МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования «Поволжский государственный университет сервиса»

(ФГБОУ ВО «ПВГУС»)

|  |  |
| --- | --- |
| УТВЕРЖДЕНО |  |
| на заседании Высшей школы интеллектуальных систем и кибертехнологий  |
|  |
| Протокол от | 15.12.2023г. | № | 4 |

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

(фонд оценочных средств)

для проведения промежуточной аттестации по дисциплине

|  |
| --- |
| **«Проектирование интеллектуальных и информационно-аналитических систем в защищенном исполнении»** |

наименование дисциплины

|  |  |
| --- | --- |
| по образовательной программе высшего образования – программе | **магистратуры** |
|  | бакалавриата, специалитета, магистратуры |

**«Информационная безопасность интеллектуальных и информационно-аналитических систем»**

|  |
| --- |
|  |

наименование образовательной программы

|  |
| --- |
| **10.04.01 «Информационная безопасность»** |
| шифр, наименование направления подготовки / специальности |

|  |  |
| --- | --- |
| Составитель | Сыротюк С.Д., доцент, Высшая школа интеллектуальных систем и кибертехнологий, к.п.н., доцент |
|  | ФИО, должность, структурное подразделение, ученая степень, ученое звание |

Тольятти

 2023

**1. Паспорт фонда оценочных средств**

* 1. **Планируемые результаты обучения по дисциплине**

| Код и наименование компетенции | Код и наименование индикатора достижения компетенции | **Основание (ПС)** для профессиональных компетенций |
| --- | --- | --- |
| УК-2. Способен управлять проектом на всех этапах его жизненного цикла | ИУК-2.1. Выстраивает этапы работы над проектом с учетом последовательности их реализации, определяет этапы жизненного цикла проектаИУК-2.2. Разрабатывает план проекта, определяет потребности в ресурсах и осуществляет контроль реализации проекта с последующим публичным представлением полученных результатов |  |
| ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание | ИОПК-1.1. Понимает принципы, требования и структуру системы обеспечения информационной безопасности и защиты информацииИОПК-1.2. Проектирует техническое задание на создание системы обеспечения информационной безопасности и защиты информации |  |
| ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности | ИОПК-2.1. Понимает принципы системного анализа и применяет их для проектирования системы обеспечения информационной безопасностиИОПК-2.2. Проектирует систему обеспечения информационной безопасности, ее компоненты и подсистемыИОПК-2.3. Разрабатывает технические проекты защищённых информационных систем |  |
| ПК-1. Способен провести обследование и анализ деятельности подразделений предприятия, и на их основе выбрать технологии и основные компоненты создаваемых интеллектуальных и информационно-аналитических систем | ИПК-1.1. Проводит предпроектное обследование и анализ деятельности подразделений предприятия и выявляет их потребности, в том числе с применением интеллектуального анализа данных;ИПК 1.2. Применяет знания принципов функционирования, а также конфигураций и состава информационно-аналитических и экспертных систем для обоснования выбора технологий и компонент создаваемых интеллектуальных и информационно-аналитических систем | 06.031 Специалист по автоматизации информационно-аналитической деятельности  |
| ПК-2. Способен разработать проектную документацию и соответствующий ей проект интеллектуальных и информационно-аналитических систем | ИПК- 2.1. Разрабатывает техническое задание на проектирование интеллектуальных и информационно-аналитических систем;ИПК-2.2. Разрабатывает проектную документацию на создаваемые интеллектуальные и информационно-аналитические системы, в том числе на средства защиты информации;ИПК-2.3. Разрабатывает проект интеллектуальных и информационно-аналитических систем и комплекс мер их защиты | 06.031 Специалист по автоматизации информационно-аналитической деятельности  |

В результате изучения дисциплины обучающийся должен:

**владеть**: навыками обоснования потребности в ресурсах и контроля их реализации на всех стадиях проекта, с последующим публичным представлением полученных результатов; навыками разработки технического задания на проектирования систем обеспечения информационной безопасности; навыками разработки технического проекта защищенных информационных систем на основе современных средств и технологий; навыками проектирования интеллектуальных и информационно-аналитических систем

**уметь:** планировать и организовывать этапы работы над проектом с учетом последовательности их реализации, и выбранной модели жизненного цикла проекта; разрабатывать техническое задание на создание системы обеспечения информационной безопасности и защиты информации; применять современные интеллектуальные и информационные технологии и стандарты проектирования при разработке технического проекта; обосновывать выбор технологий и компонент создаваемых интеллектуальных и информационно-аналитических систем

**знать:**  методы и стандарты проектного управления, методологию управления жизненным циклом проекта; принципы обеспечения информационной безопасности и защиты информации и требования нормативных документов для разработки проекта технического задания; принципы системного анализа, знает требования ТЗ к разработке технического проекта по обеспечению информационной безопасности; принципы анализа предметной области исследования; принципы функционирования информационно-аналитических и экспертных систем; преимущества интеллектуальных технологий и систем

**1.2. Содержание дисциплины**

|  |  |  |  |
| --- | --- | --- | --- |
| № | Тема (раздел дисциплины)(в соответствии с РПД) | Код компетенции | Индикатор достижения компетенции |
| 1 | Тема 1. Функциональное моделирование информационно-аналитической системы в области управления информационной безопасностью | ПК-1 | ИПК-1.1, ИПК-1.2 |
| 2 | Тема 2. Интеллектуальные средства и методы математического моделирования систем защиты информации в соответствии с требованиями ТЗ | ОПК-1ОПК-2ПК-2 | ИОПК-1.1, ИОПК-1.2;ИОПК-2.1-ИОПК-2.3;ИПК-2.1-ИПК-2.3 |
| 3 | Тема 3. Построение аналитических предложений с помощью оперативного анализа данных в соответствии с требованиями ТЗ и ТП | ПК-1 | ИПК-1.1-ИПК-1.2 |
| 4 | Тема 4. Проектирование и реализация прототипа интеллектуальных и информационно-аналитических защищенных систем | ПК-1УК-2 | ИПК-1.1-ИПК-1.2;ИУК-2.1-ИУК-2.2; |

**1.3. Система оценивания по дисциплине**

Дисциплина изучается в течение двух семестров.

Форма промежуточной аттестации по дисциплине в третьем семестре – экзамен, в четвертом семестре - экзамен/защита КП

|  |  |
| --- | --- |
| **Шкалы оценки уровня** **сформированности результатов обучения** | **Шкала оценки уровня освоения дисциплины** |
| Уровневая шкала оценки компетенций | 100 бальная шкала, % | 100 бальная шкала, % | 5-балльная шкала,дифференцированная оценка/балл | недифференцированная оценка |
| допороговый | ниже 61 | ниже 61 | «неудовлетворительно» / 2 |  не зачтено |
| пороговый | 61-85,9 | 61-69,9 | «удовлетворительно» / 3  | зачтено |
| 70-85,9 | «хорошо» / 4 | зачтено |
| повышенный  | 86-100 | 86-100 | «отлично» / 5 | зачтено |

**2. Перечень оценочных материалов для проведения промежуточной аттестации**

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в ходе текущего контроля успеваемости (в процессе проведения практических занятий, тестирования, опросов).

В ходе проведения промежуточной аттестации осуществляется контроль и оценка результатов освоения компетенций.

**Перечень вопросов к защите курсового проекта**

**УК-2:ИУК-2.1.ИУК-2.2; ПК-1:ИПК-1.1-ИПК-1.2; ПК-2:ИПК-2.1-ИПК-2.3**

1. Цель и задачи проекта.
2. Проблема, которая решается с помощью данного проекта.
3. Как проводился сбор и анализ информации на предприятии?
4. Какая технология проектирования используется в проекте?
5. Структура и архитектура базы данных / базы знаний в проекте.
6. Какое программное обеспечение используется для проектирования/разработки проекта?
7. Как обеспечивается информационная безопасность и защита информации в информационной системе?
8. Какие информационные технологии применяются для решения прикладных задач по обработке информации?
9. Какие языки программирования использовались в проекте?
10. Каково дальнейшее развитие проекта?

