**ПК-2. Способен проводить разработку и анализ объектов информационной безопасности**

|  |  |  |  |
| --- | --- | --- | --- |
| Индикаторы, дескрипторы достижения компетенции | Комплекс заданий для оценки компетенций  (сквозная нумерация) | Ключи правильных ответов | Критерии оценки |
| **Дисциплина «Разработка и эксплуатация автоматизированных систем в защищенном исполнении» (Б1.Б.46)** | | | |
| **ИПК-2.1.** Разрабатывает защищенные открытые информационные системы  **ИПК-2.2.** Выполняет анализ защищенности информационных систем  **Знать:**  **−** основные характеристики и показатели надежности информационных систем (ИПК-2.1) − основные модели надежности информационных систем, их построение и анализ (ИПК-2.1) − психологические особенности взаимодействия человека с автоматизируемой системой (ИПК-2.1) − agile модели управления жизненным циклом программного обеспечения (ИПК-2.1) − модели, методы, шаблоны проектирования каркасов программного обеспечения (ИПК-2.1)  − основные характеристики и показатели надежности систем (ИПК-2.2) − стратегии профилактического обслуживания (ИПК2.2) − способы оценки параметров качества разрабатываемых и эксплуатируемых систем информационной безопасности (ИПК-2.2)  **Уметь:**  − сформулировать задачу обеспечения надежности (ИПК-2.1) − разрабатывать «дружественные» графические интерфейсы (ИПК-2.1) − выбирать модель жизненного цикла IT проекта и управлять проектом на всех этапах его жизненного цикла (ИПК-2.1) − обеспечить эргономическое качество автоматизированной системы (ИПК-2.1)  − профилактически обслуживать информационные системы(ИПК-2.2)  **Владеть:**  − аппаратом теории надежности, инструментарием и методами обеспечения и расчета надежности информационной системы (ИПК-2.1)  − методами повышения качества функционирования автоматизированной системы (ИПК-2.2) − методами верификации программного обеспечения (ИПК-2.2) | **1. Какие из следующих факторов влияют на надежность системы?**  1. Качество компонентов, дизайн системы, эксплуатационные условия  2. Только количество компонентов в системе  3. Только стоимость системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **2. Что такое фаллический граф в теории надежности?**  1. Граф, который используется для анализа структуры и взаимозависимости компонентов системы  2. Граф для представления отказов компонентов  3. Граф, описывающий производительность системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **3. Как используются методы надежности в атомных реакторах?**  1. Методы надежности применяются для предотвращения катастрофических сбоев и обеспечения бесперебойной работы системы  2. Они не применяются в таких системах  3. Методы надежности только для оценки производительности | 1 | Верный ответ – 1 балл, неверный – 0. |
| **4. Какие из следующих стратегий могут быть использованы для улучшения надежности системы?**  1. Использование резервирования, улучшение качества компонентов, применение методов предсказания отказов  2. Применение только новых компонентов  3. Снижение цены на компоненты | 1 | Верный ответ – 1 балл, неверный – 0. |
| **5. Что такое анализ жизненного цикла системы?**  1. Процесс оценки надежности системы на всех этапах ее жизни — от проектирования до вывода из эксплуатации  2. Процесс повышения производительности системы  3. Оценка стоимости системы на этапе производства | 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 систем | 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. |
| **Дисциплина «Анализ вредоносного программного обеспечения» (Б1.В.ОД.1)** | | | |
| **ИПК-2.2.** Выполняет анализ защищенности информационных систем  **Знать:**  − структуру вредоносных программ (ИПК-2.2)  − принципы проникновения и функционирования вредоносных программ (ИПК-2.2)  − основные типы вирусных атак (ИПК-2.2)  **Уметь:**  − проводить работы по сертификации средств защиты информации в автоматизированных системах (ИПК-2.2)  − проводить профилактику компьютерных систем на поиск уязвимостей от вирусного программного обеспечения (ИПК-2.2)  − выполнять поиск вредоносных программ и осуществлять действия по их извлечению (ИПК-2.2) **Владеть:**  − основными антивирусными инструментами; навыками использования антивирусного ПО (ИПК-2.2) | **1. Что такое вредоносное программное обеспечение?**  1. Программное обеспечение, разработанное с целью причинения ущерба компьютерам, сетям или данным  2. Программное обеспечение для повышения производительности  3. Программное обеспечение, предназначенное для исправления ошибок системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **2. Что такое вирус в контексте вредоносного ПО?**  1. Программа, которая может реплицировать себя и заражать другие программы или файлы  2. Программа, оптимизирующая работу компьютера  3. Программа, предназначенная для защиты системы от угроз | 1 | Верный ответ – 1 балл, неверный – 0. |
| **3. Какую функцию выполняет червь в контексте вредоносного ПО?**  1. Червь — это программа, которая распространяется через сети, заражая другие устройства  2. Червь — это способ восстановления файлов  3. Червь — это вирус, который работает только в интернете | 1 | Верный ответ – 1 балл, неверный – 0. |
| **4. Что такое троян в контексте вредоносного ПО?**  1. Программа, которая маскируется под безвредное ПО, но выполняет вредоносные действия  2. Программа для резервного копирования данных  3. Программа для повышения производительности компьютера | 1 | Верный ответ – 1 балл, неверный – 0. |
| **5. Какова основная цель анализа вредоносного ПО?**  1. Определить тип, поведение и цели вредоносной программы, а также способы защиты от нее  1. Проверить производительность программы  2. Составить список программ, которые необходимо установить | 1 | Верный ответ – 1 балл, неверный – 0. |
| **6. Что такое сэндбокс (sandbox) в анализе вредоносного ПО?**  1. Это изолированная среда, в которой можно безопасно запустить подозрительное ПО для анализа  2. Среда для резервного копирования данных  3. Программное обеспечение для защиты от вирусов | 1 | Верный ответ – 1 балл, неверный – 0. |
| **7. Какую информацию можно извлечь из анализа вредоносного ПО?**  1. Тип угрозы, методы распространения, способы предотвращения и устранения  2. Только стоимость вредоносного ПО  3. Время работы программы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **8. Что такое динамический анализ вредоносного ПО?**  1. Анализ программы в реальном времени с изучением ее поведения в процессе выполнения  2. Анализ исходного кода программы  3. Анализ программы без ее запуска | 1 | Верный ответ – 1 балл, неверный – 0. |
| **9. Что такое статический анализ вредоносного ПО?**  1. Анализ кода программы без ее выполнения, включая анализ структуры и команд  2. Анализ поведения программы в реальном времени  3. Анализ скорости работы программы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **10. Какие инструменты используются для анализа вредоносного ПО?**  1. Дебаггеры, дизассемблеры, виртуальные машины, сэндбоксы  2. Только антивирусные программы  3. Программы для восстановления данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **11. Что такое дизассемблирование в контексте анализа вредоносного ПО?**  1. Процесс преобразования исполняемого кода программы в ассемблерный язык для дальнейшего анализа  2. Процесс восстановления данных  3. Процесс компиляции программы в исходный код | 1 | Верный ответ – 1 балл, неверный – 0. |
| **12. Какое назначение имеет анализ сетевых активностей вредоносного ПО?**  1. Определение того, как вредоносное ПО использует сетевые ресурсы для распространения или выполнения атак  2. Определение размера программы  3. Определение типа операционной системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **13. Что такое эвристический анализ в контексте защиты от вредоносного ПО?**  1. Метод, который использует правила и алгоритмы для поиска неизвестных угроз, основанных на их поведении  2. Метод анализа только известных угроз  3. Метод восстановления данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **14. Как работают антивирусные программы для защиты от вредоносного ПО?**  1. Антивирусные программы сканируют файлы и процессы на наличие известных сигнатур вредоносных программ  2. Антивирусы только очищают систему от вирусов  3. Антивирусы восстанавливают поврежденные файлы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **15. Что такое поведенческий анализ в контексте обнаружения вредоносного ПО?**  1. Метод анализа, основанный на наблюдении за поведением программы во время ее выполнения  2. Метод анализа исходного кода программы  3. Метод восстановления поврежденных файлов | 1 | Верный ответ – 1 балл, неверный – 0. |
| **16. Что такое облачный анализ в контексте защиты от вредоносного ПО?**  1. Анализ угроз и вредоносных программ с использованием облачных вычислительных ресурсов для быстрого сканирования  2. Анализ только локальных файлов  3. Анализ производительности системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **17. Какую роль в анализе вредоносного ПО играет мониторинг системных вызовов?**  1. Системные вызовы позволяют отслеживать взаимодействие программы с операционной системой и выявлять подозрительные действия  2. Мониторинг системных вызовов не имеет значения для анализа  3. Мониторинг используется для проверки производительности программы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **18. Что такое виртуализация в анализе вредоносного ПО?**  1. Использование виртуальных машин для безопасного выполнения подозрительных программ и анализа их поведения  2. Использование виртуальных машин для увеличения производительности программы  3. Виртуализация компонентов операционной системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **19. Что такое сбор данных о поведении вредоносного ПО в сети?**  1. Анализ данных, полученных о сетевых действиях вредоносного ПО, чтобы понять, как оно распространяется и взаимодействует с другими системами  2. Сбор данных о производительности системы  3. Сбор данных о размере вредоносного ПО | 1 | Верный ответ – 1 балл, неверный – 0. |
