**Вопросы**

1)Жизненный цикл ИС.

**Ответ:**

Жизненный цикл информационной системы – период времени, который

начинается с момента принятия решения о необходимости создания

информационной системы и заканчивается в момент ее полного изъятия из

эксплуатации.

2)Основные методологии разработки ИС: MSF, RUP и т.п ГОСТ Р ИСО/МЭК 12207.

**Ответ:**

Основные методологии разработки информационных систем (ИС), представляют собой наборы советов, принципов и процедур, которые помогают в разработке ИС.

MSF предоставляет набор инструментов и советов, включающих в себя планирование, управление рисками, коммуникации в команде и другие аспекты.

RUP, обеспечивает методику разработки и управления жизненным циклом ПО, охватывая анализ, дизайн, разработку, тестирование и внедрение.

ГОСТ Р ИСО/МЭК 12207 предоставляет международный стандарт для процессов жизненного цикла ПО, включая разработку, техническую документацию, тестирование и управление изменениями.

3)Техническое задание: основные разделы согласно стандартам.

**Ответ:**

Введение, Основные требования, Состав и структура ИС, Требование к интерфейсам, Требование к защите информации, Требование к тестированию и качеству, Порядок контроля и приемки.

4)Основные процессы и взаимосвязь между документами в ИС согласно стандартам.

**Ответ:**

Процессы жизненного цикла, Процессы поддержки, Процессы поставки, Процессы управления.

Взаимосвязь между документами и процессами в ИС очень тесная. Например, в процессе разработки ИС создаются и используются такие документы как техническое задание, технический проект, план тестирования, отчеты о тестировании и т.д.

5)Виды внедрения, план внедрения.

**Ответ:**

Виды: Фазовое внедрение, Прямое внедрение, Внедрение по модулям, Параллельное внедрение, Фазированное внедрение.

План внедрения: Предварительный анализ, Планирование, Подготовка ИС к внедрению, Обучение пользователей, Запуск к внедрению, Поддержка и сопровождение.

6)Структура и этапы проектирования ИС.

**Ответ:**

Структуры: Предварительная разработка, Архитектурное проектирование, Техническое проектирование, Тестовое проектирование, Инфраструктурное проектирование.

Этапы проектирования: Предпроектный, Проектирование, Разработка, Тестирование, Отладка, Внедрение на объект.

7)Стандарты ЕСПД.

**Ответ:**

Стандарты ЕСПД подразделяются на следующие группы: Общие положения(код 0), Основополагающие стандарты(код 1), Правила выполнения документации разработки(код 2), Правила выполнения документации изготовления(код 3), Правила выполнения документации сопровождения(код 4), Правила выполнения эксплуатационной документации(код 5), Правила выполнения программной документации(код 6), Резервные группы(код 7,8), Прочие стандарты(код 9).

8)Методы разработки обучающей документации.

**Ответ:**

1)ADDIE – метод циклического процесса, который включает в себя анализ, проектирование, разработку, внедрение и оценку.

2)Agile – процесс разработки разбивается на короткие участки, в течение которых создается и уточняется документация.

3)SAM – модель последовательного приближения предлагает итеративный процесс разработки, который включает в себя постоянное совершенствование и доработку материала.

4)Content Chunking – подход предлагает разделение информации на небольшие части информации или чанки, что упрощает усвоения материала пользователем.

9)Порядок внесения и регистрации изменений в документации.

**Ответ:**

Идентификация необходимых изменений, Оценка влияния изменений, Разработка изменений, Проверка, Внесение изменений, Регистрация изменений, Уведомление заинтересованных лиц, Обеспечение доступности.

10)Формирование репозитория проекта внедрения.

**Ответ:**

Формирование делится на несколько этапов: 1)Выбор системы управления версиями, 2)Создание репозитория, 3)Организация структуры репозитория, 4)Инициализация и первоначальная загрузка файлов, 5)Управление доступом, 6)Создание документации, 7)Непрерывная поддержка.

11)Сравнительный анализ инструментов организационного проектирования.

**Ответ:**

Сравнительный анализ инструментов организационного проектирования может быть проведен на примере инструментов Visio и ARIS -предоставляют возможности для создания организационных структур, процессов и моделей.

1. Функциональность:

Visio предоставляет широкий набор инструментов для создания различных типов диаграмм, включая организационные структуры, процессы, потоки данных и др. Однако, функциональность Visio в области управления организационными процессами не так развита.

ARIS специализируется на управлении бизнес-процессами и предоставляет более продвинутые инструменты для моделирования организационных процессов, анализа и оптимизации.