**Перечень вопросов для подготовки к экзамену в третьем семестре**

**ОПК-1: ИОПК-1.1, ИОПК-1.2. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание.**

1. Перечислите принципы обеспечения информационной безопасности и защиты информации
2. Основными принципами информационной безопасности являются конфиденциальность, целостность и доступность. Каждый элемент программы информационной безопасности должен быть предназначен для реализации одного или нескольких из этих принципов. В совокупности они называются триадой. Раскройте содержание принципа Конфиденциальность
3. Основными принципами информационной безопасности являются конфиденциальность, целостность и доступность. Каждый элемент программы информационной безопасности должен быть предназначен для реализации одного или нескольких из этих принципов. В совокупности они называются триадой. Раскройте содержание принципа Целостность
4. Основными принципами информационной безопасности являются конфиденциальность, целостность и доступность. Каждый элемент программы информационной безопасности должен быть предназначен для реализации одного или нескольких из этих принципов. В совокупности они называются триадой. Раскройте содержание принципа Доступность
5. Опишите основное содержание ГОСТ 34.602-2020
6. Опишите основные действия на этапе «Предварительное проектирование» в соответствии с ГОСТ 34.602-2020
7. Опишите основные действия на этапе «Техническое задание» в соответствии с ГОСТ 34.602-2020
8. Опишите основные действия на этапе «Разработка» в соответствии с ГОСТ 34.602-2020
9. Опишите основные действия на этапе «Внедрение» в соответствии с ГОСТ 34.602-2020
10. Опишите основные действия на этапе «Эксплуатация» в соответствии с ГОСТ 34.602-2020
11. Опишите основные действия на этапе «Снятие с эксплуатации» в соответствии с ГОСТ 34.602-2020

**ОПК-2: ИОПК-2.1-ИОПК-2.3.** **Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности.**

1. Какими принципами следует руководствоваться для проектирования системы обеспечения информационной безопасности с применением принципов системного анализа, следующими основными принципами?
2. В чем заключается принцип «Системный подход» для проектирования системы обеспечения информационной безопасности?
3. В чем заключается принцип «Анализ потребностей и требований» для проектирования системы обеспечения информационной безопасности?
4. В чем заключается принцип «Идентификация уязвимостей и угроз» для проектирования системы обеспечения информационной безопасности?
5. В чем заключается принцип «Проектирование решений» для проектирования системы обеспечения информационной безопасности?
6. В чем заключается принцип «Моделирование и оценка» для проектирования системы обеспечения информационной безопасности?
7. В чем заключается принцип «Управление изменениями» для проектирования системы обеспечения информационной безопасности?
8. В чем заключается принцип «Комплексный подход к решению проблем» для проектирования системы обеспечения информационной безопасности?
9. В чем заключается принцип «Непрерывное усовершенствование» для проектирования системы обеспечения информационной безопасности?
10. Перечислите этапы проектирования системы обеспечения информационной безопасности, ее компоненты и подсистемы
11. Что включает в себя этап проектирования системы обеспечения информационной безопасности, ее компоненты и подсистемы «Анализ текущего состояния»?
12. Что включает в себя этап проектирования системы обеспечения информационной безопасности, ее компоненты и подсистемы «Определение потребностей и требований»?
13. Что включает в себя этап проектирования системы обеспечения информационной безопасности, ее компоненты и подсистемы «Разработка стратегии безопасности»?
14. Что включает в себя этап проектирования системы обеспечения информационной безопасности, ее компоненты и подсистемы «Проектирование архитектуры системы»?
15. Что включает в себя этап проектирования системы обеспечения информационной безопасности, ее компоненты и подсистемы «Разработка политик и процедур безопасности»?
16. Что включает в себя этап проектирования системы обеспечения информационной безопасности, ее компоненты и подсистемы «Выбор технологий и инструментов»?
17. Что включает в себя этап проектирования системы обеспечения информационной безопасности, ее компоненты и подсистемы «Разработка плана внедрения»?
18. Что включает в себя этап проектирования системы обеспечения информационной безопасности, ее компоненты и подсистемы «Внедрение и тестирование»?
19. Что включает в себя этап проектирования системы обеспечения информационной безопасности, ее компоненты и подсистемы «Мониторинг, аудит и управление изменениями»?

**ПК-1: ИПК-1.1-ИПК-1.2. Способен провести обследование и анализ деятельности подразделений предприятия, и на их основе выбрать технологии и основные компоненты создаваемых интеллектуальных и информационно-аналитических систем.**

1. Что входит в понятие информационного хранилища?
2. Каковы принципы построения информационных хранилищ?
3. Перечислите задачи и средства администрирования ИАС.
4. Перечислите средства администрирования ИАС
5. Перечислите требования к качеству данных и способы его обеспечения при загрузке в информационное хранилище.
6. Каковы проблемы, разрешаемые при приведении данных к единой структуре информационного хранилища?
7. В чем заключается концепции построения структур хранилищ данных?
8. Назовите назначение, состав и выполняемые функции базы метаданных – репозитория хранилищ данных.
9. Перечислите принципы создания репозитория хранилищ данных.
10. Перечислите элементы моделей данных хранилища, дайте их краткое описание (факт-таблица, таблицы измерений, консольная таблица).
11. По степени "интеллектуальности" обработки данных при анализе выделяют три класса задач анализа. Перечислите их.
12. Что является характерной чертой информационно-поискового анализа?
13. Что является характерной чертой интеллектуального анализа?
14. Что является характерной чертой оперативно-аналитического анализа?
15. Дайте описание рисунку 1 и краткую характеристику каждой из подсистем.

****

Рис.1

**ПК-2: ИПК-2.1-ИПК-2.3. Способен разработать проектную документацию и соответствующий ей проект интеллектуальных и информационно-аналитических систем.**

1. Как называется комбинация взаимодействующих элементов, организованных для достижения одной или нескольких поставленных целей?
2. Как можно охарактеризовать состояние проектируемой системы?
3. Что такое эмерджентность?
4. Чем характеризуется развитие нового поколения аналитических систем для их использования в сфере защиты информации?
5. Привести пример задач, которые могут быть решены с помощью информационных интеллектуальных систем.
6. Что можно отнести к основным требованиям нормативных документов по разработке технического задания (ТЗ)
7. На основе полученного опыта. Приведите пример преимущества использования интеллектуальных систем в кибербезопасности.
8. Какие важные функции, на ваш взгляд, выполняет техническое задание (ТЗ)?
9. Пояснить, кто занимается разработкой Технического задания?
10. Какие были выявлены преимущества использования интеллектуальных систем для защиты информации?
11. Что отражает для организации создание комплексной системы защиты информации?
12. Описать базовые принципы создания комплексной системы защиты безопасности, которые были получены на этапе предпроектного исследования
13. Перечислить несколько основных, на ваш взгляд, функций проектируемой интеллектуальной системы защиты информации по обеспечению информационной безопасности
14. Что входит в понятие информационно-аналитического обеспечения управления разработкой Технического проекта (ТП) на основе ТЗ?
15. Для чего нужны аналитические документы, которые были собраны и проанализированы на этапе предпроектного анализа?
16. Какие из доступных методов анализа данных, вы можете рекомендовать к освоению, исходя из собственного опыта?
17. Сформулировать понятие технологии проектирования интеллектуальных систем и описать ее основные этапы.
18. Как можно представить технологию проектирования и эксплуатации интеллектуальных систем в понятном и простом виде?
19. Как оценить, что разработанная проектная документация и соответствующий ей проект интеллектуальных и информационно-аналитических систем соответствуют друг другу?
20. На какой стадии осуществляется «Определение функциональной и технической архитектур»

