыки, чтобы найти и исправить ошибку?
25. Ваша команда занимается разработкой нового проекта, и у вас есть много задач, которые нужно выполнить в определенные сроки. Как вы можете использовать свои организационные навыки, чтобы эффективно

распределить задачи между членами команды и достичь поставленных целей?

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.