| **20. Как анализируется влияние вредоносного ПО на систему?**  1. Путем наблюдения за изменениями в файлах, системных процессах, сетевых соединениях и системных настройках  2. Только путем восстановления удаленных данных  3. Путем анализа времени отклика системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **Дисциплина «Защищенное администрирование информационных систем» (Б1.В.ОД.2)** | | | |
| **ИПК-2.2.** Выполняет анализ защищенности информационных систем  **Знать:**  − структуру системы разграничения доступа (ИПК2.2)  **Уметь:**  − проводить анализ защищенности автоматизированных систем (ИПК-2.2) **Владеть:**  **−** средствами администрирования и управления ОС Linux (ИПК-2.2) − инструментами анализа качества работы ОС (ИПК2.2) | **1. Что такое защищенное администрирование информационных систем?**  1. Комплекс мероприятий и процедур, направленных на обеспечение безопасности информационной системы при ее эксплуатации  2. Процесс оптимизации работы системы  3. Управление пользовательскими правами в системе | 1 | Верный ответ – 1 балл, неверный – 0. |
| **2. Какова основная цель защищенного администрирования информационных систем?**  1. Обеспечение конфиденциальности, целостности и доступности данных, а также защиты от несанкционированного доступа  2. Повышение производительности системы  3. Обучение пользователей работе с системой | 1 | Верный ответ – 1 балл, неверный – 0. |
| **3. Какую роль в защищенном администрировании играет контроль доступа?**  1. Он ограничивает доступ пользователей и устройств к системе, предотвращая несанкционированный доступ к данным и ресурсам  2. Он используется для ускорения работы системы  3. Он помогает управлять приложениями в системе | 1 | Верный ответ – 1 балл, неверный – 0. |
| **4. Что такое управление учетными записями пользователей?**  1. Процесс создания, изменения и удаления учетных записей пользователей с учетом принципа минимальных прав  2. Процесс организации рабочих мест пользователей  3. Процесс защиты данных от утечек | 1 | Верный ответ – 1 балл, неверный – 0. |
| **5. Что такое политика безопасности информационной системы?**  1. Набор правил и процедур, направленных на обеспечение безопасности системы и защиту данных  2. Правила использования системы  3. Стратегия оптимизации работы системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **6. Какова цель разграничения доступа в защищенной информационной системе?**  1. Предотвратить несанкционированный доступ к данным и ресурсам, а также ограничить права пользователей в соответствии с их ролями  2. Обеспечить доступ ко всем данным для всех пользователей  3. Ускорить работу системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **7. Что такое аудит безопасности в контексте защищенного администрирования?**  1. Процесс мониторинга и анализа действий пользователей и системных процессов для выявления нарушений политики безопасности  2. Процесс оптимизации работы системы  3. Процесс устранения неполадок в системе | 1 | Верный ответ – 1 балл, неверный – 0. |
| **8. Какова роль резервного копирования в защите информации?**  1. Создание резервных копий данных для восстановления в случае утраты или повреждения информации  2. Оптимизация использования памяти  3. Ускорение работы системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **9. Что такое шифрование данных в контексте защищенного администрирования?**  1. Процесс преобразования данных в нечитаемую форму с целью защиты от несанкционированного доступа  2. Процесс ускорения обработки данных  3. Процесс архивации данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **10. Какую роль играют средства защиты от вирусов и вредоносного ПО в системе безопасности?**  1. Предотвращают заражение системы вирусами и другим вредоносным ПО, которое может нарушить работу системы  2. Защищают систему от переполнения памяти  3. Предотвращают сбои системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **11. Что такое многофакторная аутентификация?**  1. Процесс, при котором для доступа к системе требуется несколько способов подтверждения личности пользователя  2. Процесс подтверждения личности с помощью одного пароля  3. Процесс повышения скорости работы системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **12. Как работает фаервол в контексте защищенного администрирования?**  1. Он контролирует и фильтрует входящий и исходящий трафик между сетью и системой  2. Он ускоряет работу системы  3. Он предотвращает доступ пользователей к сети | 1 | Верный ответ – 1 балл, неверный – 0. |
| **13. Каковы основные принципы настройки прав доступа в информационных системах?**  1. Принцип минимальных прав, принцип разделения обязанностей, принцип наименьшего воздействия  2. Принцип максимальной доступности  3. Принцип полной открытости доступа | 1 | Верный ответ – 1 балл, неверный – 0. |
| **14. Что такое защита от DDoS-атак в администрировании информационных систем?**  1. Механизмы, направленные на предотвращение перегрузки системы с помощью массовых запросов  2. Защита от несанкционированного доступа  3. Защита от физических повреждений системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **15. Какую роль играют журналы безопасности в информационных системах?**  1. Они помогают отслеживать действия пользователей и системных процессов для анализа и выявления угроз безопасности  2. Они ускоряют работу системы  3. Они сохраняют резервные копии данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **16. Что такое виртуализация в контексте безопасности информационных систем?**  1. Процесс создания виртуальных машин, которые изолируют приложения и системы, обеспечивая дополнительный уровень безопасности  2. Процесс использования нескольких операционных систем на одном устройстве  3. Процесс увеличения мощности системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **17. Какие меры защиты используются для предотвращения утечек информации через каналы связи?**  1. Шифрование данных, мониторинг трафика, контроль доступа к сети  2. Применение антивирусных программ  3. Ограничение скорости передачи данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **18. Какую роль играет двухфакторная аутентификация?**  1. Она требует подтверждения личности пользователя через два различных канала, таких как пароль и код, отправленный на мобильное устройство  2. Она используется только для ускорения работы системы  3. Она ограничивает права пользователей в системе | 1 | Верный ответ – 1 балл, неверный – 0. |
| **19. Что такое защита от утечек данных (DLP-системы)?**  1. Технологии, направленные на мониторинг и блокировку утечек конфиденциальной информации из системы  2. Программы для ускорения работы системы  3. Программы для защиты от вирусов | 1 | Верный ответ – 1 балл, неверный – 0. |
| **20. Какую функцию выполняют средства защиты от вирусов и шпионских программ?**  1. Они обнаруживают и блокируют вирусы и другие угрозы для системы безопасности  2. Они ускоряют выполнение программ  3. Они восстанавливают поврежденные файлы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **Дисциплина «Комплексная защита информации» (Б1.В.ОД.3)** | | | |
| **ИПК-2.2.** Выполняет анализ защищенности информационных систем  **Знать:**  − цели и задачи построения КСЗИ (ИПК-2.2)  − общие принципы проектирования КСЗИ (ИПК-2.2)  − принципы системы управления службы безопасности предприятия (ИПК-2.2)  − факторы, влияющие на организацию КСЗИ (ИПК2.2)  − международные модели и стандарты проектирования КСЗИ (ИПК-2.2)  − виды политик информационной безопасности (ИПК-2.2)  − основные угрозы и уязвимости информационных систем (ИПК-2.2)  − модели безопасности компьютерных систем (ИПК2.2)  − правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в организации (ИПК-2.2)  − организационные меры по защите информации (ИПК-2.2)  **Уметь:**  − выявлять и оценивать источники угроз (ИПК-2.2)  − выявлять способы дестабилизирующего воздействия на информацию (ИПК-2.2)  − применять российскую и международную практику построения проблемно-ориентированных КСЗИ (ИПК-2.2)  − организовать службу защиты информации в соответствии с нормативными правовыми актами, нормативными и методическими документами органов государственной власти (ИПК-2.2)  − реализовывать и проводить анализ политик информационной безопасности (ИПК-2.2)  − оценивать риски информационной безопасности в отношении компьютерных систем (ИПК-2.2)  − оформлять аналитический отчет по результатам проведенного анализа (ИПК-2.2)  − разрабатывать предложения по устранению выявленных уязвимостей (ИПК-2.2)  **Владеть:**  − методами аудита информационной безопасности предприятий различных форм собственности (ИПК2.2)  − методами построение процессов системы управления КСЗИ (ИПК-2.2) | **1. Что представляет собой комплексная защита информации?**  1. Это система мер, направленных на защиту данных от различных угроз, включая физическую, техническую, организационную и программную защиту  2. Защита только от вирусов  3. Защита от утечек информации через интернет | 1 | Верный ответ – 1 балл, неверный – 0. |
| **2. Какова основная цель комплексной защиты информации?**  1. Обеспечение конфиденциальности, целостности и доступности информации, а также защита от утечек и несанкционированного доступа  2. Ускорение работы с информацией  3. Повышение производительности системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **3. Какие виды угроз защищает комплексная защита информации?**  1. Физические, технические, организационные и программные угрозы безопасности  2. Только физические угрозы  3. Только вирусные атаки | 1 | Верный ответ – 1 балл, неверный – 0. |
| **4. Какую роль в комплексной защите информации играет шифрование?**  1. Шифрование защищает данные, превращая их в нечитаемую форму для защиты от несанкционированного доступа  2. Ускоряет передачу данных  3. Упрощает работу с информацией | 1 | Верный ответ – 1 балл, неверный – 0. |
| **5. Что такое контроль доступа в контексте комплексной защиты информации?**  1. Процесс ограничения прав доступа к данным и ресурсам системы, чтобы только авторизованные пользователи могли работать с информацией  2. Управление данными  3. Контроль качества информации | 1 | Верный ответ – 1 балл, неверный – 0. |