**Перечень вопросов для подготовки к экзамену в четвертом семестре**

**УК-2: ИУК-2.1-ИУК-2.2. Способен управлять проектом на всех этапах его жизненного цикла.**

1. Опишите основное содержание ГОСТ Р 54 869-2011 «Проектный менеджмент. Требования к управлению проектом»
2. Опишите основное содержание стандарта PMBOK
3. Опишите основное содержание стандарта ICB IPMA
4. Опишите основное содержание стандарта ITIL
5. Опишите основное содержание стандарта MOF
6. Опишите основное содержание стандарта ITPM
7. Опишите основное содержание стандарта COBIT
8. Опишите основное содержание ГОСТ Р 56875-2016
9. Опишите основное содержание ГОСТ Р 24668-2022
10. Опишите основное содержание ГОСТ Р 70462.1-2022/ISO/IEC TR 24029-1-2021
11. Опишите основное содержание ПНСТ 776-2022
12. Опишите основное содержание ГОСТ Р 59277-2020
13. Опишите основное содержание ГОСТ Р 59276-2020
14. Опишите основное содержание ГОСТ Р 59925-2021
15. Опишите основное содержание ГОСТ Р 59926-2021
16. Опишите основное содержание ГОСТ Р 70466-2022/ISO/IEC TR 205471:2020
17. Опишите основное содержание ГОСТ Р 59898-2021
18. Опишите основное содержание национального стандарта ПНСТ 864-2023
19. Дайте краткую характеристику каскадной модели управления проектами (Waterfall)
20. Дайте краткую характеристику гибким методикам управления проектами (Agile, SCRUM, Kanban и т.д.)
21. Дайте краткую характеристику гибридным методикам управления проектами (Waterwall+Agile)
22. Дайте описание метода проектирования внешней и внутренней оценки деятельности интеллектуальных информационных систем и технологий на основе стандартов (BSC–метод)
23. Дайте описание метода проектирования внешней и внутренней оценки деятельности интеллектуальных информационных систем и технологий на основе стандартов (TEI–метод)
24. Дайте описание метода проектирования внешней и внутренней оценки деятельности интеллектуальных информационных систем и технологий на основе стандартов (EVA–метод)
25. Дайте описание метода проектирования внешней и внутренней оценки деятельности интеллектуальных информационных систем и технологий на основе стандартов (EVS–метод)

**ПК-1: ИПК-1.1-ИПК-1.2. Способен провести обследование и анализ деятельности подразделений предприятия, и на их основе выбрать технологии и основные компоненты создаваемых интеллектуальных и информационно-аналитических систем.**

1. Дайте описание подсистемы ввода данных в СППР
2. Дайте описание подсистемы хранения в СППР
3. Дайте описание подсистемы анализа в СППР
4. Дайте понятие и краткую характеристику такому методу анализа как Data Mining
5. В чем заключается правило 1 «Многомерность», изложенное Коддом и определяющее OLAP?
6. В чем заключается правило 2 «Прозрачность», изложенное Коддом и определяющее OLAP?
7. В чем заключается правило 3 «Доступность», изложенное Коддом и определяющее OLAP?
8. В чем заключается правило 4 «Постоянная производительность при разработке отчетов», изложенное Коддом и определяющее OLAP?
9. В чем заключается правило 5 «Постоянная Клиент-серверная архитектура», изложенное Коддом и определяющее OLAP?
10. В чем заключается правило 6 «Равноправие измерений», изложенное Коддом и определяющее OLAP?
11. В чем заключается правило 7 «Динамическое управление разреженными матрицами, изложенное Коддом и определяющее OLAP?
12. В чем заключается правило 8 «Поддержка многопользовательского режима», изложенное Коддом и определяющее OLAP?
13. В чем заключается правило 9 «Неограниченные перекрестные операции», изложенное Коддом и определяющее OLAP?
14. В чем заключается правило 10 «Интуитивная манипуляция данными», изложенное Коддом и определяющее OLAP?
15. В чем заключается правило 11 «Гибкие возможности получения отчетов», изложенное Коддом и определяющее OLAP?
16. В чем заключается правило 12 «Неограниченная размерность и число уровней агрегации», изложенное Коддом и определяющее OLAP?
17. В 1995 г. Пендсон и Крит на основании правил Кодда разработали тест FASMI, определив OLAP как "Быстрый Анализ Разделяемой Многомерной Информации". В чем особенность данного теста?
18. Назовите способы реализации OLAP-сервера

