|  |  |  |  |
| --- | --- | --- | --- |
| **ОПК-14. Способен осуществлять разработку, внедрение и эксплуатацию автоматизированных систем с учетом требований по защите информации, проводить подготовку исходных данных для технико-экономического обоснования** | | | |
| Индикаторы, дескрипторы достижения компетенции | Комплекс заданий для оценки компетенций  (сквозная нумерация) | Ключи правильных ответов | Критерии оценки |
| **Дисциплина «Технологии и методы программирования» (Б1.Б.27)** | | | |
| ИОПК -14.2 Осуществляет разработку, внедрение и сопровождение открытых информационных систем.  **Знать:**  − этапы жизненного цикла программного обеспечения (ИОПК-14.2);  − характеристики качества человеко-машинного интерфейса (ИОПК-14.2);  − методы отладки и тестирования программного обеспечения  (ИОПК-14.2) ;  − характеристики качества программного обеспечения  (ИОПК-14.2) .  **Уметь:**  − проводить отладку и тестирование программных модулей (ИОПК -14.2);  − составлять документацию на ПО (ИОПК -14.2);  **Владеть:**  − инструментами по отладке программного обеспечения  (ИОПК-14.2);  − методами тестирования программного обеспечения  (ИОПК -14.2) | **1.** Выберите все правильные варианты ответа.  Какие процессы из перечисленных далее относится к основным процессам жизненного цикла ПО?  1) разработка,  2) обеспечение качества,  3) эксплуатация. | 1, 3 | Верный ответ – 1 неверный – 0. |
| **2.** Выберите правильный вариант ответа.  Выберите модель разработки ПО, в котором все этапы жизненного цикла (ЖЦ) идут строго один за одним:  1) каскадная (водопадная) модель ЖЦ разработки ПО,  2) модель прототипирования,  3) итерационная модель ЖЦ разработки ПО. | 1 | Верный ответ – 1 неверный – 0. |
| **3.** Выберите правильный вариант ответа.  **Выберите правильное определение «программный дефект»:**  1) неправильный код программы (ошибка в коде);  2) неправильное состояние программы (ошибка в состоянии);  3) видимое неправильное поведение программы (ошибка в поведении), которое обнаруживает пользователь ПО. | 1 | Верный ответ – 1 неверный – 0. |
| **4.** Что из перечисленного **не относится** к методам выявления требований к ПО:  1) проведение интервью бизнес – аналитиков с пользователями;  2) проведение совместных семинаров разработчиков и пользователей;  3) наблюдение бизнес – аналитиков за пользователями на рабочих местах;  4) анализ документов. | 2 | Верный ответ – 1 неверный – 0. |
| **5.** Установите соответствие между названием и определением метода тестирования ПО по знанию о программном коде:   |  |  |  |  | | --- | --- | --- | --- | | А | Тестирование белого ящика | 1 | разработчик теста доступа к исходному коду программ не имеет | | Б | Тестирование черного ящика | 2 | разработчик теста имеет доступ к исходному коду программ, но при непосредственном выполнении тестов доступ к коду, как правило, не требуется | | В | Тестирование серого ящика | 3 | разработчик теста имеет доступ к исходному коду программ | | |  |  | | --- | --- | | А | 3 | | Б | 1 | | В | 2 | | Верный ответ – 1 неверный – 0. |
| **6.** Установите соответствие между названием и определением:   |  |  |  |  | | --- | --- | --- | --- | | А | дефект | 1 | неправильное состояние программы (ошибка в состоянии) | | Б | заражение | 2 | неправильный код программы (ошибка в коде), который создает программист | | В | сбой | 3 | видимое неправильное поведение программы (ошибка в поведении), которое обнаруживает человек (пользователь ПО) | | |  |  | | --- | --- | | А | 2 | | Б | 1 | | В | 3 | | Верный ответ – 1 неверный – 0. |
| **7.** Установите соответствие между названием и определением требований к ПО:   |  |  |  |  | | --- | --- | --- | --- | | А | Системные требования | 1 | проектирования и реализации накладывают границы на возможности выбора разработчика при проектировании продукта | | Б | Функциональные требования | 2 | определяют, каким должно быть поведение продукта в тех или иных условиях | | В | Ограничения | 3 | описывает требования к продукту, который содержит многие компоненты или подсистемы | | |  |  | | --- | --- | | А | 3 | | Б | 2 | | В | 1 | | Верный ответ – 1 неверный – 0. |
| **8.** Установите правильную последовательность процесса выбора характеристик качества:  1) выявление конкретных ожиданий по каждому атрибуту,  2) использование широкого набора атрибутов качества,  3) сокращение списка,  4) определение приоритетов атрибутов. | 2, 3, 4, 1 | Верный ответ – 1 неверный – 0. |