| **6. Каковы основные компоненты комплексной защиты информации?**  1. Технические средства, организационные меры, юридические подходы и средства защиты данных  2. Только программные средства защиты  3. Только физическая безопасность | 1 | Верный ответ – 1 балл, неверный – 0. |
| **7. Что такое многофакторная аутентификация?**  1. Процесс подтверждения личности пользователя с использованием двух или более факторов (например, пароль и отпечаток пальца)  2. Использование одного пароля для всех пользователей  3. Контроль за действиями пользователя в системе | 1 | Верный ответ – 1 балл, неверный – 0. |
| **8. Какую роль играют средства защиты от вредоносного ПО в комплексной защите информации?**  1. Они обнаруживают и блокируют вирусы и другое вредоносное ПО, которое может угрожать безопасности данных  2. Они ускоряют работу системы  3. Они помогают защищать данные от внешних атак | 1 | Верный ответ – 1 балл, неверный – 0. |
| **9. Что такое аудит безопасности в рамках комплексной защиты информации?**  1. Процесс мониторинга и анализа действий пользователей, системных процессов и событий безопасности для выявления нарушений  2. Установка программных обновлений  3. Оценка производительности системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **10. Какова роль обучения сотрудников в комплексной защите информации?**  1. Обучение сотрудников правильному обращению с данными и системами безопасности помогает предотвратить ошибки и утечки информации  2. Обучение для повышения производительности  3. Обучение для упрощения работы с системой | 1 | Верный ответ – 1 балл, неверный – 0. |
| **11. Какой метод защиты информации используется для защиты данных при их передаче?**  1. Шифрование данных при передаче по сети  2. Использование надежных паролей  3. Ограничение доступа к сети | 1 | Верный ответ – 1 балл, неверный – 0. |
| **12. Что такое защита данных в облачных сервисах?**  1. Использование шифрования и контроля доступа для защиты данных, размещенных в облаке, от несанкционированного доступа и утечек  2. Использование только облачных сервисов  3. Защита данных на локальных устройствах | 1 | Верный ответ – 1 балл, неверный – 0. |
| **13. Какую роль играет резервное копирование данных в комплексной защите?**  1. Резервные копии данных позволяют восстановить информацию в случае ее потери или повреждения  2. Ускоряет доступ к данным  3. Упрощает хранение данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **14. Что такое защита информации на уровне базы данных?**  1. Применение методов шифрования и контроля доступа для защиты данных, хранимых в базе данных  2. Обновление данных в базе  3. Разделение данных по категориям | 1 | Верный ответ – 1 балл, неверный – 0. |
| **15. Какой механизм помогает защищать информацию от угроз, связанных с внутренними пользователями?**  1. Политики минимальных прав доступа и мониторинг действий пользователей  2. Удаление пользователей из системы  3. Разделение пользователей по типам | 1 | Верный ответ – 1 балл, неверный – 0. |
| **16. Что такое системы предотвращения вторжений (IPS)?**  1. Системы, которые анализируют трафик сети и блокируют подозрительные действия, предотвращая вторжения  2. Системы для ускорения работы сети  3. Программы для создания резервных копий | 1 | Верный ответ – 1 балл, неверный – 0. |
| **17. Какую роль играет защита от атак типа "отказ в обслуживании" (DoS)?**  1. Механизмы, предотвращающие перегрузку системы чрезмерным количеством запросов  2. Защита от вирусов  3. Защита от потери данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **18. Какую роль в защите информации играют фаерволы?**  1. Они фильтруют и контролируют входящий и исходящий трафик, предотвращая несанкционированный доступ к сети  2. Защита от физических повреждений  3. Ускорение работы системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **19. Что такое использование виртуальных частных сетей (VPN) для защиты информации?**  1. VPN шифрует трафик и защищает его от перехвата при передаче через небезопасные сети, такие как интернет  2. Применение фаервола  3. Создание резервных копий данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **20. Какую роль играет контроль версий в защите информации?**  1. Контроль версий позволяет отслеживать изменения в данных и программном обеспечении, предотвращая несанкционированные модификации  2. Контроль за выполнением программ  3. Повышение производительности системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **Дисциплина «Интеллектуальный анализ данных» (Б1.В.ОД.4)** | | | |
| **ИПК-2.1.** Разрабатывает защищенные открытые информационные системы  **ИПК-2.2.** Выполняет анализ защищенности информационных систем  **Знать:**  − основные тренды развития технологий больших данных (ИПК-2.1);  − платформы реализации технологий больших данных (ИПК-2.1);  **Уметь:**  − проводить анализ, предлагать и обосновывать выбор решений на основе технологии больших данных (ИПК-2.2);  − разрабатывать приложения для платформ больших данных (ИПК-2.1);  − реализовывать на практике программы с применением технологий больших данных (ИПК-2.1); **Владеть:**  − основными алгоритмами, применяемыми в технологиях больших данных (ИПК-2.1). | **1. Что такое интеллектуальный анализ данных (Data Mining)?**  1. Процесс извлечения полезной информации и знаний из больших объемов данных с помощью различных методов и алгоритмов  2. Процесс хранения данных  3. Процесс архивации данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **2. Какую роль играет предобработка данных в интеллектуальном анализе?**  1. Предобработка данных помогает очистить и подготовить данные для дальнейшего анализа, улучшая качество результатов  2. Ускоряет процесс анализа данных  3. Создает отчеты на основе данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **3. Какие задачи решает интеллектуальный анализ данных?**  1. Прогнозирование, классификация, кластеризация, ассоциативный анализ, выявление аномалий и др.  2. Только классификация данных  3. Только сбор и хранение данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **4. Что такое классификация в интеллектуальном анализе данных?**  1. Процесс разделения данных на заранее определенные категории или классы  2. Процесс сбора данных  3. Процесс хранения данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **5. Что такое кластеризация в контексте анализа данных?**  1. Процесс группировки объектов, данных или наблюдений в кластеры, где объекты внутри кластера схожи друг с другом  2. Процесс классификации данных  3. Процесс шифрования данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **6. Какова роль ассоциативных правил в интеллектуальном анализе данных?**  1. Ассоциативные правила помогают выявлять закономерности и связи между различными переменными в данных  2. Они используются для классификации данных  3. Они используются для создания отчетов | 1 | Верный ответ – 1 балл, неверный – 0. |
| **7. Какую задачу решает метод регрессии в анализе данных?**  1. Метод регрессии используется для предсказания числовых значений на основе исторических данных  2. Он используется для разделения данных на категории  3. Он используется для шифрования данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **8. Что такое поддержка и доверие в контексте ассоциативного анализа?**  1. Поддержка - это частота появления определенной ассоциации в данных, доверие - это вероятность того, что одна ассоциация следует за другой  2. Оценка производительности системы  3. Оценка стоимости хранения данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **9. Что такое алгоритм кластеризации k-средних?**  1. Алгоритм, который делит данные на k кластеров, минимизируя расстояние между объектами внутри каждого кластера  2. Алгоритм для классификации текстов  3. Алгоритм для поиска ассоциативных правил | 1 | Верный ответ – 1 балл, неверный – 0. |
| **10. Какую роль играет визуализация данных в интеллектуальном анализе?**  1. Визуализация помогает анализировать и интерпретировать результаты анализа данных, представляя их в графическом виде  2. Визуализация ускоряет процесс обработки данных  3. Визуализация используется только для хранения данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **11. Что такое метод поддержки векторных машин (SVM)?**  1. Метод классификации, который ищет гиперплоскость, максимально разделяющую данные разных классов  2. Метод для кластеризации данных  3. Метод для предсказания числовых значений | 1 | Верный ответ – 1 балл, неверный – 0. |
| **12. Как работает метод ближайших соседей (KNN)?**  1. Метод классификации и регрессии, который основывается на сходстве с ближайшими объектами в обучающем наборе данных  2. Метод для сжатия данных  3. Метод для вычисления ассоциативных правил | 1 | Верный ответ – 1 балл, неверный – 0. |
| **13. Какую роль играет алгоритм наивного байесовского классификатора в** интеллектуальном анализе данных?  1. Алгоритм, который используется для классификации данных, предполагая независимость признаков  2. Алгоритм для предсказания числовых значений  3. Алгоритм для кластеризации данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **14. Что такое анализ чувствительности в интеллектуальном анализе данных?**  1. Анализ, направленный на определение того, как изменения входных данных могут повлиять на результаты анализа  2. Оценка качества данных  3. Процесс предобработки данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **15. Какую задачу решает алгоритм дерева решений?**  1. Алгоритм, который используется для классификации и регрессии путем разделения данных на основе условий, представленных в виде дерева  2. Алгоритм для создания ассоциативных правил  3. Алгоритм для шифрования данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **16. Что такое анализ временных рядов в контексте анализа данных?**  1. Анализ временных рядов включает в себя изучение данных, собранных во времени, для предсказания будущих значений  2. Анализ статичных данных  3. Кластеризация данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **17. Какие данные используются для анализа в задачах интеллектуального анализа?**  1. Большие объемы структурированных и неструктурированных данных, полученных из различных источников  2. Только структурированные данные  3. Только текстовые данные | 1 | Верный ответ – 1 балл, неверный – 0. |