**Вопросы (задания) для подготовки к экзамену**

**с «ключами» правильных ответов в третьем семестре**

| № | Содержание вопроса | Правильный ответ |
| --- | --- | --- |
| **ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание.**  |
|  | Перечислите принципы обеспечения информационной безопасности и защиты информации | Основными принципами обеспечения информационной безопасности в АСОИ являются следующие 1. Системности.
2. Комплексности.
3. Непрерывности защиты.
4. Разумной достаточности.
5. Гибкости управления и применения.
6. Открытости алгоритмов и механизмов защиты.
7. Простоты применения защитных мер и средств.
 |
|  | Основными принципами информационной безопасности являются конфиденциальность, целостность и доступность. Каждый элемент программы информационной безопасности должен быть предназначен для реализации одного или нескольких из этих принципов. В совокупности они называются триадой. Раскройте содержание принципа Конфиденциальность | Меры по обеспечению конфиденциальности призваны предотвратить несанкционированное разглашение информации. Цель принципа конфиденциальности - сохранить личную информацию в тайне и обеспечить ее видимость и доступ к ней только тем лицам, которые владеют ею или нуждаются в ней для выполнения своих организационных функций |
|  | Основными принципами информационной безопасности являются конфиденциальность, целостность и доступность. Каждый элемент программы информационной безопасности должен быть предназначен для реализации одного или нескольких из этих принципов. В совокупности они называются триадой. Раскройте содержание принципа Целостность | Последовательность включает в себя защиту от несанкционированных изменений (добавлений, удалений, переделок и т.д.) данных. Принцип целостности обеспечивает точность и надежность данных и исключает их некорректное изменение, как случайное, так и злонамеренное |
|  | Основными принципами информационной безопасности являются конфиденциальность, целостность и доступность. Каждый элемент программы информационной безопасности должен быть предназначен для реализации одного или нескольких из этих принципов. В совокупности они называются триадой. Раскройте содержание принципа Доступность | Доступность - это защита способности системы делать программные системы и данные полностью доступными, когда они нужны пользователю (или в определенное время). Цель доступности - сделать технологическую инфраструктуру, приложения и данные доступными, когда они необходимы для организационного процесса или для клиентов организации |
|  | Опишите основное содержание ГОСТ 34.602-2020  | ГОСТ 34.602-2020 - это стандарт, который устанавливает этапы разработки автоматизированных систем (АС) и программ для них. Этот стандарт определяет следующие этапы разработки автоматизированных систем: 1. Предварительное проектирование. 2. Техническое задание. 3. Разработка. 4. Внедрение. 5. Эксплуатация. 6. Снятие с эксплуатации. Эти этапы являются общими для разработки различных типов автоматизированных систем и программного обеспечения и предоставляют основные рекомендации по организации процесса разработки |
|  | Опишите основные действия на этапе «Предварительное проектирование» в соответствии с ГОСТ 34.602-2020 | 1. Предварительное проектирование: - Определение требований к системе - Анализ возможных решений - Проектирование общей концепции системы |
|  | Опишите основные действия на этапе «Техническое задание» в соответствии с ГОСТ 34.602-2020 | 2. Техническое задание:- Формирование технического задания на разработку системы- Определение функциональных и нефункциональных требований к системе- Определение структуры и архитектуры системы |
|  | Опишите основные действия на этапе «Разработка» в соответствии с ГОСТ 34.602-2020 | 3. Разработка: - Непосредственное создание программного обеспечения и аппаратной части системы - Тестирование и отладка разрабатываемых компонентов |
|  | Опишите основные действия на этапе «Внедрение» в соответствии с ГОСТ 34.602-2020 | 4. Внедрение: - Установка и настройка системы на месте эксплуатации - Проведение пилотной эксплуатации, обучение персонала |
|  | Опишите основные действия на этапе «Эксплуатация» в соответствии с ГОСТ 34.602-2020 | 5. Эксплуатация:- Поддержка и сопровождение системы в процессе ее эксплуатации - Мониторинг работы системы, обновление и модернизация |
|  | Опишите основные действия на этапе «Снятие с эксплуатации» в соответствии с ГОСТ 34.602-2020 | 6. Снятие с эксплуатации: - Процессы по выводу системы из эксплуатации, сохранению данных, утилизации оборудования |
| **ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности** |
|  | Какими принципами следует руководствоваться для проектирования системы обеспечения информационной безопасности с применением принципов системного анализа, следующими основными принципами? | Для проектирования системы обеспечения информационной безопасности с применением принципов системного анализа, следует руководствоваться следующими основными принципами: 1) Системный подход. 2) Анализ потребностей и требований. 3) Идентификация уязвимостей и угроз. 4) Проектирование решений. 5) Моделирование и оценка. 6) Управление изменениями. 7) Комплексный подход к решению проблем. 8) Непрерывное усовершенствование. Применение этих принципов позволит разработать эффективную систему обеспечения информационной безопасности, способную эффективно защищать информацию организации от угроз |
|  | В чем заключается принцип «Системный подход» для проектирования системы обеспечения информационной безопасности? | Рассмотрение системы обеспечения информационной безопасности как единого целого, включающего взаимосвязанные компоненты и процессы |
|  | В чем заключается принцип «Анализ потребностей и требований» для проектирования системы обеспечения информационной безопасности? | Выявление и анализ потребностей пользователей, бизнес-процессов и других заинтересованных сторон, а также формулирование конкретных требований к системе обеспечения информационной безопасности |
|  | В чем заключается принцип «Идентификация уязвимостей и угроз» для проектирования системы обеспечения информационной безопасности? | Анализ возможных уязвимостей информационной инфраструктуры и идентификация потенциальных угроз для информационной безопасности |
|  | В чем заключается принцип «Проектирование решений» для проектирования системы обеспечения информационной безопасности? | Разработка архитектуры системы обеспечения информационной безопасности, включая выбор методов защиты, механизмов контроля доступа и других технологий |
|  | В чем заключается принцип «Моделирование и оценка» для проектирования системы обеспечения информационной безопасности? | Использование моделей и симуляций для оценки эффективности предлагаемых решений по обеспечению информационной безопасности |
|  | В чем заключается принцип «Управление изменениями» для проектирования системы обеспечения информационной безопасности? | Учет возможных изменений в информационной инфраструктуре организации и разработка гибкой системы обеспечения информационной безопасности, способной адаптироваться к новым условиям |
|  | В чем заключается принцип «Комплексный подход к решению проблем» для проектирования системы обеспечения информационной безопасности? | Учет взаимодействия системы обеспечения информационной безопасности с другими информационными системами и процессами в организации |
|  | В чем заключается принцип «Непрерывное усовершенствование» для проектирования системы обеспечения информационной безопасности? | Постоянное совершенствование системы обеспечения информационной безопасности на основе анализа инцидентов безопасности, изменений в угрозах и технологических достижений |
|  | Перечислите этапы проектирования системы обеспечения информационной безопасности, ее компоненты и подсистемы | Этапы проектирования системы обеспечения информационной безопасности и ее компонентов могут быть описаны следующим образом:1. Анализ текущего состояния2. Определение потребностей и требований3. Разработка стратегии безопасности4. Проектирование архитектуры системы5. Разработка политик и процедур безопасности6. Выбор технологий и инструментов7. Разработка плана внедрения8. Внедрение и тестирование9. Обучение персонала10. Мониторинг, аудит и управление изменениямиЭти этапы помогут разработать и успешно внедрить систему обеспечения информационной безопасности, соответствующую потребностям организации |
|  | Что включает в себя этап проектирования системы обеспечения информационной безопасности, ее компоненты и подсистемы «Анализ текущего состояния»? | Этап 1. Анализ текущего состояния: - Оценка текущего уровня информационной безопасности, выявление уязвимостей и угроз, анализ существующих политик и процедур безопасности |
|  | Что включает в себя этап проектирования системы обеспечения информационной безопасности, ее компоненты и подсистемы «Определение потребностей и требований»? | Этап 2. Определение потребностей и требований: - Идентификация потребностей пользователей, бизнес-процессов и других заинтересованных сторон, формулирование требований к системе обеспечения информационной безопасности. |
|  | Что включает в себя этап проектирования системы обеспечения информационной безопасности, ее компоненты и подсистемы «Разработка стратегии безопасности»? | Этап 3. Разработка стратегии безопасности: - Определение целей и приоритетов в области информационной безопасности, разработка стратегии защиты информации и принципов управления безопасностью |
|  | Что включает в себя этап проектирования системы обеспечения информационной безопасности, ее компоненты и подсистемы «Проектирование архитектуры системы»? | Этап 4. Проектирование архитектуры системы: - Разработка архитектуры системы обеспечения информационной безопасности, включая выбор компонентов (например, брандмауэры, системы мониторинга, системы управления доступом и т.д.) и определение их взаимодействия |
|  | Что включает в себя этап проектирования системы обеспечения информационной безопасности, ее компоненты и подсистемы «Разработка политик и процедур безопасности»? | Этап 5. Разработка политик и процедур безопасности: - Создание политик безопасности, установление правил доступа, процедур реагирования на инциденты безопасности и других документов, определяющих правила использования информационных ресурсов |
|  | Что включает в себя этап проектирования системы обеспечения информационной безопасности, ее компоненты и подсистемы «Выбор технологий и инструментов»? | Этап 6. Выбор технологий и инструментов: - Определение необходимых технологий, программных и аппаратных средств для реализации системы обеспечения информационной безопасности |
|  | Что включает в себя этап проектирования системы обеспечения информационной безопасности, ее компоненты и подсистемы «Разработка плана внедрения»? | Этап 7. Разработка плана внедрения: - Определение этапов внедрения системы обеспечения информационной безопасности, планирование ресурсов, обучение персонала и тестирование системы |
|  | Что включает в себя этап проектирования системы обеспечения информационной безопасности, ее компоненты и подсистемы «Внедрение и тестирование»? | Этап 8. Внедрение и тестирование: - Реализация плана внедрения системы обеспечения информационной безопасности, проверка работоспособности компонентов системы, проведение тестирования на прочность. |
|  | Что включает в себя этап проектирования системы обеспечения информационной безопасности, ее компоненты и подсистемы «Мониторинг, аудит и управление изменениями»? | Этап 9. Обучение персонала: - Обучение сотрудников по правилам использования новой системы обеспечения информационной безопасности |
| **ПК-1. Способен провести обследование и анализ деятельности подразделений предприятия, и на их основе выбрать технологии и основные компоненты создаваемых интеллектуальных и информационно-аналитических систем.**  |
| 1 | Что входит в понятие информационного хранилища?  | Информационное хранилище (Data Warehousing) - это место хранения данных предприятия, предназначенное для упрощения принятия управленческих решений. Информационное хранилище включает в себя не только данные, но также инструменты, процедуры, обучение, персонал и другие ресурсы, облегчающие доступ к данным и делающие его более осмысленным для лиц, принимающих решения. |
| 2 | Каковы принципы построения информационных хранилищ?  | Инмон (Inmon) — автор концепции информационных хранилищ выделяет следующие характерные для них свойства: – предметную ориентированность; – интегрированность; – неизменчивость; – поддержка хронологии |
| 3 | Перечислите задачи и средства администрирования ИАС.  | **К задачам администрирования информационно-аналитических систем (ИАС)** относятся:1. Загрузка и обновление данных
2. Планирование работы с ИАС
3. Эксплуатация ИАС
4. Создание (участие в создании) моделей предметной области, гиперкубов и интерфейсов пользователей
5. Контроль за их наполнением
 |
| 4 | Перечислите средства администрирования ИАС | Все средства анализа и ИХ можно поделить на три больших класса:1. Средства массового применения, к которым относятся Excel, Statistica
2. Встроенные в интегрированные ЭИС инструментальные средства создания и поддержки ИХ и анализа
3. Специализированные инструментальные средства создания ИХ и обеспечения различного вида анализа
 |
| 5 | Перечислите требования к качеству данных и способы его обеспечения при загрузке в информационное хранилище.  | Требования к качеству данных следующие:1. Точность данных
2. Полнота данных
3. Согласованность данных
4. Уникальность данных
5. Целостность данных