| **9.** Установите правильную последовательность тестирования в зависимости от глубины тестового покрытия:  1) смок тест,  2) тестирование только на корректных данных,  3) полное тестирование системы на корректных и некорректных данных. | 1, 2, 3 | Верный ответ – 1 неверный – 0. |
| **10.** Установите правильную последовательность процесса создания требований к системе  1) анализа требований,  2) выявления требований,  3) проверка спецификаций,  4) формулирование спецификаций. | 2, 1, 4, 3 | Верный ответ – 1 неверный – 0. |
| **11.** **Введите вначале наименование процесса**  \_\_\_\_\_\_\_\_\_\_— процесс исследования программного обеспечения (ПО) с целью получения информации о качестве продукта. | Тестирование | Верный ответ – 1 неверный – 0. |
| **12.** **Введите цвет ящика в родительном падеже**  При тестировании методом \_\_\_\_\_\_\_\_\_\_ ящика программа рассматривается как объект, внутренняя структура которого неизвестна. | черного | Верный ответ – 1 неверный – 0. |
| **13.** Введите ответ в поле ввода (в именительном падеже с большой буквы) наименование процесса:  \_\_\_\_\_\_\_\_\_\_ это процесс поиска существующей ошибки в программном обеспечении. | Отладка | Верный ответ – 1 неверный – 0. |
| **14.** Введите ответ в поле ввода (в именительном падеже с большой буквы):  \_\_\_\_\_\_\_\_\_\_ модель жизненного цикла ПО предполагает разбиение проекта на части (этапы) и прохождение этапов жизненного цикла на каждом их них. | Итерационная | Верный ответ – 1 неверный – 0. |
| **Дисциплина «Управление информационной безопасностью» (Б1.Б.40)** | | | |
| **ИОПК-14.1.** Применяет методы управления инцидентами информационной безопасности и непрерывности бизнеса при эксплуатации открытых информационных систем.  **Знать:**  − методы управления инцидентами информационной безопасности в открытых информационных системах  (ИОПК-14.1.)  **Уметь:**  − идентифицировать инциденты информационной безопасности в открытых информационных системах  (ИОПК-14.1.)  **Владеть:**  − методами реагирования на инциденты информационной безопасности в открытых информационных системах  (ИОПК - 14.1.) | **1. Как предотвращаются угрозы, связанные с физической безопасностью?**  1. Установкой антивирусных программ  2. Использованием систем контроля доступа и видеонаблюдения  3. Резервным копированием | 2 | Верный ответ – 1 балл, неверный – 0. |
| **2. Какую роль играет мониторинг в управлении информационной безопасностью?**  1. Помогает в раннем выявлении угроз и нарушений  2. Обновляет ПО  3. Архивирует файлы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **3. Что такое тестирование на проникновение (пен-тест)?**  1. Метод проверки системы на уязвимости с целью выявления потенциальных угроз  2. Хранение резервных копий  3. Создание отчетов | 1 | Верный ответ – 1 балл, неверный – 0. |
| **4. Какие действия могут быть предприняты в случае атаки вируса?**  1. Изолировать зараженные системы и провести восстановление из резервной копии  2. Установить новый фаервол  3. Перезапуск системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **5. Какую роль играет аудит в управлении инцидентами?**  1. Оценка произошедших инцидентов и выработка рекомендаций по предотвращению  2. Перезапуск серверов  3. Сжатие данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **6. Что такое управление рисками в информационной безопасности?**  1. Процесс уменьшения объема данных  2. Процесс оценки и минимизации угроз для информации и инфраструктуры  3. Управление файлообменом | 2 | Верный ответ – 1 балл, неверный – 0. |
| **7. Какую роль играет аудит в управлении информационной безопасностью?**  1. Сжатие данных  2. Оценка соответствия политик безопасности и выявление уязвимостей  3. Обновление программного обеспечения | 2 | Верный ответ – 1 балл, неверный – 0. |
| **8. Что такое критическая информация для организации?**  1. Личные файлы сотрудников  2. Информация, которая имеет наибольшее значение для функционирования организации  3. Архивные данные | 2 | Верный ответ – 1 балл, неверный – 0. |
| **9. Как можно классифицировать информацию по уровню важности?**  1. Только по объему данных  2. На основе конфиденциальности, ценности и воздействия на организацию  3. По времени хранения | 2 | Верный ответ – 1 балл, неверный – 0. |
| **10. Что такое ISO/IEC 27005?**  1. Стандарт безопасности для медицинской информации  2. Руководство по управлению рисками информационной безопасности  3. Стандарт для аудита систем | 2 | Верный ответ – 1 балл, неверный – 0. |