| **18. Что такое алгоритм генетических алгоритмов в контексте анализа данных?**  1. Алгоритм, который использует механизмы эволюции (например, отбор, мутации, кроссинговер) для поиска решения  2. Алгоритм для классификации текстов  3. Алгоритм для сжатия данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **19. Какова цель использования кластеризации в интеллектуальном анализе?**  1. Кластеризация позволяет группировать данные в отдельные группы, что помогает в выявлении скрытых закономерностей  2. Оценка рисков  3. Прогнозирование значений | 1 | Верный ответ – 1 балл, неверный – 0. |
| **20. Как работает метод нейронных сетей в интеллектуальном анализе данных?**  1. Нейронные сети моделируют работу человеческого мозга для решения задач классификации, регрессии и кластеризации  2. Это метод предсказания будущих значений  3. Это метод для создания отчетов о данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **Дисциплина «Основы построения защищенных компьютерных сетей» (Б1.В.ОД.6)** | | | |
| **ИПК-2.1.** Разрабатывает защищенные открытые информационные системы  **ИПК-2.2.** Выполняет анализ защищенности информационных систем  **Знать:**  − основные понятия информационной безопасности в компьютерных сетях  − технологии обеспечения безопасности в локальных сетях  − основные протоколы, службы, функционирование, средства обеспечения безопасности, средства управления и контроля  − типовые угрозы сетевой безопасности  − основные критерии анализа сетевой безопасности  **Уметь:**  − выполнять процедуры анализа сетевой безопасности  − применять защищенные протоколы, межсетевые экраны и средства обнаружения вторжений для защиты информации в сетях  − осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты  **Владеть:**  − методами обеспечения безопасности телекоммуникационных связей и административный контроль  − средствами повышения надежности и безопасности функционирования компьютерных сетей  − методами анализа результатов работы средств обнаружения вторжений | **1. Что такое защищенная компьютерная сеть?**  1. Сеть, которая использует различные методы и технологии для защиты данных от несанкционированного доступа и атак  2. Сеть с высокой пропускной способностью  3. Сеть, использующая только проводное соединение | 1 | Верный ответ – 1 балл, неверный – 0. |
| **2. Каковы основные угрозы безопасности компьютерных сетей?**  1. Несанкционированный доступ, вирусы, атаки типа "отказ в обслуживании", утечка данных  2. Низкая скорость передачи данных  3. Проблемы с подключением к интернету | 1 | Верный ответ – 1 балл, неверный – 0. |
| **3. Что такое модель безопасности "CIA" в контексте компьютерных сетей?**  1. Конфиденциальность, целостность и доступность данных  2. Модель, описывающая физические устройства в сети  3. Модель для управления трафиком сети | 1 | Верный ответ – 1 балл, неверный – 0. |
| **4. Какой метод используется для обеспечения конфиденциальности данных в защищенной сети?**  1. Шифрование данных  2. Использование слабых паролей  3. Ограничение пропускной способности | 1 | Верный ответ – 1 балл, неверный – 0. |
| **5. Что такое "firewall" (межсетевой экран)?**  1. Устройство или программное обеспечение для контроля и фильтрации входящего и исходящего трафика сети  2. Программа для улучшения производительности сети  3. Устройство для увеличения скорости интернета | 1 | Верный ответ – 1 балл, неверный – 0. |
| **6. Что такое VPN (виртуальная частная сеть)?**  1. Технология для создания защищенного канала связи между удаленными узлами через общедоступную сеть  2. Протокол маршрутизации данных в сети  3. Программное обеспечение для ускорения сети | 1 | Верный ответ – 1 балл, неверный – 0. |
| **7. Какие типы межсетевых экранов существуют?**  1. Фильтрующий, прокси-сервер, stateful inspection  2. Только аппаратные  3. Только программные | 1 | Верный ответ – 1 балл, неверный – 0. |
| **8. Какую роль играет аутентификация в защите компьютерных сетей?**  1. Аутентификация проверяет подлинность пользователей, предотвращая несанкционированный доступ  2. Аутентификация увеличивает скорость передачи данных  3. Аутентификация не влияет на безопасность | 1 | Верный ответ – 1 балл, неверный – 0. |
| **9. Что такое политика безопасности в компьютерной сети?**  1. Набор правил и процедур, направленных на защиту информации в сети  2. Процесс настройки маршрутизаторов  3. Программа для мониторинга трафика | 1 | Верный ответ – 1 балл, неверный – 0. |
| **10. Какую роль в защите сетей играют антивирусные программы?**  1. Они защищают от вирусов и другого вредоносного ПО, которое может угрожать безопасности сети  2. Улучшают производительность сети  3. Применяют шифрование данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **11. Какие атаки могут быть направлены на компьютерные сети?**  1. Отказ в обслуживании (DoS), подмена адреса (spoofing), перехват трафика (sniffing)  2. Проблемы с подключением устройств к сети  3. Ошибки в маршрутизации | 1 | Верный ответ – 1 балл, неверный – 0. |
| **12. Что такое атака "отказ в обслуживании" (DoS)?**  1. Атака, направленная на перегрузку системы или сети, делая её недоступной для пользователей  2. Атака на физическую инфраструктуру сети  3. Ошибка в алгоритмах маршрутизации | 1 | Верный ответ – 1 балл, неверный – 0. |
| **13. Какие механизмы защиты могут использоваться для предотвращения DDoS-атак?**  1. Использование систем распределенной защиты, фильтрации трафика, балансировки нагрузки  2. Увеличение скорости интернет-соединения  3. Шифрование трафика | 1 | Верный ответ – 1 балл, неверный – 0. |
| **14. Как работают технологии IDS/IPS (системы обнаружения и предотвращения вторжений)?**  1. Они анализируют трафик сети на наличие подозрительных действий и могут блокировать их  2. Используют механизмы шифрования  3. Улучшают скорость работы сети | 1 | Верный ответ – 1 балл, неверный – 0. |
| **15. Какой основной принцип лежит в основе концепции "сегментации сети"?**  1. Разделение сети на изолированные части для минимизации ущерба при атаке  2. Использование одного маршрутизатора для всех устройств  3. Снижение скорости сети для уменьшения угроз | 1 | Верный ответ – 1 балл, неверный – 0. |
| **16. Какую роль играют DNS-серверы в безопасности сети?**  1. DNS-серверы могут быть целью атак, таких как DNS-спуфинг, и должны быть защищены от манипуляций с записями  2. Ускоряют передачу данных  3. Улучшают маршрутизацию трафика | 1 | Верный ответ – 1 балл, неверный – 0. |
| **17. Что такое "DNS-спуфинг"?**  1. Атака, при которой злоумышленник подменяет записи DNS-сервера, направляя трафик на фальшивые сайты  2. Способ ускорения работы DNS-сервера  3. Метод защиты DNS-серверов от атак | 1 | Верный ответ – 1 балл, неверный – 0. |
| **18. Как работают технологии "антивирусной фильтрации" в сети?**  1. Они анализируют входящий и исходящий трафик на наличие вредоносных программ и блокируют их  2. Фильтруют только текстовую информацию  3. Обеспечивают передачу данных без потерь | 1 | Верный ответ – 1 балл, неверный – 0. |
| **19. Какую роль играют прокси-серверы в защите сети?**  1. Прокси-серверы скрывают реальный IP-адрес пользователей, фильтруют трафик и защищают от внешних атак  2. Прокси-серверы увеличивают скорость сети  3. Прокси-серверы обеспечивают защищенное соединение с интернетом | 1 | Верный ответ – 1 балл, неверный – 0. |
| **20. Как предотвращается утечка информации через сеть?**  1. Использование шифрования данных, мониторинг и контроль доступа к сетевым ресурсам  2. Ограничение пропускной способности сети  3. Установка антивирусных программ на устройства | 1 | Верный ответ – 1 балл, неверный – 0. |
| **Дисциплина «Шаблоны проектирования программного обеспечения» (Б1.В.ДВ.1.1)** | | | |
| **ИПК-2.1.** Разрабатывает защищенные открытые информационные системы  **Знать:**  средства автоматизации разработки программного обеспечения открытых информационных систем (ИПК-2.1)  **Уметь:**  вести разработку программного обеспечения в интегрированных среде разработки Intellij Idea (ИПК-2.1)  применять шаблоны объектно-ориентированного проектирования для обеспечения слабой связности модулей программного обеспечения. (ИПК-2.1)  **Владеть:**  современными инструментами сборки программных проектов. (ИПК-2.1)  базовыми методами отладки и тестирования объектно-ориентированных программных систем. (ИПК-2.1) | **1. Какой способ создания и запуска потоков корректен?**  1. Создать объект класса Runnable. 2. Вызвать у созданного объекта метод run() (после этого начнет выполняться метод start(), реализованный у переданного объекта)  2. Создать объект класса ClassName extends Thread. 2. Вызвать у созданного объекта метод start() (после этого начнет выполняться метод run(), реализованный у переданного объекта)  3. Создать объект класса ClassName implements Thread. 2. Вызвать у созданного объекта метод start() (после этого начнет выполняться метод run(), реализованный у переданного объекта)  4. Создать объект класса ClassName implements Runnable. 2. Вызвать у созданного объекта метод run() (после этого начнет выполняться метод start(), реализованный у переданного объекта) | 2 | Верный ответ – 1 балл, неверный – 0. |
| 1. **2. Чем отличаются методы interrupt, interrupted, isInterrupted?**   1. interrupt() — устанавливает флаг прерывания потока  isInterrupted() — возвращает состояние флага прерывания и оставляет этот флаг нетронутым.  interrupted() — возвращает состояние флага и сбрасывает его.  2. interrupt() — возвращает состояние флага и сбрасывает его.  isInterrupted() — возвращает состояние флага прерывания и оставляет этот флаг нетронутым.  interrupted() — устанавливает флаг прерывания потока  3. interrupt() — возвращает состояние флага прерывания и оставляет этот флаг нетронутым.  isInterrupted() — возвращает состояние флага и сбрасывает его.  interrupted() — устанавливает флаг прерывания потока  4. interrupt() — устанавливает флаг прерывания потока  isInterrupted() — возвращает состояние флага и сбрасывает его.  interrupted() — возвращает состояние флага прерывания и оставляет этот флаг нетронутым. | 1 | Верный ответ – 1 балл, неверный – 0. |