Способы обеспечения качества данных при загрузке в информационное хранилище могут включать:Использование ETL-процессовПроверка на дубликатыВалидация данныхМониторинг качества данныхАудит данныхОбучение персонала |
| 6 | Каковы проблемы, разрешаемые при приведении данных к единой структуре информационного хранилища? | Проведение данных к единой структуре информационного хранилища позволяет решить следующие проблемы:1.Избавление от избыточности данных: При объединении данных из различных источников их дублирование и избыточность могут быть устранены, что позволяет экономить место и упрощает анализ.2.Обеспечение единого формата данных: Различные источники могут предоставлять данные в разных форматах. Приведение их к единому формату упрощает их анализ и обработку.3.Улучшение качества данных: При объединении данных и приведении их к единой структуре можно устранить ошибки, пропуски и несоответствия, что повышает качество данных.4. Обеспечение целостности данных:Единая структура информационного хранилища позволяет поддерживать целостность данных и обеспечивать их надежность. 5.Упрощение доступа к данным:Единая структура упрощает доступ к данным для аналитиков, бизнес-пользователей и других заинтересованных лиц. 6.Повышение эффективности анализа: Структурированные данные легче анализировать, выявлять тенденции и принимать обоснованные решения на основе данных. 7.Снижение затрат на обработку данных: Унификация структуры данных позволяет снизить затраты на их обработку и хранение за счет оптимизации процессов работы с данными. |
| 7 | В чем заключается концепции построения структур хранилищ данных?  | Концепция построения структуры хранилищ данных включает в себя несколько ключевых аспектов: 1.Идентификация бизнес-требований 2. Анализ и моделирование данных 3. Выбор технологий и инструментов 4. Проектирование структуры хранилища данных 5. Развертывание и настройка хранилища данных 6. Загрузка данных 7.Обеспечение качества данных 8. Поддержка и мониторингЭти шаги помогают построить структуру хранилища данных, которая отвечает потребностям бизнеса и обеспечивает эффективное использование данных для принятия решений |
| 8 | Назовите назначение, состав и выполняемые функции базы метаданных – репозитория хранилищ данных.  | База метаданных-репозитория хранилища данных является центральным хранилищем информации о данных, их структуре, связях, источниках, процессах загрузки и трансформации. Ее основное назначение - обеспечить управление метаданными, необходимыми для работы с данными в хранилище. Вот основные составляющие и функции базы метаданных-репозитория хранилища данных: 1. Метаданные 2 Описание процессов загрузки и трансформации 3. Связи между данными 4. История изменений 5 Пользователи и права доступа 6. Модели данных 7.Аудит и мониторинг.Функции базы метаданных-репозитория хранилища данных включают управление метаданными, обеспечение целостности и актуальности информации, поддержку процессов анализа и отчетности, управление доступом к данным, а также обеспечение прозрачности и понимания структуры данных для пользователей |
| 9 | Перечислите принципы создания репозитория хранилищ данных.  | Создание репозитория хранилища данных включает в себя несколько ключевых принципов, которые помогают обеспечить эффективное управление данными и обеспечить их качество. Вот некоторые из основных принципов создания репозитория хранилища данных: 1.Централизация данных. 2. Единая модель данных. 3.Стандартизация именования. 4.Документирование метаданных. 5.Управление версиями 6.Аудит и контроль доступа. 7.Интеграция с другими системами. 8.Мониторинг и оптимизация. Эти принципы помогают создать надежный и эффективный репозиторий хранилища данных, который будет служить основой для анализа, отчетности и принятия решений в организации |
| 10 | Перечислите элементы моделей данных хранилища, дайте их краткое описание (факт-таблица, таблицы измерений, консольная таблица). | 1. Факт-таблица (Fact Table): - таблица содержит числовые данные, которые отражают факты или события, происходящие в бизнес-процессе. Это основная таблица для анализа данных и содержит ключи для связи с таблицами измерений.2.Таблица измерений (Dimension Table): Таблица измерений содержит описательные атрибуты, которые характеризуют измерения фактов в факт-таблице. Эти атрибуты позволяют анализировать данные по различным измерениям (например, по времени, продуктам, клиентам и т. д.). 3.Консольная таблица (Lookup Table): Консольная таблица представляет собой таблицу справочных данных, которые используются для связывания значений в факт-таблице с соответствующими значениями в таблицах измерений. Она содержит уникальные значения и соответствующие им ключи для связи с другими таблицами. Консольные таблицы облегчают анализ данных и уменьшают дублирование информации. Эти элементы моделей данных хранилища обеспечивают структурирование данных, позволяют проводить анализ и отчетность на основе данных и обеспечивают эффективное использование информации для принятия решений  |
| 11 | По степени "интеллектуальности" обработки данных при анализе выделяют три класса задач анализа. Перечислите их. | По степени "интеллектуальности" обработки данных при анализе выделяют три класса задач анализа: информационно-поисковый; оперативно-аналитический; интеллектуальный |
| 12 | Что является характерной чертой информационно-поискового анализа? | СППР осуществляет поиск необходимых данных. Характерной чертой такого анализа является выполнение заранее определенных запросов |
| 13 | Что является характерной чертой интеллектуального анализа? | СППР осуществляет поиск функциональных и логических закономерностей в накопленных данных, построение моделей и правил, которые объясняют найденные закономерности и/или (с определенной вероятностью) прогнозируют развитие некоторых процессов |
| 14 | Что является характерной чертой оперативно -аналитического анализа? | СППР производит группирование и обобщение данных в любом виде, необходимом аналитику. В отличие от информационно-поискового анализа в данном случае невозможно заранее предсказать необходимые аналитику запросы |
| 15 | Дайте описание рисунку 1 Рис. 1 | На рисунке 1 представлена обобщенная архитектура СППР. Рассмотрим отдельные подсистемы:1. Подсистема ввода
2. Подсистема хранения.
3. Подсистема анализа
 |
| **ПК-2. Способен разработать проектную документацию и соответствующий ей проект интеллектуальных и информационно-аналитических систем.**  |
|  | Как называется комбинация взаимодействующих элементов, организованных для достижения одной или нескольких поставленных целей? | Эта комбинация взаимодействующих элементов, организованных для достижения одной или нескольких поставленных целей называется, согласно ГОСТ (ГОСТ Р ИСО МЭК 15288-2005) при проектировании информационных систем просто системой. Ответ - система |
|  | Как можно охарактеризовать состояние проектируемой системы? | Под состоянием проектируемой системы называется совокупность свойств или признаков, которые в каждый момент времени отражают наиболее существенные особенности поведения системы |
|  | Что такое эмерджентность? | Эмерджентностью появление у системы свойств, не присущих элементам системы; принципиальная несводимость свойств системы к сумме свойств составляющих ее компонентов? |
|  | Чем характеризуется развитие нового поколения аналитических систем для их использования в сфере защиты информации? | В последнее десятилетие наблюдаетсяактивное развитие нового поколения аналитических систем, которые основаны на передовых технологиях искусственного интеллекта. Они входят в такое понятие, как«интеллектуальные информационные системы». Они имеют большой потенциал в сфере защиты информации благодаря возможности разработки систем, которые обучаютсяи способны автономно принимать решения,а также обнаружить и классифицировать потенциальные атаки или угрозы. |
|  | Привести пример задач, которые могут быть решены с помощью информационных интеллектуальных систем. | Задачи, которые могут быть решены интеллектуальными информационными системами (ИИС), например:– Интерпретация данных. Эта задача подразумевает определение смысла данных и анализ множества вариантов для достижения согласованности, и корректности результатов.– Диагностика. Решение этой задачи предполагает соотношение объекта с определенным классом объектов или обнаружение неисправностей в системе.– Мониторинг. Решение этой задачи предполагает непрерывный анализ данных в режиме реального времени и оповещение о превышении допустимых значений параметров.– Проектирование. Решение этой задачи включает подготовку спецификаций для создания «объектов» с заранее определенными свойствами.– Прогнозирование. При решении этой задачи представлена возможность предсказывания последствий определенных событий или явлений на основе данных параметрической динамической модели, прикоторой значения параметров подбирают под заданную ситуацию. |