| **11. Что такое криптография в контексте информационной безопасности?**  1. Сжатие данных  2. Метод защиты информации с использованием шифрования  3. Сканирование файлов | 2 | Верный ответ – 1 балл, неверный – 0. |
| **12. Какой из этих методов используется для защиты данных на уровне приложения?**  1. Установка пароля на операционную систему  2. Шифрование данных в приложениях  3. Защита серверного оборудования | 2 | Верный ответ – 1 балл, неверный – 0. |
| **13. Что такое доступ на основе ролей (RBAC)?**  1. Метод контроля доступа, при котором пользователи получают доступ на основе их ролей  2. Метод хранения данных  3. Система архивации | 1 | Верный ответ – 1 балл, неверный – 0. |
| **14. Как называется процесс обеспечения целостности данных?**  1. Сжатие данных  2. Использование хеш-функций и цифровых подписей  3. Резервное копирование | 2 | Верный ответ – 1 балл, неверный – 0. |
| **15. Что такое защита от DDoS-атак?**  1. Методы защиты от перегрузки сетевых ресурсов с помощью распределенных атак  2. Шифрование данных  3. Аутентификация пользователей | 1 | Верный ответ – 1 балл, неверный – 0. |
| **16. Какую роль в управлении информационной безопасностью играет обучение сотрудников?**  1. Обучение сотрудников правильным методам защиты информации и предотвращения атак  2. Сжатие и хранение данных  3. Программное обеспечение для защиты от вирусов | 1 | Верный ответ – 1 балл, неверный – 0. |
| и  1. PCI DSS  2. ISO/IEC 27001  3. GDPR | 1 | Верный ответ – 1 балл, неверный – 0. |
| **18. Какой из методов управления информационной безопасностью является наиболее важным для защиты данных при передаче?**  1. Использование защищенных протоколов (например, HTTPS)  2. Обновление антивируса  3. Резервное копирование | 1 | Верный ответ – 1 балл, неверный – 0. |
| **19. Что такое план управления инцидентами безопасности?**  1. Метод мониторинга сети  2. Процесс быстрого реагирования на угрозы и инциденты безопасности  3. Метод повышения производительности системы | 2 | Верный ответ – 1 балл, неверный – 0. |
| **20. Что такое непрерывность бизнеса в контексте информационной безопасности?**  1. Процесс обеспечения минимальных потерь и восстановления работы при угрозах безопасности  2. Программное обеспечение для управления инцидентами  3. Уменьшение объемов данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **Дисциплина «Разработка и эксплуатация автоматизированных систем в защищенном исполнении» (Б1.Б.46)** | | | |
| **ИОПК-14.2.** Осуществляет разработку, внедрение и сопровождение открытых информационных систем.  **Знать:**  − стратегии профилактического обслуживания (ИОПК -14.2)  − основные характеристики и показатели надежности систем (ИОПК -14.2) − основные модели надежности, их построение и анализ (ИОПК-14.2)  − способы оценки параметров качества разрабатываемых и эксплуатируемых автоматизируемых систем (ИОПК -14.2) **Уметь:**  − строить модели надежности и выполнять их анализ (ИОПК -14.2)  **Владеть:**  − методами повышения качества функционирования автоматизированной системы (ИОПК-14.2) − аппаратом теории надежности (ИОПК-14.2) | 1. Что такое надежность в контексте инженерии?  1. Способность системы выполнять свои функции в течение заданного времени и при заданных условиях  2. Количество компонентов в системе  3. Способность системы работать без сбоев | 1 | Верный ответ – 1 балл, неверный – 0. |
| 2. Что такое отказ в теории надежности?  1. Невозможность системы выполнять свою функцию в соответствии с требованиями  2. Ожидаемая продолжительность работы системы  3. Снижение производительности системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| 3. Что такое вероятность отказа?  1. Вероятность того, что система или компонент выйдут из строя в течение заданного времени  2. Время работы системы до первого сбоя  3. Вероятность успешного выполнения операции | 1 | Верный ответ – 1 балл, неверный – 0. |
| 4. Что такое среднее время до отказа (MTTF)?  1. Среднее время, которое проходит до первого отказа системы или компонента  2. Время восстановления после отказа  3. Среднее количество отказов в системе | 1 | Верный ответ – 1 балл, неверный – 0. |