| 1. **3. Для потока справедливо следующее утверждение:**   1. Сбой одного потока всегда влияет на другой поток  2. Поток – это информация о текущем состоянии выполнения, включая регистры процессора и системные данные  3. Поток – это «легковесный» подкомпонент процесса, который выполняется в контексте процесса и разделяет с ним память и ресурсы. | 3 | Верный ответ – 1 балл, неверный – 0. |
| 1. **4. Семафор обеспечивает пропуск в критическую секцию:**   1. строго один поток,  2. 2 потока,  3. 3 потока,  4. Любое количество потоков в условиях ограничений на вычислительные ресурсы | 4 | Верный ответ – 1 балл, неверный – 0. |
| 1. **5. Какой задачи межпроцессного взаимодействия не существует:**   1. «Инкапсуляция поведения»  2. «Читатели Писатели»  3. «Спящий брадобрей»  4. «Обедающие философы» | 1 | Верный ответ – 1 балл, неверный – 0. |
| 1. **6. Установите соответствие между названием понятиями ресурса и определениями**   А. Разделяемый  Б. Потокобезопасный  В. Потоконебезопасный  1. Это объект или структура данных, которая может использоваться несколькими потоками одновременно без риска повреждения данных, состояния гонки (race conditions) или взаимоблокировок (deadlocks).  2. Ресурс, доступ к которому может быть предоставлен нескольким процессам или потокам одновременно, но который требует координации для предотвращения конфликтов, некорректной работы или повреждения данных.  3.Это объект или структура данных, которая не обеспечивает корректной работы при доступе из нескольких потоков одновременно. | А-2  Б-1  В-3 | Верный ответ – 1 балл, неверный – 0. |
| 1. **7. Установите соответствие между командами:**   А. down(mutex)  Б. up(mutex)  В. down(semaphor)  Г. up(semaphor)  1. l.unlock()  2. s.acquire()  3. s.release()  4. l.lock() | А-4  Б-1  В-2  Г-3 | Верный ответ – 1 балл, неверный – 0. |
| 1. **8. Установите соответствие между концепциями Java Concurrency и их описаниями.**   А. ThreadPool  Б. ReentrantLock  В. volatile  1. Гибкая альтернатива synchronized, которая позволяет более точно контролировать блокировки.  2. Маркирует переменную как доступную для нескольких потоков, гарантируя видимость изменений.  3. Упрощает управление потоками за счёт повторного использования уже созданных потоков. | А-3  Б-1  В-2 | Верный ответ – 1 балл, неверный – 0. |
| 1. **9. Установите соответствие между названием метода и его определением:**   А. wait()  Б. notify()  В. notifyAll()  1. Пробуждает все потоки, находящиеся в состоянии ожидания на данном объекте.  2. Поток, вызвавший этот метод, переходит в состояние ожидания, освобождая монитор объекта.  3. Пробуждает один из потоков, который находится в состоянии ожидания на данном объекте. | А-2  Б-3  В-1 | Верный ответ – 1 балл, неверный – 0. |
| 1. **10. Установите соответствие между видом интерфейса и его определением:**   А. интерфейс  Б. маркер-интерфейс  В. функциональный интерфейс  1. Тип в Java, который определяет набор методов, которые класс должен реализовать и используемый для достижения абстракции и создания контрактов между компонентами системы.  2. Содержит только один абстрактный метод.  3. Не содержит методов и полей, используется для предоставления определённой метаинформации о классе. | А-1  Б-3  В-2 | Верный ответ – 1 балл, неверный – 0. |
| 1. **11. Установите правильную последовательность работы synchronized блока**   1. Поток выполняет код внутри блока  2. Другие потоки могут получить доступ к монитору  3. Поток захватывает монитор объекта  4. Поток освобождает монитор объекта | 3, 1, 4, 2 | Верный ответ – 1 балл, неверный – 0. |
| 1. **12. Установите правильную последовательность работы метода wait().**   1. поток освобождает монитор  2. Поток ожидает вызова notify() или notifyAll()  3. Поток переводится в состояние ожидания  4. Поток снова захватывает монитор | 1, 3, 2,4 | Верный ответ – 1 балл, неверный – 0. |
| 1. **13. Установите правильную последовательность работы ReentrantLock()**   1. поток пытается захватить блокировку (lock())  2. Поток выполняет критическую секцию.  3. Поток освобождает блокировку (unlock()).  4. Другой поток получает доступ к блокировке. | 1,2,3,4 | Верный ответ – 1 балл, неверный – 0. |
| 1. **14. Какова правильная последовательность работы с аннотацией @Configuration в Spring?**   1. методы с аннотацией @Bean вызываются для создания экземпляров.  2. контекст Spring сканирует класс и обнаруживает аннотацию @Configuration.  3. бины регистрируются в контейнере IoC Spring.  4. класс с аннотацией @Configuration создаётся. | 4, 2, 1, 3 | Верный ответ – 1 балл, неверный – 0. |
| 1. **15. Установите правильную последовательность действий с которой @ComponentScan обнаруживает компоненты?**   1. Сканирует указанные пакеты на наличие классов с аннотацией @Component  2. Проверяет производные аннотации: @Service, @Repository, @Controller  3. Создаёт бины для обнаруженных классов | 1, 2, 3 | Верный ответ – 1 балл, неверный – 0. |
| **16. Режим, при котором поток постоянно опрашивает условия в ожидании попадания в критическую секцию называется …** | активное ожидание | Верный ответ – 1 балл, неверный – 0. |
| **17.** Два процесса не должны одновременно находиться в критических областях, в программе не должно быть предположений о скорости или количестве процессоров, процесс, находящийся вне критической области, не может блокировать другие процессы, невозможна ситуация, в которой процесс вечно ждет попадания в критическую область в совокупности определяют… | условия исключения состязаний | Верный ответ – 1 балл, неверный – 0. |
| **18. Взаимоисключение, синхронизация, взаимоблокировка, голодание относятся к ….** | задачам управления процессами | Верный ответ – 1 балл, неверный – 0. |
| **19. Монитор, который связан с объектом Object o и контролирует монопольный доступ к части метода, в программном коде может быть представлен …** | synchronized(o){  // защищенная часть  // программы  } | Верный ответ – 1 балл, неверный – 0. |
| **20. Часть программы, которая одновременно может быть выполнена только одним потоком или процессом, называется …** | критическая секция | Верный ответ – 1 балл, неверный – 0. |
| **Дисциплина «Методы проектирования программного обеспечения» (Б1.В.ДВ.1.2)** | | | |
| ИПК-2.1. Разрабатывает защищенные открытые информационные системы  **Знать:**  средства автоматизации разработки программного обеспечения открытых информационных систем (ИПК-2.1)  **Уметь:**  вести разработку программного обеспечения в интегрированных среде разработки Intellij Idea (ИПК-2.1)  применять шаблоны объектно-ориентированного проектирования для обеспечения слабой связности модулей программного обеспечения. (ИПК-2.1)  **Владеть:**  современными инструментами сборки программных проектов. (ИПК-2.1)  базовыми методами отладки и тестирования объектно-ориентированных программных систем. (ИПК-2.1) | **1. Какой способ создания и запуска потоков корректен?**  1. Создать объект класса Runnable. 2. Вызвать у созданного объекта метод run() (после этого начнет выполняться метод start(), реализованный у переданного объекта)  2. Создать объект класса ClassName extends Thread. 2. Вызвать у созданного объекта метод start() (после этого начнет выполняться метод run(), реализованный у переданного объекта)  3. Создать объект класса ClassName implements Thread. 2. Вызвать у созданного объекта метод start() (после этого начнет выполняться метод run(), реализованный у переданного объекта)  4. Создать объект класса ClassName implements Runnable. 2. Вызвать у созданного объекта метод run() (после этого начнет выполняться метод start(), реализованный у переданного объекта) | 2 | Верный ответ – 1 балл, неверный – 0. |
| **2. Чем отличаются методы interrupt, interrupted, isInterrupted?**  1. interrupt() — устанавливает флаг прерывания потока  isInterrupted() — возвращает состояние флага прерывания и оставляет этот флаг нетронутым.  interrupted() — возвращает состояние флага и сбрасывает его.  2. interrupt() — возвращает состояние флага и сбрасывает его.  isInterrupted() — возвращает состояние флага прерывания и оставляет этот флаг нетронутым.  interrupted() — устанавливает флаг прерывания потока  3. interrupt() — возвращает состояние флага прерывания и оставляет этот флаг нетронутым.  isInterrupted() — возвращает состояние флага и сбрасывает его.  interrupted() — устанавливает флаг прерывания потока  4. interrupt() — устанавливает флаг прерывания потока  isInterrupted() — возвращает состояние флага и сбрасывает его.  interrupted() — возвращает состояние флага прерывания и оставляет этот флаг нетронутым. | 1 | Верный ответ – 1 балл, неверный – 0. |
| **3. Для потока справедливо следующее утверждение:**  1. Сбой одного потока всегда влияет на другой поток  2. Поток – это информация о текущем состоянии выполнения, включая регистры процессора и системные данные  3. Поток – это «легковесный» подкомпонент процесса, который выполняется в контексте процесса и разделяет с ним память и ресурсы. | 3 | Верный ответ – 1 балл, неверный – 0. |
| **4. Семафор обеспечивает пропуск в критическую секцию:**  1. строго один поток,  2. 2 потока,  3. 3 потока,  4. Любое количество потоков в условиях ограничений на вычислительные ресурсы | 4 | Верный ответ – 1 балл, неверный – 0. |
| **5. Какой задачи межпроцессного взаимодействия не существует:**  1. «Инкапсуляция поведения»  2. «Читатели Писатели»  3. «Спящий брадобрей»  4. «Обедающие философы» | 1 | Верный ответ – 1 балл, неверный – 0. |
| **6. Установите соответствие между названием понятиями ресурса и определениями**  А. Разделяемый  Б. Потокобезопасный  В. Потоконебезопасный  1. Это объект или структура данных, которая может использоваться несколькими потоками одновременно без риска повреждения данных, состояния гонки (race conditions) или взаимоблокировок (deadlocks).  2. Ресурс, доступ к которому может быть предоставлен нескольким процессам или потокам одновременно, но который требует координации для предотвращения конфликтов, некорректной работы или повреждения данных.  3.Это объект или структура данных, которая не обеспечивает корректной работы при доступе из нескольких потоков одновременно. | А-2  Б-1  В-3 | Верный ответ – 1 балл, неверный – 0. |