|  | Что можно отнести к основным требованиям нормативных документов по разработке технического задания (ТЗ) | Грамотно составленное ТЗ предусматривает наличие нескольких обязательных составных частей, которые можно отнести к основным требованиям, это:* Подробное описание целей реализации проекта.
* Основные требования и ожидания от конечного продукта.
* Ключевые этапы выполнения работ.
* Календарный график или сроки исполнения.
 |
|  | На основе полученного опыта. приведите пример преимущества использования интеллектуальных систем в кибербезопасности. | В процессе приобретения опыта было выявлено, что одним важным преимуществом использования интеллектуальных систем в кибербезопасности является их способность к самообучению на основе полученного опыта. Опыт предыдущих атак поможет улучшить имеющиеся алгоритмы поведения и обеспечить более точное обнаружение угрозв будущем |
|  | Какие важные функции, на ваш взгляд, выполняет техническое задание (ТЗ)? | На наш взгляд, Техническое задание выполняет ряд важных функций, которые обеспечивают безопасность трудового взаимодействия Заказчика и Исполнителя. Это проявляется в следующем:* Раскладывает в голове у Заказчика и Разработчика, то, как должна выглядеть система и что она должна делать.
* Защищает Разработчика от вдруг появившихся новых требований Заказчика, то есть Разработчик должен выполнить всё то, что написано в ТЗ.
* Если Заказчик хочет видеть в программе ещё одну какую-либо функцию, то за неё нужно платить отдельно и составлять на неё отдельно Техническое задание.
* Защищает Заказчика от лени и некомпетентности Разработчика, то есть программа должна выглядеть именно так, как написано в ТЗ.
* На основании Технического задания Заказчик может предъявить претензии к Разработчику
 |
|  | Пояснить, кто занимается разработкой Технического задания? | Техническое задание предполагает работу группы лиц:* Аналитиков со стороны Заказчика — они определяют необходимость системы, выдвигают в письменном виде требования к новой программе.
* Аналитиков со стороны Разработчика — они должны обследовать область, по которой будет разрабатываться программа. Учесть все схемы, алгоритмы и нюансы работы, которую будет выполнять система.
* Технический писатель — сотрудник, который соберёт все данные аналитиков и запишет их согласно ГОСТу.
 |
|  | Какие были выявлены преимущества использования интеллектуальных систем для защиты информации? | Использование интеллектуальных системдля защиты информации имеет ряд преимуществ. В первую очередь, интеллектуальные системы обладают способностью анализировать большие объемы данных и обнаруживать потенциальные угрозы с большей точностью и эффективностью, чем традиционные методы. Они могут автоматически мониторить и анализировать данные, обнаруживать аномалии и подозрительную активность, которые могут указывать на угрозы и атаки |
|  | Что отражает для организации создание комплексной системы защиты информации? | Создание комплексной системы защиты информации (КСЗИ) для организации отражает системный подход к обеспечению информационной безопасности (ИБ) компании, предотвращению хищений и утечек информации ограниченного доступа, а также оптимизирует работу ИТ-системы предприятия, снижает капитальные и операционные затраты компании |
|  | Описать базовые принципы создания комплексной системы защиты безопасности, которые были получены на этапе предпроектного исследования | Принципы создания комплексной системы защиты информации. выявленные на этапе предпроектного исследования. включают:А) соответствие мер защиты КСЗИ реальным угрозам ИБ;Б) соответствие требованиям законодательства, ведомственных нормативных документов в сфере обеспечения ИБ;В) интеграцию с существующими процессами управления и средствами обеспечения ИБ;Г) использование современных технических и программных средств защиты информации ведущих российских и зарубежных вендоров |
|  | Перечислить несколько основных, на ваш взгляд, функций проектируемой интеллектуальной системы защиты информации по обеспечению информационной безопасности | В результате формирования навыков предпроектного анализа было выявлено, что основные функции интеллектуальной КСЗИ по обеспечению ИБ могут состоять в:1) управление доступом (идентификация, аутентификация, авторизация и контроль доступа пользователей на всех уровнях корпоративной информационной системы — IDM);2) управление регистрацией и учетом, обеспечение целостности (средства защиты АРМ и серверов);3) регистрация событий информационной безопасности (SIEM);4) межсетевое экранирование, организация IPSec VPN и защищенного удаленного доступа;5) обнаружение и предотвращение вторжений (IPS/IDS);6) контроль и анализ защищённости;7) защита от вирусов и спама;8) предотвращение утечек и контроль доступа пользователей в интернет (DLP). |
|  | Что входит в понятие информационно-аналитического обеспечения управления разработкой Технического проекта (ТП) на основе ТЗ? | Информационно-аналитическое обеспечение управления представляет собой совокупность организационных, методических и интеллектуальных видов деятельности по сбору, систематизации, анализу, хранению, использованию и распространению сведений о различных аспектах функционирования системы |
|  | Для чего нужны аналитические документы, которые были собраны и проанализированы на этапе предпроектного анализа? | Аналитические документы формируются в результате аналитической обработки данных.Аналитическая обработка данных — это технология обработки данных, заключающаяся в подготовке агрегированной информации на основе больших массивов данных. Данный тип анализа данных является классическим и используется при обработке данных, хранящихся, например, в СУБД |
|  | Какие из доступных методов анализа данных, вы можете рекомендовать к освоению, исходя из собственного опыта? |  Считаю, что можно рекомендовать к обучению следующие методы. Которые легко реализовать имеющимися инструментальными средствами.Метод «Описательная статистика»;Метод «Визуализация данных»;Метод «Кластерный анализ»; Метод «Корреляционный анализ»;Метод «Регрессионный анализ»Методы машинного обучения |
|  | Сформулировать понятие технологии проектирования интеллектуальных систем и описать ее основные этапы. | Технология представляет собой порядок взаимодействия структурных элементовсистемы. Технология может состоять из совокупности отдельных алгоритмов. Интегральный характер носит технология проектирования и эксплуатации интеллектуальной системы.Эта технология включает в себя следующие этапы:1) идентификация;2) концептуализация;3) формализация;4) реализация (выполнение);5) отладка и тестирование;6) опытная эксплуатация. |
|  | Как можно представить технологию проектирования и эксплуатации интеллектуальных систем в понятном и простом виде? | Технологию проектирования и эксплуатации интеллектуальных систем можнопредставить в виде совокупности трех технологий:1)Технология создания, она определяется этапами идентификации, концептуализации иформализации.Этап концептуализации специфичен и характерен только дляинтеллектуальных систем;2) Технология использования, представленная соответствующими инструкциями, она формируется на этапах реализации, отладки и корректируется на этапе опытнойэксплуатации.3) Технология функционирования, она связана с этапом формализации |
|  | Как оценить, что разработанная проектная документация и соответствующий ей проект интеллектуальных и информационно-аналитических систем соответствуют друг другу? | Это можно сделать, если составить документ «Технические условия» (ТУ). В нем могут быть прописаны особенности приемки результатов соответствия выполненного технического задания (ТЗ). Но сейчас это применяется редко. |
|  | На какой стадии осуществляется «Определение функциональной и технической архитектур» | Определение и функциональной и технической архитектур осуществляется на стадии IV «Технический проект (ТП)». На этой стадии выполняется:1) Описание функциональной архитектуры (включая описание каждой функции, задачи, методов реализации). 2) Описание технической архитектуры (включая описание размещения технических средств, условий эксплуатации, режима функционирования, организации резервного копирования и т.д.) |