| 5. Какова роль теории надежности в проектировании систем?  1. Определение и управление рисками, минимизация вероятности отказов и повышение долговечности системы  2. Оценка производительности системы  3. Определение стоимости компонентов системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| 6. Что такое коэффициент надежности?  1. Это вероятность того, что система или компонент будут работать без отказа в течение заданного времени  2. Время, в течение которого система может работать без проблем  3. Коэффициент использования компонентов системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| 7. Каковы основные методы повышения надежности системы?  1. Резервирование, использование более надежных компонентов, повышение качества проектирования  2. Повышение скорости работы системы  3. Увеличение числа пользователей системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| 8. Что такое резервирование в контексте надежности?  1. Использование дополнительных компонентов или систем, которые могут заменить вышедшие из строя  2. Увеличение срока службы компонентов  3. Снижение затрат на эксплуатацию | 1 | Верный ответ – 1 балл, неверный – 0. |
| 9. Что такое отказоустойчивость системы?  1. Способность системы продолжать выполнение своих функций даже при отказах некоторых ее компонентов  2. Способность системы восстанавливать данные после сбоя  3. Время, необходимое для восстановления после отказа | 1 | Верный ответ – 1 балл, неверный – 0. |
| 10. Что такое система с избыточностью?  1. Система, в которой используется несколько компонентов или путей для выполнения одной и той же функции  2. Система, которая может работать только с одним компонентом  3. Система, не нуждающаяся в дополнительном обслуживании | 1 | Верный ответ – 1 балл, неверный – 0. |
| 11. Что такое функция надежности в теории надежности?  1. Функция, описывающая вероятность того, что система или компонент не выйдут из строя в течение определенного времени  2. Ожидаемое время работы системы  3. Время, необходимое для устранения отказа | 1 | Верный ответ – 1 балл, неверный – 0. |
| 12. Что такое функция распределения вероятности времени до отказа?  1. Функция, которая описывает вероятность того, что отказ произойдет в течение заданного времени  2. Среднее время работы системы  3. Функция, описывающая поведение отказа системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| 13. Что такое экспоненциальное распределение в теории надежности?  1. Математическая модель, которая описывает время до отказа компонента или системы с постоянной интенсивностью отказов  2. Модель, описывающая случайные колебания в системе  3. Модель, используемая для анализа производительности системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| 14. Какова особенность нормального распределения в контексте надежности?  1. Время до отказа распределяется нормально, когда среднее время до отказа значимо больше, чем вариация времени  2. Оно используется для моделирования только экстремальных отказов  3. Оно применяется только для краткосрочных систем | 1 | Верный ответ – 1 балл, неверный – 0. |
| 15. Что такое коэффициент интенсивности отказов?  1. Параметр, описывающий скорость появления отказов в системе  2. Среднее время до первого отказа  3. Параметр, описывающий производительность системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| 16. Что такое модель "системы с последовательным соединением"?  1. Система, в которой отказ любого компонента приводит к отказу всей системы  2. Система, состоящая только из одного компонента  3. Система, где каждый компонент независим и может функционировать автономно | 1 | Верный ответ – 1 балл, неверный – 0. |
| 17. Каково основное различие между параллельным и последовательным соединением компонентов в системе?  1. При параллельном соединении отказ одного компонента не приводит к отказу всей системы, при последовательном — приводит  2. Параллельные компоненты всегда более надежны  3. Последовательное соединение используется только в простых системах | 1 | Верный ответ – 1 балл, неверный – 0. |
| 18. Что такое метод Монте-Карло в расчетах надежности?  1. Метод, основанный на случайном моделировании для оценки надежности системы  2. Метод для определения стоимости компонентов  3. Метод для анализа временных задержек | 1 | Верный ответ – 1 балл, неверный – 0. |
| 19. Какую роль играет теорема о цепях в теории надежности?  1. Теорема позволяет рассчитать общую надежность системы, состоящей из нескольких взаимосвязанных компонентов  2. Она используется только для линейных систем  3. Теорема помогает вычислить среднее время до отказа | 1 | Верный ответ – 1 балл, неверный – 0. |
| 20. Что такое "метод наименьших квадратов" в расчете надежности?  1. Метод, используемый для нахождения наилучших оценок параметров модели на основе экспериментальных данных  2. Метод для анализа данных с фиксированными параметрами  3. Метод для вычисления средней продолжительности отказа | 1 | Верный ответ – 1 балл, неверный – 0. |