| **7. Установите соответствие между командами:**  А. down(mutex)  Б. up(mutex)  В. down(semaphor)  Г. up(semaphor)  1. l.unlock()  2. s.acquire()  3. s.release()  4. l.lock() | А-4  Б-1  В-2  Г-3 | Верный ответ – 1 балл, неверный – 0. |
| **8. Установите соответствие между концепциями Java Concurrency и их описаниями.**  А. ThreadPool  Б. ReentrantLock  В. volatile  1. Гибкая альтернатива synchronized, которая позволяет более точно контролировать блокировки.  2. Маркирует переменную как доступную для нескольких потоков, гарантируя видимость изменений.  3. Упрощает управление потоками за счёт повторного использования уже созданных потоков. | А-3  Б-1  В-2 | Верный ответ – 1 балл, неверный – 0. |
| **9. Установите соответствие между названием метода и его определением:**  А. wait()  Б. notify()  В. notifyAll()  1. Пробуждает все потоки, находящиеся в состоянии ожидания на данном объекте.  2. Поток, вызвавший этот метод, переходит в состояние ожидания, освобождая монитор объекта.  3. Пробуждает один из потоков, который находится в состоянии ожидания на данном объекте. | А-2  Б-3  В-1 | Верный ответ – 1 балл, неверный – 0. |
| **10. Установите соответствие между видом интерфейса и его определением:**  А. интерфейс  Б. маркер-интерфейс  В. функциональный интерфейс  1. Тип в Java, который определяет набор методов, которые класс должен реализовать и используемый для достижения абстракции и создания контрактов между компонентами системы.  2. Содержит только один абстрактный метод.  3. Не содержит методов и полей, используется для предоставления определённой метаинформации о классе. | А-1  Б-3  В-2 | Верный ответ – 1 балл, неверный – 0. |
| **11. Установите правильную последовательность работы synchronized блока**  1. Поток выполняет код внутри блока  2. Другие потоки могут получить доступ к монитору  3. Поток захватывает монитор объекта  4. Поток освобождает монитор объекта | 3, 1, 4, 2 | Верный ответ – 1 балл, неверный – 0. |
| **12. Установите правильную последовательность работы метода wait().**  1. поток освобождает монитор  2. Поток ожидает вызова notify() или notifyAll()  3. Поток переводится в состояние ожидания  4. Поток снова захватывает монитор | 1, 3, 2,4 | Верный ответ – 1 балл, неверный – 0. |
| **13. Установите правильную последовательность работы ReentrantLock()**  1. поток пытается захватить блокировку (lock())  2. Поток выполняет критическую секцию.  3. Поток освобождает блокировку (unlock()).  4. Другой поток получает доступ к блокировке. | 1,2,3,4 | Верный ответ – 1 балл, неверный – 0. |
| **14. Какова правильная последовательность работы с аннотацией @Configuration в Spring?**  1. методы с аннотацией @Bean вызываются для создания экземпляров.  2. контекст Spring сканирует класс и обнаруживает аннотацию @Configuration.  3. бины регистрируются в контейнере IoC Spring.  4. класс с аннотацией @Configuration создаётся. | 4, 2, 1, 3 | Верный ответ – 1 балл, неверный – 0. |
| **15. Установите правильную последовательность действий с которой @ComponentScan обнаруживает компоненты?**  1. Сканирует указанные пакеты на наличие классов с аннотацией @Component  2. Проверяет производные аннотации: @Service, @Repository, @Controller  3. Создаёт бины для обнаруженных классов | 1, 2, 3 | Верный ответ – 1 балл, неверный – 0. |
| **16.** Режим, при котором поток постоянно опрашивает условия в ожидании попадания в критическую секцию называется … | активное ожидание | Верный ответ – 1 балл, неверный – 0. |
| **17.** Два процесса не должны одновременно находиться в критических областях, в программе не должно быть предположений о скорости или количестве процессоров, процесс, находящийся вне критической области, не может блокировать другие процессы, невозможна ситуация, в которой процесс вечно ждет попадания в критическую область в совокупности определяют… | условия исключения состязаний | Верный ответ – 1 балл, неверный – 0. |
| **18.** Взаимоисключение, синхронизация, взаимоблокировка, голодание относятся к …. | задачам управления процессами | Верный ответ – 1 балл, неверный – 0. |
| **19.** Монитор, который связан с объектом Object o и контролирует монопольный доступ к части метода, в программном коде может быть представлен … | synchronized(o){  // защищенная часть  // программы  } | Верный ответ – 1 балл, неверный – 0. |
| **20.** Часть программы, которая одновременно может быть выполнена только одним потоком или процессом, называется … | критическая секция | Верный ответ – 1 балл, неверный – 0. |
| **«Проектно-технологическая практика» (Б2.П.1)** | | | |
| **ИПК-2.2**. Выполняет анализ защищенности информационных систем  **Знать**:  − основные понятия и общее содержание проблемы информационной безопасности (ИПК-2.2)  − угрозы и уязвимости информации (ИПК-2.2)  **Уметь**:  − оценивать методы и средства информационной безопасности, их значение для обеспечения защиты личности, общества и государства (ИПК-2.2)  − оценивать угрозы и уязвимости информации (ИПК2.2)  **Владеть**:  − навыками обработки, интерпретации и обобщения информации (ИПК-2.2)  − методами идентификации и аутентификации пользователей (ИПК-2.2)  − основными методами защиты информации (ИПК-2.2) | **1. Что такое тестирование программного обеспечения? (укажите цифру правильного ответа):**  1. Процесс проверки и оценки качества программного продукта путем выявления ошибок и дефектов  2. Процесс написания исходного кода  3. Процесс разработки новых функций программы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **2. Какую цель преследует тестирование программного обеспечения? (укажите через запятую неправильные ответы):**  1. Обнаружение ошибок и дефектов, обеспечение качества и надежности программы  2. Улучшение внешнего вида программы  3. Повышение производительности компьютера | 2,3 | Верный ответ – 1 балл, неверный – 0. |
| **3. Какова основная цель юнит-тестирования?**  1. Проверка отдельных компонентов программы на их корректную работу  2. Тестирование интерфейса пользователя  3. Тестирование безопасности системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **4. Что такое интеграционное тестирование?**  1. Процесс проверки взаимодействия между модулями или компонентами системы  2. Тестирование производительности  3. Тестирование всех компонентов в реальной рабочей среде | 1 | Верный ответ – 1 балл, неверный – 0. |
| **5. Что такое системное тестирование?**  1. Проверка всей системы как целого, чтобы убедиться в ее соответствии функциональным требованиям  2. Тестирование кода на уровне отдельных функций  3. Тестирование пользовательского интерфейса | 1 | Верный ответ – 1 балл, неверный – 0. |
| **6. Какую роль играет тестирование на этапе разработки программного обеспечения?**  1. Оно помогает найти и исправить ошибки на ранних стадиях разработки, предотвращая их распространение в готовом продукте  2. Оно ускоряет процесс создания кода  3. Оно помогает улучшить графику приложения | 1 | Верный ответ – 1 балл, неверный – 0. |
| **7. Что такое функциональное тестирование?**  1. Тестирование, которое фокусируется на проверке, соответствует ли программное обеспечение заявленным функциональным требованиям  2. Тестирование пользовательского интерфейса  3. Тестирование производительности и масштабируемости | 1 | Верный ответ – 1 балл, неверный – 0. |
| **8. Какую задачу решает тестирование производительности программного обеспечения?**  1. Проверка, как программа ведет себя под высокой нагрузкой и насколько она эффективно использует ресурсы  2. Проверка интерфейса пользователя  3. Тестирование локализации программы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **9. Что такое тестирование безопасности?**  1. Процесс проверки уязвимостей программы, чтобы убедиться, что она защищена от атак и утечек данных  2. Проверка производительности программы  3. Тестирование локализации программного обеспечения | 1 | Верный ответ – 1 балл, неверный – 0. |
| **10. Что такое альфа-тестирование?**  1. Тестирование, проводимое разработчиками на ранней стадии разработки перед передачей в тестовую команду  2. Тестирование программы на реальных пользователях  3. Тестирование на внешних условиях | 1 | Верный ответ – 1 балл, неверный – 0. |
| **11. Что такое бета-тестирование?**  1. Тестирование, проводимое внешними пользователями, с целью получения обратной связи и выявления ошибок в реальных условиях  2. Тестирование в процессе разработки  3. Проводится только внутри компании-разработчика | 1 | Верный ответ – 1 балл, неверный – 0. |
| **12. Какую роль играет автоматизированное тестирование в процессе разработки?**  1. Автоматизированное тестирование ускоряет проверку повторяющихся сценариев и помогает обеспечить стабильность продукта  2. Оно заменяет необходимость в ручном тестировании  3. Оно используется только для функциональных тестов | 1 | Верный ответ – 1 балл, неверный – 0. |
| **13. Что такое тестирование пользовательского интерфейса (UI)?**  1. Проверка удобства и функциональности интерфейса, а также корректности отображения элементов на экране  2. Проверка работы базы данных  3. Тестирование производительности системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **14. Что такое регрессионное тестирование?**  1. Тестирование, которое проверяет, не нарушены ли ранее работавшие функции программы после внесения изменений  2. Проверка новых функций  3. Тестирование безопасности системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **15. Что такое тестирование совместимости?**  1. Проверка, как программа работает на различных операционных системах, устройствах или в разных браузерах  2. Тестирование только производительности  3. Проверка производительности на одном устройстве | 1 | Верный ответ – 1 балл, неверный – 0. |
| **16. Какие инструменты обычно используются для автоматизированного тестирования?**  1. Selenium, JUnit, TestNG, Appium  2. Visual Studio  3. Программы для мониторинга безопасности | 1 | Верный ответ – 1 балл, неверный – 0. |
| **17. Какой из следующих типов тестирования фокусируется на пользовательском опыте?**  1. Юзабилити-тестирование  2. Тестирование безопасности  3. Тестирование функциональности | 1 | Верный ответ – 1 балл, неверный – 0. |