**Вопросы (задания) для подготовки к экзамену**

**с «ключами» правильных ответов в четвертом семестре**

| № | Содержание вопроса | Правильный ответ |
| --- | --- | --- |
| **УК-2. Способен управлять проектом на всех этапах его жизненного цикла** |
|  | Опишите основное содержание ГОСТ Р 54 869-2011 «Проектный менеджмент. Требования к управлению проектом»  | Настоящий стандарт устанавливает требования к управлению проектом для обеспечения эффективного достижения целей проекта. Настоящий стандарт может использоваться с целью оценки соответствия управления проектом, установленным в стандарте требованиям |
|  | Опишите основное содержание стандарта PMBOK | Стандарт управления проектом идентифицирует принципы управления проектом, направляющие поведение и действия специалистов по проектам и прочих заинтересованных сторон, работающих над проектами или вовлеченных в них. Применяется вне зависимости от области и подхода к поставке (например, предиктивного, адаптивного или гибридного). |
|  | Опишите основное содержание стандарта ICB IPMA | Стандарт, описывающий международные требования к компетентности специалистов по управлению проектами, разработанный международной ассоциацией управления проектами IPMA. Стандарт используется в качестве основы для международной сертификации специалистов по управлению проектами по четырехуровневой системе 4LC |
|  | Опишите основное содержание стандарта ITIL | Конкретный набор практик и рекомендаций для управления IT-сервисами. Библиотека ITIL предоставляет подробные инструкции и рекомендации по процессам и задачам, связанным с IT-сервисами |
|  | Опишите основное содержание стандарта MOF | Набор рекомендаций, на основе которого можно разрабатывать процедуры, элементы управления и роли, необходимые для эффективной работы ИТ-инфраструктуры. MOF основан на стандарте ITIL (IT Infrastructure Library) и учитывает специфику платформы Майкрософт. |
|  | Опишите основное содержание стандарта ITPM | Стандарт представляет собой общий подход к управлению IT-сервисами в организации. Он включает в себя разработку, предоставление услуг и поддержку IT-сервисов, а также управление всеми процессами, связанными с этими сервисами. ITSM охватывает широкий спектр деятельности, и включает в себя множество методологий и стандартов, включая и ITIL |
|  | Опишите основное содержание стандарта COBIT | Стандарт управления и аудита в области информационных технологий. Основой стандарта COBIT являются 34 высокоуровневые цели контроля, по одной на каждый ИТ-процесс, которые сгруппированы в 4 домена: Планирование и Организация, Проектирование и Внедрение, Эксплуатация и Сопровождение, Мониторинг |
|  | Опишите основное содержание ГОСТ Р 56875-2016 | ГОСТ Р 56875-2016. Информационные технологии. Системы безопасности комплексные и интегрированные. Типовые требования к архитектуре и технологиям интеллектуальных систем мониторинга для обеспечения безопасности предприятий и территорийНастоящий стандарт определяет назначение и устанавливает общие технические требования к архитектуре, составу компонентов и функциям интегрированных интеллектуальных систем мониторинга и обеспечения безопасности распределенных объектов предприятий (ИИСМиОБП) и территорий стратегических и социально-значимых объектов в регионах Российской Федерации. |
|  | Опишите основное содержание ГОСТ Р 24668-2022 | ГОСТ Р 24668-2022. Информационные технологии. Искусственный интеллект. Структура управления процессами для анализа больших данных (ИСО/МЭК 24668:2022)Настоящий документ описывает рамочную структуру (концепцию) для разработки процессов, обеспечивающих эффективное использование возможностей аналитики больших данных в масштабах всей организации, вне зависимости от ее принадлежности к определенному сектору или отрасли |
|  | Опишите основное содержание ГОСТ Р 70462.1-2022/ISO/IEC TR 24029-1-2021 | ГОСТ Р70462.1-2022/ISO/IEC TR 24029-1-2021. Информационные технологии. Интеллект искусственный. Оценка робастности нейронных сетей. Часть 1.В настоящем стандарте представлена справочная информация о существующих методах оценки робастности нейронных сетей. |
|  | Опишите основное содержание ПНСТ 776-2022 | ПНСТ 776-2022 Информационные технологии. Интеллект искусственный. Управление рискамиВ настоящем стандарте представлены рекомендации по управлению рисками, с которыми сталкиваются организации при разработке и применении методов и систем искусственного интеллекта (ИИ). Рекомендации также направлены на оказание помощи организациям с интеграцией управления рисками в их деятельность и функции, связанные с ИИ |
|  | Опишите основное содержание ГОСТ Р 59277-2020 | ГОСТ Р 59277-2020. Системы искусственного интеллекта. Классификация систем искусственного интеллектаНастоящий стандарт устанавливает классификацию систем искусственного интеллекта (ССИ). Настоящий стандарт предназначен для применения в сфере теоретической и практической деятельности по классификации систем искусственного интеллекта. В настоящем стандарте установлена схема классификации, отражающая основные особенности СИИ для решения прикладных задач, помогающая определить направления их стандартизации |
|  | Опишите основное содержание ГОСТ Р 59276-2020 | ГОСТ Р 59276-2020. Системы искусственного интеллекта. Способы обеспечения доверия. Общие положенияВ настоящем стандарте рассматриваются вопросы обеспечения доверия к системам искусственного интеллекта со стороны потребителей результатов работы этих систем и, при необходимости, со стороны организаций, ответственных за регулирование вопросов создания и применения систем искусственного интеллекта, на основе подтверждения их качества |
|  | Опишите основное содержание ГОСТ Р 59925-2021 | ГОСТ Р 59925-2021. Информационные технологии. Большие данные. Техническое задание. Требования к содержанию и оформлениюНастоящий стандарт устанавливает требования к построению, содержанию, изложению, оформлению, порядку согласования и утверждения технического задания в области оперирования большими данными, а также определяет особенности указанных технических заданий для государственных и муниципальных закупок |
|  | Опишите основное содержание ГОСТ Р 59926-2021 | ГОСТ Р 59926-2021. Информационные технологии. Эталонная архитектура больших данных. Часть 2. Варианты использования и производные требованияНастоящий стандарт содержит анализ вариантов использования больших данных в различных областях применения, а также выводы, сделанные на основе этого анализа. |
|  | Опишите основное содержание ГОСТ Р 70466-2022/ISO/IEC TR 205471:2020 | ГОСТ Р 70466-2022/ISO/IEC TR 205471:2020. Информационные технологии. Эталонная архитектура больших данных. Часть 1.Настоящий стандарт содержит описание структуры эталонной архитектуры больших данных и процесса применения стандарта в рассматриваемой предметной области |
|  | Опишите основное содержание ГОСТ Р 59898-2021 | ГОСТ Р 59898-2021. Оценка качества систем искусственного интеллекта. Общие положенияНастоящий стандарт устанавливает общие требования к оценке качества СИИ, включая:- виды существенных характеристик СИИ, подтверждение значений которых установленным требованиям обеспечивает доверие к этим системам;- порядок выбора и оценки метрик качества на основании представленного набора существенных характеристик;- требования к набору входных и выходных данных для тестирования СИИ;- вопросы планирования, разработки программы и процедуры оценки качества СИИ в целях подтверждения его надежности, безопасности и функциональности |
|  | Опишите основное содержание национального стандарта ПНСТ 864-2023 | Национальный стандарт ПНСТ 864-2023 «Умные (SMART) стандарты. Общие положения»Документ по стандартизации, содержащий нормативные требования к объектам стандартизации, который является объектом информационной системы документов по стандартизации и представляется в виде контейнера неструктурированных и структурированных данных |
|  | Дайте краткую характеристику каскадной модели управления проектами (Waterfall) | Модель процесса разработки программного обеспечения, в которой процесс разработки выглядит как поток, последовательно проходящий фазы анализа требований, проектирования, реализации, тестирования, интеграции и поддержки. |
|  | Дайте краткую характеристику гибким методикам управления проектами (Agile, SCRUM, Kanban и т.д.) | Разработаны для решения проблем, появляющихся в процессе работы над проектами с использованием традиционных методов управления. Они позволяет управлять проектами в гибком и адаптивном режиме, что дает возможность быстро реагировать на изменения, которые могут возникнуть в процессе работы. |
|  | Дайте краткую характеристику гибридным методикам управления проектами (Waterwall+Agile) | Каскадный подход помогает выдерживать структуру проекта, придерживаться заданных границ и соблюдать контрольные точки. В свою очередь, гибкие методологии позволяют в рамках этого огромного графика оперативно решать вопросы, не уходить в излишнюю бюрократию, быть на короткой связи со всеми заинтересованными лицами, проверять гипотезы и достаточно быстро встраивать их в проект при необходимости, а также отслеживать состояние команд. |