| **18. Что такое "черный ящик" в контексте тестирования?**  1. Метод тестирования, при котором тестировщик не знает внутренней реализации системы и проверяет ее только с точки зрения функциональности  2. Тестирование, при котором проверяется только внутренняя структура кода  3. Метод тестирования с подробным анализом исходного кода | 1 | Верный ответ – 1 балл, неверный – 0. |
| **19. Что такое "белый ящик" в контексте тестирования?**  1. Метод тестирования, при котором тестировщик имеет доступ к исходному коду и проверяет его на наличие ошибок  2. Тестирование только пользовательского интерфейса  3. Тестирование на реальных устройствах | 1 | Верный ответ – 1 балл, неверный – 0. |
| **20. Что такое тестирование на отказоустойчивость?**  1. Проверка, как программа продолжает работать в случае отказа отдельных компонентов или проблем с системой  2. Тестирование только производительности  3. Проверка на безопасность приложения | 1 | Верный ответ – 1 балл, неверный – 0. |
| **«Практика по получению опыта контрольно-аналитической деятельности» (Б2.П.2)** | | | |
| **ИПК-2.2.**  Выполняет анализ защищенности информационных систем  **Знать**:  − основные понятия и проблемы информационной безопасности (ИПК-2.2)  − угрозы и уязвимости информации (ИПК-2.2)  **Уметь:**  − оценивать методы и средства информационной безопасности (ИПК-2.2)  − оценивать угрозы и уязвимости информации (ИПК2.2)  **Владеть:**  − навыками обработки, интерпретации и обобщения информации (ИПК-2.2)  − методами идентификации и аутентификации пользователей (ИПК-2.2)  − основными методами защиты информации (ИПК-2.2) | **1. Что такое системы предотвращения вторжений (IPS)?**  1. Системы, которые анализируют трафик сети и блокируют подозрительные действия, предотвращая вторжения  2. Системы для ускорения работы сети  3. Программы для создания резервных копий | 1 | Верный ответ – 1 балл, неверный – 0. |
| **2. Какую роль играет защита от атак типа "отказ в обслуживании" (DoS)?**  1. Механизмы, предотвращающие перегрузку системы чрезмерным количеством запросов  2. Защита от вирусов  3. Защита от потери данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **3. Какую роль в защите информации играют фаерволы?**  1. Они фильтруют и контролируют входящий и исходящий трафик, предотвращая несанкционированный доступ к сети  2. Защита от физических повреждений  3. Ускорение работы системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **4. Что такое использование виртуальных частных сетей (VPN) для защиты информации?**  1. VPN шифрует трафик и защищает его от перехвата при передаче через небезопасные сети, такие как интернет  2. Применение фаервола  3. Создание резервных копий данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **5. Какую роль играет контроль версий в защите информации?**  1. Контроль версий позволяет отслеживать изменения в данных и программном обеспечении, предотвращая несанкционированные модификации  2. Контроль за выполнением программ  3. Повышение производительности системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **6. Какова цель разграничения доступа в защищенной информационной системе?**  1. Предотвратить несанкционированный доступ к данным и ресурсам, а также ограничить права пользователей в соответствии с их ролями  2. Обеспечить доступ ко всем данным для всех пользователей  3. Ускорить работу системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **7. Что такое аудит безопасности в контексте защищенного администрирования?**  1. Процесс мониторинга и анализа действий пользователей и системных процессов для выявления нарушений политики безопасности  2. Процесс оптимизации работы системы  3. Процесс устранения неполадок в системе | 1 | Верный ответ – 1 балл, неверный – 0. |
| **8. Какова роль резервного копирования в защите информации?**  1. Создание резервных копий данных для восстановления в случае утраты или повреждения информации  2. Оптимизация использования памяти  3. Ускорение работы системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **9. Что такое шифрование данных в контексте защищенного администрирования?**  1. Процесс преобразования данных в нечитаемую форму с целью защиты от несанкционированного доступа  2. Процесс ускорения обработки данных  3. Процесс архивации данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **10. Какую роль играют средства защиты от вирусов и вредоносного ПО в системе безопасности?**  1. Предотвращают заражение системы вирусами и другим вредоносным ПО, которое может нарушить работу системы  2. Защищают систему от переполнения памяти  3. Предотвращают сбои системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **11. Что такое многофакторная аутентификация?**  1. Процесс, при котором для доступа к системе требуется несколько способов подтверждения личности пользователя  2. Процесс подтверждения личности с помощью одного пароля  3. Процесс повышения скорости работы системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **12. Как работает фаервол в контексте защищенного администрирования?**  1. Он контролирует и фильтрует входящий и исходящий трафик между сетью и системой  2. Он ускоряет работу системы  3. Он предотвращает доступ пользователей к сети | 1 | Верный ответ – 1 балл, неверный – 0. |
| **13. Каковы основные принципы настройки прав доступа в информационных системах?**  1. Принцип минимальных прав, принцип разделения обязанностей, принцип наименьшего воздействия  2. Принцип максимальной доступности  3. Принцип полной открытости доступа | 1 | Верный ответ – 1 балл, неверный – 0. |
| **14. Что такое защита от DDoS-атак в администрировании информационных систем?**  1. Механизмы, направленные на предотвращение перегрузки системы с помощью массовых запросов  2. Защита от несанкционированного доступа  3. Защита от физических повреждений системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **15. Какую роль играют журналы безопасности в информационных системах?**  1. Они помогают отслеживать действия пользователей и системных процессов для анализа и выявления угроз безопасности  2. Они ускоряют работу системы  3. Они сохраняют резервные копии данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **16. Что такое виртуализация в контексте безопасности информационных систем?**  1. Процесс создания виртуальных машин, которые изолируют приложения и системы, обеспечивая дополнительный уровень безопасности  2. Процесс использования нескольких операционных систем на одном устройстве  3. Процесс увеличения мощности системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **17. Какие меры защиты используются для предотвращения утечек информации через каналы связи?**  1. Шифрование данных, мониторинг трафика, контроль доступа к сети  2. Применение антивирусных программ  3. Ограничение скорости передачи данных | 1 | Верный ответ – 1 балл, неверный – 0. |
| **18. Какую роль играет двухфакторная аутентификация?**  1. Она требует подтверждения личности пользователя через два различных канала, таких как пароль и код, отправленный на мобильное устройство  2. Она используется только для ускорения работы системы  3. Она ограничивает права пользователей в системе | 1 | Верный ответ – 1 балл, неверный – 0. |
| **19. Что такое защита от утечек данных (DLP-системы)?**  1. Технологии, направленные на мониторинг и блокировку утечек конфиденциальной информации из системы  2. Программы для ускорения работы системы  3. Программы для защиты от вирусов | 1 | Верный ответ – 1 балл, неверный – 0. |
| **20. Какую функцию выполняют средства защиты от вирусов и шпионских программ?**  1. Они обнаруживают и блокируют вирусы и другие угрозы для системы безопасности  2. Они ускоряют выполнение программ  3. Они восстанавливают поврежденные файлы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **«Эксплуатационная практика» (Б2.П.3)** | | | |
| **ИПК-2.1.** Разрабатывает защищенные открытые информационные системы  **Знать**:  − основные характеристики, показатели и модели надежности систем (ИПК-2.1)  − стратегии профилактического обслуживания (ИПК2.1)  − модели, методы, шаблоны проектирования каркасов программного обеспечения (ИПК-2.1)  **Уметь**:  − разрабатывать, проводить отладку и тестирование программных модулей (ИПК-1.2) **Владеть**:  − методами повышения качества функционирования автоматизированной системы, методами контроля и диагностики аппаратных и программных средств (ИПК-2.1) | **1. Как защищается транспортный уровень в сети?**  1. Использованием протоколов SSL/TLS для шифрования данных  2. Защита на транспортном уровне не требуется  3. Протоколы TCP/IP не защищены | 1 | Верный ответ – 1 балл, неверный – 0. |
| **2. Какую роль играют криптографические протоколы в защите сети?**  1. Они обеспечивают конфиденциальность и целостность данных, передаваемых по сети  2. Криптографические протоколы ускоряют передачу данных  3. Криптографические протоколы не нужны для защиты | 1 | Верный ответ – 1 балл, неверный – 0. |
| **3. Как защищаются почтовые серверы от угроз?**  1. Использованием антивирусных фильтров, аутентификации и шифрования почтовых сообщений  2. Почтовые серверы не требуют защиты  3. Использованием одного пароля для всех серверов | 1 | Верный ответ – 1 балл, неверный – 0. |
| **4. Как работают механизмы защиты от перехвата трафика в защищенных сетях?**  1. Использование шифрования данных и цифровых сертификатов для обеспечения безопасности передачи информации  2. Трафик не требует защиты  3. Защита от перехвата не применяется в современных сетях | 1 | Верный ответ – 1 балл, неверный – 0. |
| **5. Какие преимущества дает использование многофакторной аутентификации в сети?**  1. Многофакторная аутентификация повышает безопасность, требуя подтверждения личности через несколько каналов  2. Она увеличивает скорость сети  3. Многофакторная аутентификация не используется в сетях | 1 | Верный ответ – 1 балл, неверный – 0. |
| **6. Что такое методология Agile?**  1. Методология разработки, основанная на гибкости, частых изменениях и взаимодействии с заказчиком  2. Методология для написания документации  3. Статическая модель разработки | 1 | Верный ответ – 1 балл, неверный – 0. |
| **7. Какое место занимает тестирование в программной инженерии?**  1. Тестирование является важной частью разработки, направленной на обнаружение ошибок и обеспечение качества ПО  2. Тестирование проводится только на этапе завершения разработки  3. Тестирование важнее всех этапов разработки | 1 | Верный ответ – 1 балл, неверный – 0. |
| **8. Что такое системный анализ в контексте программной инженерии?**  1. Изучение и анализ требований заказчика для разработки эффективного программного решения  2. Процесс создания интерфейсов и графиков  3. Метод разработки новой операционной системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **9. Какова цель проектирования в программной инженерии?**  1. Создание архитектуры программного продукта, которая будет эффективной, надежной и удобной для пользователей  2. Написание исходного кода  3. Формирование требований к системе | 1 | Верный ответ – 1 балл, неверный – 0. |
| **10. Что такое моделирование в программной инженерии?**  1. Представление системы в виде абстракции для анализа, проектирования и проверки решений  2. Процесс оптимизации кода  3. Создание интерфейсов и макетов | 1 | Верный ответ – 1 балл, неверный – 0. |
| **11. Какие из следующих факторов влияют на надежность системы?**  1. Качество компонентов, дизайн системы, эксплуатационные условия  2. Только количество компонентов в системе  3. Только стоимость системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **12. Что такое фаллический граф в теории надежности?**  1. Граф, который используется для анализа структуры и взаимозависимости компонентов системы  2. Граф для представления отказов компонентов  3. Граф, описывающий производительность системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **13. Как используются методы надежности в атомных реакторах?**  1. Методы надежности применяются для предотвращения катастрофических сбоев и обеспечения бесперебойной работы системы  2. Они не применяются в таких системах  3. Методы надежности только для оценки производительности | 1 | Верный ответ – 1 балл, неверный – 0. |
| **14. Какие из следующих стратегий могут быть использованы для улучшения надежности системы?**  1. Использование резервирования, улучшение качества компонентов, применение методов предсказания отказов  2. Применение только новых компонентов  3. Снижение цены на компоненты | 1 | Верный ответ – 1 балл, неверный – 0. |
| **15. Что такое анализ жизненного цикла системы?**  1. Процесс оценки надежности системы на всех этапах ее жизни — от проектирования до вывода из эксплуатации  2. Процесс повышения производительности системы  3. Оценка стоимости системы на этапе производства | 1 | Верный ответ – 1 балл, неверный – 0. |
| **16. 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. |
| **17. 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. |
| **18. 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. |
| **19. 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. |
| **20. 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. |
| **«Преддипломная практика» (Б2.П.4)** | | | |
| **ИПК-2.1.** Разрабатывает защищенные открытые информационные системы  **ИПК-2.2**.  Выполняет анализ защищенности информационных систем  **Знать**:  − платформы реализации технологий больших данных (ИПК-2.1);  − системы разграничения доступа (ИПК-2.2) **Уметь**:  − разрабатывать приложения для платформ больших данных (ИПК-2.1);  − реализовывать на практике программы с применением технологий больших данных (ИПК-2.1);  − проводить анализ защищенности автоматизированных систем (ИПК-2.2) **Владеть**:  − основными алгоритмами, применяемыми в технологиях больших данных (ИПК-2.1);  − средствами администрирования и управления ОС Linux (ИПК-2.2)  − инструментами анализа качества работы ОС (ИПК-2.2)  **Знать**:  − технологии обеспечения безопасности в локальных сетях (ИПК-2.1, 2.2) − угрозы сетевой безопасности  (ИПК-2.1, 2.2)  **Уметь**:  − выполнять процедуры анализа сетевой безопасности (ИПК-2.2)  − осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты  (ИПК2.1, 2.2)  **Владеть**:  − методами обеспечения безопасности телекоммуникационных связей и административный контроль  (ИПК-2.1, 2.2) | **1. Как защитить беспроводные сети от угроз?**  1. Использование шифрования, скрытие SSID, установка сильных паролей и мониторинг трафика  2. Увеличение мощности сигнала  3. Отключение всех беспроводных устройств | 1 | Верный ответ – 1 балл, неверный – 0. |
| **2. Какой стандарт защиты используется в Wi-Fi для обеспечения безопасности соединений?**  1. WPA2 (Wi-Fi Protected Access 2)  2. WEP  3. Bluetooth | 1 | Верный ответ – 1 балл, неверный – 0. |
| **3. Какие методы защиты могут быть использованы в корпоративных сетях?**  1. Сегментация сети, использование VPN, шифрование данных, аутентификация и контроль доступа  2. Только увеличение скорости сети  3. Применение одного пароля для всех пользователей | 1 | Верный ответ – 1 балл, неверный – 0. |
| **4. Как обеспечить защиту веб-приложений в сети?**  1. Использование защиты от SQL-инъекций, шифрования, межсетевых экранов и других технологий  2. Использование одного пароля для всех приложений  3. Отказ от использования шифрования | 1 | Верный ответ – 1 балл, неверный – 0. |
| **5. Какие проблемы могут возникать при недостаточной защите сети?**  1. Неавторизованный доступ, утечка конфиденциальной информации, потеря данных и атаки  2. Увеличение скорости передачи данных  3. Ошибки в маршрутизации | 1 | Верный ответ – 1 балл, неверный – 0. |
| **6. Что такое облачный анализ в контексте защиты от вредоносного ПО?**  1. Анализ угроз и вредоносных программ с использованием облачных вычислительных ресурсов для быстрого сканирования  2. Анализ только локальных файлов  3. Анализ производительности системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **7. Какую роль в анализе вредоносного ПО играет мониторинг системных вызовов?**  1. Системные вызовы позволяют отслеживать взаимодействие программы с операционной системой и выявлять подозрительные действия  2. Мониторинг системных вызовов не имеет значения для анализа  3. Мониторинг используется для проверки производительности программы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **8. Что такое виртуализация в анализе вредоносного ПО?**  1. Использование виртуальных машин для безопасного выполнения подозрительных программ и анализа их поведения  2. Использование виртуальных машин для увеличения производительности программы  3. Виртуализация компонентов операционной системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **9. Что такое сбор данных о поведении вредоносного ПО в сети?**  1. Анализ данных, полученных о сетевых действиях вредоносного ПО, чтобы понять, как оно распространяется и взаимодействует с другими системами  2. Сбор данных о производительности системы  3. Сбор данных о размере вредоносного ПО | 1 | Верный ответ – 1 балл, неверный – 0. |
| **10. Как анализируется влияние вредоносного ПО на систему?**  1. Путем наблюдения за изменениями в файлах, системных процессах, сетевых соединениях и системных настройках  2. Только путем восстановления удаленных данных  3. Путем анализа времени отклика системы | 1 | Верный ответ – 1 балл, неверный – 0. |
| **11. Какие атаки могут быть направлены на компьютерные сети?**  1. Отказ в обслуживании (DoS), подмена адреса (spoofing), перехват трафика (sniffing)  2. Проблемы с подключением устройств к сети  3. Ошибки в маршрутизации | 1 | Верный ответ – 1 балл, неверный – 0. |
| **12. Что такое атака "отказ в обслуживании" (DoS)?**  1. Атака, направленная на перегрузку системы или сети, делая её недоступной для пользователей  2. Атака на физическую инфраструктуру сети  3. Ошибка в алгоритмах маршрутизации | 1 | Верный ответ – 1 балл, неверный – 0. |
| **13. Какие механизмы защиты могут использоваться для предотвращения DDoS-атак?**  1. Использование систем распределенной защиты, фильтрации трафика, балансировки нагрузки  2. Увеличение скорости интернет-соединения  3. Шифрование трафика | 1 | Верный ответ – 1 балл, неверный – 0. |
| **14. Как работают технологии IDS/IPS (системы обнаружения и предотвращения вторжений)?**  1. Они анализируют трафик сети на наличие подозрительных действий и могут блокировать их  2. Используют механизмы шифрования  3. Улучшают скорость работы сети | 1 | Верный ответ – 1 балл, неверный – 0. |
| **15. Какой основной принцип лежит в основе концепции "сегментации сети"?**  1. Разделение сети на изолированные части для минимизации ущерба при атаке  2. Использование одного маршрутизатора для всех устройств  3. Снижение скорости сети для уменьшения угроз | 1 | Верный ответ – 1 балл, неверный – 0. |
| **16. Какую роль играют DNS-серверы в безопасности сети?**  1. DNS-серверы могут быть целью атак, таких как DNS-спуфинг, и должны быть защищены от манипуляций с записями  2. Ускоряют передачу данных  3. Улучшают маршрутизацию трафика | 1 | Верный ответ – 1 балл, неверный – 0. |
| **17. Что такое "DNS-спуфинг"?**  1. Атака, при которой злоумышленник подменяет записи DNS-сервера, направляя трафик на фальшивые сайты  2. Способ ускорения работы DNS-сервера  3. Метод защиты DNS-серверов от атак | 1 | Верный ответ – 1 балл, неверный – 0. |
| **18. Как работают технологии "антивирусной фильтрации" в сети?**  1. Они анализируют входящий и исходящий трафик на наличие вредоносных программ и блокируют их  2. Фильтруют только текстовую информацию  3. Обеспечивают передачу данных без потерь | 1 | Верный ответ – 1 балл, неверный – 0. |
| **19. Какую роль играют прокси-серверы в защите сети?**  1. Прокси-серверы скрывают реальный IP-адрес пользователей, фильтруют трафик и защищают от внешних атак  2. Прокси-серверы увеличивают скорость сети  3. Прокси-серверы обеспечивают защищенное соединение с интернетом | 1 | Верный ответ – 1 балл, неверный – 0. |
| **20. Как предотвращается утечка информации через сеть?**  1. Использование шифрования данных, мониторинг и контроль доступа к сетевым ресурсам  2. Ограничение пропускной способности сети  3. Установка антивирусных программ на устройства | 1 | Верный ответ – 1 балл, неверный – 0. |