|  | Дайте описание метода проектирования внешней и внутренней оценки деятельности интеллектуальных информационных систем и технологий на основе стандартов (BSC–метод) | Предполагает проведение оценки эффективности ИС, воспользовавшись комплексной функцией, которая состоит из набора показателей, которые учитывают все моменты деятельности компании. |
|  | Дайте описание метода проектирования внешней и внутренней оценки деятельности интеллектуальных информационных систем и технологий на основе стандартов (TEI–метод) | Проводится расчет эффективности ИС на основании следующих факторов:преимущества (происходит сравнение текущей информационной системы с будущей, выявляются преимущества и недостатки будущей системы);гибкость (возможность новой информационной системы адаптироваться к новым условиям);риск (оценивается вероятность понести финансовые потери в случае использования информационной системы на предприятии) |
|  | Дайте описание метода проектирования внешней и внутренней оценки деятельности интеллектуальных информационных систем и технологий на основе стандартов (EVA–метод) | Позволяет оценить, какую фактическую прибыль приносит использование данного программного обеспечения для компании |
|  | Дайте описание метода проектирования внешней и внутренней оценки деятельности интеллектуальных информационных систем и технологий на основе стандартов (EVS–метод) | Предполагает оценивание того, какой положительный эффект приносит использование данного программного обеспечения для компании |
| **ПК-1. Способен провести обследование и анализ деятельности подразделений предприятия, и на их основе выбрать технологии и основные компоненты создаваемых интеллектуальных и информационно-аналитических систем** |
|  | Дайте описание подсистемы ввода данных в СППР | Подсистема ввода данных -в таких подсистемах, называемых OLTP (Online transaction processing), реализуется операционная (транзакционная) обработка данных. Для их реализации используют обычные системы управления базами данных (СУБД) |
|  | Дайте описание подсистемы хранения в СППР | Подсистема хранения- Для реализации данной подсистемы используют современные СУБД и концепцию хранилищ данных |
|  | Дайте описание подсистемы анализа в СППР | Подсистема анализа - Данная подсистема может быть построена на основе: подсистемы информационно-поискового анализа на базе реляционных СУБД и статических запросов с использованием языка SQL (Structured Query Language); подсистемы оперативного анализа. Для реализации таких подсистем применяется технология оперативной аналитической обработки данных OLAP (On-line analytical processing), использующая концепцию многомерного представления данных; подсистемы интеллектуального анализа. Данная подсистема реализует методы и алгоритмы Data Mining ("добыча данных") |
|  | Дайте понятие и краткую характеристику такому методу анализа как Data Mining | Data Mining — исследование и обнаружение "машиной" (алгоритмами, средствами искусственного интеллекта) в сырых данных скрытых знаний, которые ранее не были известны, нетривиальны, практически полезны, доступны для интерпретации человеком |
|  | В чем заключается правило 1 «Многомерность», изложенное Коддом и определяющее OLAP? | Многомерность — OLAP-система на концептуальном уровне должна представлять данные в виде многомерной модели, что упрощает процессы анализа и восприятия информации |
|  |  В чем заключается правило 2 «Прозрачность», изложенное Коддом и определяющее OLAP? | Прозрачность — OLAP-система должна скрывать от пользователя реальную реализацию многомерной модели, способ организации, источники, средства обработки и хранения |
|  | В чем заключается правило 3 «Доступность», изложенное Коддом и определяющее OLAP? | Доступность — OLAP-система должна предоставлять пользователю единую, согласованную и целостную модель данных, обеспечивая доступ к данным независимо от того, как и где они хранятся |
|  | В чем заключается правило 4 «Постоянная производительность при разработке отчетов», изложенное Коддом и определяющее OLAP? | «Постоянная производительность при разработке отчетов», изложенное Коддом и определяющее OLAP — производительность OLAP-систем не должна значительно уменьшаться при увеличении количества измерений, по которым выполняется анализ |
|  | В чем заключается правило 5 «Постоянная Клиент-серверная архитектура», изложенное Коддом и определяющее OLAP? | Клиент-серверная архитектура — OLAP-система должна быть способна работать в среде "клиент-сервер", т. к. большинство данных, которые сегодня требуется подвергать оперативной аналитической обработке, хранятся распределенно. Главной идеей здесь является то, что серверный компонент инструмента OLAP должен быть достаточно интеллектуальным и позволять строить общую концептуальную схему на основе обобщения и консолидации различных логических и физических схем корпоративных БД для обеспечения эффекта прозрачности |
|  | В чем заключается правило 6 «Равноправие измерений», изложенное Коддом и определяющее OLAP? | Равноправие измерений — OLAP-система должна поддерживать многомерную модель, в которой все измерения равноправны. При необходимости дополнительные характеристики могут быть предоставлены отдельным измерениям, но такая возможность должна быть предоставлена любому измерению |
|  | В чем заключается правило 7 «Динамическое управление разреженными матрицами, изложенное Коддом и определяющее OLAP? | Динамическое управление разреженными матрицами — OLAP-система должна обеспечивать оптимальную обработку разреженных матриц. Скорость доступа должна сохраняться вне зависимости от расположения ячеек данных и быть постоянной величиной для моделей, имеющих разное число измерений и различную степень разреженности данных |
|  | В чем заключается правило 8 «Поддержка многопользовательского режима», изложенное Коддом и определяющее OLAP? | Поддержка многопользовательского режима — OLAP-система должна предоставлять возможность работать нескольким пользователям совместно с одной аналитической моделью или создавать для них различные модели из единых данных. При этом возможны как чтение, так и запись данных, поэтому система должна обеспечивать их целостность и безопасность |
|  | В чем заключается правило 9 «Неограниченные перекрестные операции», изложенное Коддом и определяющее OLAP? | Неограниченные перекрестные операции — OLAP-система должна обеспечивать сохранение функциональных отношений, описанных с помощью определенного формального языка между ячейками гиперкуба при выполнении любых операций среза, вращения, консолидации или детализации. Система должна самостоятельно (автоматически) выполнять преобразование установленных отношений, не требуя от пользователя их переопределения |
|  | В чем заключается правило 10 «Интуитивная манипуляция данными», изложенное Коддом и определяющее OLAP? | Интуитивная манипуляция данными — OLAP-система должна предоставлять способ выполнения операций среза, вращения, консолидации и детализации над гиперкубом без необходимости пользователю совершать множество действий с интерфейсом. Измерения, определенные в аналитической модели, должны содержать всю необходимую информацию для выполнения вышеуказанных операций |
|  | В чем заключается правило 11 «Гибкие возможности получения отчетов», изложенное Коддом и определяющее OLAP? | Гибкие возможности получения отчетов — OLAP-система должна поддерживать различные способы визуализации данных, т. е. отчеты должны представляться в любой возможной ориентации. Средства формирования отчетов должны представлять синтезируемые данные или информацию, следующую из модели данных в ее любой возможной ориентации  |
|  | В чем заключается правило 12 «Неограниченная размерность и число уровней агрегации», изложенное Коддом и определяющее OLAP? | Неограниченная размерность и число уровней агрегации — исследование о возможном числе необходимых измерений, требующихся в аналитической модели, показало, что одновременно может использоваться до 19 измерений. Отсюда вытекает настоятельная рекомендация, чтобы аналитический инструмент мог одновременно предоставить хотя бы 15, а предпочтительно — 20 измерений.  |
|  | В 1995 г. Пендсон и Крит на основании правил Кодда разработали тест FASMI, определив OLAP как "Быстрый Анализ Разделяемой Многомерной Информации". В чем особенность данного теста? | FAST— OLAP-система должна обеспечивать выдачу большинства ответов пользователям в пределах приблизительно 5 с. При этом самые простые запросы обрабатываются в течение 1 с, и очень немногие более 20 с. |
|  | Назовите способы реализации OLAP-сервера  | Выделяют три основных способа реализации: MOLAP — для реализации многомерной модели используют многомерные БД; ROLAP — для реализации многомерной модели используют реляционные БД; HOLAP — для реализации многомерной модели используют и многомерные и реляционные БД |