2. Гибкость:

Visio является более универсальным инструментом и может быть использован для различных целей, включая организационное проектирование.

ARIS более специализирован на управлении бизнес-процессами и может быть более гибким в этом контексте.

3. Интеграция:

Visio может интегрироваться с другими приложениями Microsoft Office, что облегчает обмен данными и информацией между системами.

ARIS: ARIS обычно интегрируется с другими системами управления, такими как ERP или CRM, что позволяет создать единую информационную среду для управления организацией.

4. Удобство использования:

Visio обладает простым и интуитивно понятным интерфейсом, что делает его доступным для широкого круга пользователей.

ARIS имеет более сложный интерфейс, требующий некоторого времени для изучения, но при этом предоставляет более продвинутые функциональные возможности.

12)Типовые функции инструментария для автоматизации процесса внедрения ИС.

**Ответ:**

Типовые функции:

1. Управление проектом: инструменты для планирования, контроля и отслеживания хода проекта по внедрению информационной системы. Включает в себя функционал для создания графиков, задач, ресурсов, бюджета и т.д.

2. Моделирование бизнес-процессов: возможность создания моделей текущих и будущих бизнес-процессов, анализа и оптимизации их работы.

3. Управление требованиями: инструменты для сбора, анализа, документирования и управления требованиями к информационной системе со стороны заказчика.

4. Тестирование и контроль качества: функционал для планирования, проведения и отслеживания тестирования информационной системы, а также контроля качества разработки.

5. Конфигурационное управление: возможности для контроля версий программного обеспечения, управления изменениями и конфигурациями системы.

6. Обучение и документация: инструменты для создания обучающих материалов, документации по информационной системе и организации обучения пользователей.

7. Интеграция и обмен данными: возможности для интеграции новой информационной системы с другими системами организации, а также обмена данными между ними.

8. Отчетность и аналитика: функционал для создания отчетов о ходе проекта, результатов тестирования, аналитики использования системы и других важных показателей.

9. Безопасность и доступ: инструменты для управления доступом к информационной системе, защиты данных, мониторинга безопасности и предотвращения угроз.

10. Мониторинг и поддержка: функционал для мониторинга работы информационной системы, выявления проблем, поддержки пользователей и решения возникающих проблем.

13)Установка, конфигурирование и настройка сетевых и телекоммуникационных средств.

**Ответ:**

Установка, конфигурирование и настройка сетевых и телекоммуникационных средств является важным этапом в развертывании информационной инфраструктуры организации. Ниже приведены основные этапы и рекомендации по выполнению этих задач:

1. Планирование: определите требования к сети и телекоммуникационным средствам, проведите аудит существующей инфраструктуры, разработайте план установки и конфигурации.

2. Выбор оборудования: выберите необходимое сетевое и телекоммуникационное оборудование в соответствии с требованиями проекта (маршрутизаторы, коммутаторы, модемы, телефонные станции и т.д.).

3. Физическая установка: установите оборудование в соответствии с рекомендациями производителя, обеспечьте правильное подключение к сети электропитания и сетевым кабелям.

4. Конфигурирование устройств: настройте сетевое оборудование, установите IP-адреса, настройки безопасности, VLAN, маршрутизацию, фильтрацию трафика и другие параметры в соответствии с требованиями проекта.

5. Настройка сетевых служб: сконфигурируйте необходимые сетевые службы, такие как DHCP, DNS, VPN, файрволлы, прокси-серверы и другие для обеспечения безопасной и эффективной работы сети.

6. Тестирование и отладка: проведите тестирование сети и телекоммуникационных средств для проверки их работоспособности, стабильности, скорости передачи данных и соответствия требованиям проекта.

7. Документация и обучение: создайте документацию по установке, конфигурации и настройке сетевых и телекоммуникационных средств, обучите пользователей и администраторов работе с новой инфраструктурой.

8. Мониторинг и поддержка: настройте системы мониторинга для отслеживания работы сети, обеспечьте регулярное обслуживание и поддержку оборудования для предотвращения неполадок.

14)Формирование интерфейсов и организация доступа пользователей к ИС.

**Ответ:**

Формирование интерфейсов и организация доступа пользователей к информационной системе играют ключевую роль в обеспечении удобства использования системы, безопасности данных и эффективности работы пользователей. Ниже приведены основные шаги и рекомендации по этим задачам:

1. Проектирование интерфейсов:

- Определите потребности пользователей и функциональные требования к интерфейсу.

- Разработайте удобные и интуитивно понятные интерфейсы с учетом лучших практик юзабилити.

- Обеспечьте согласованность дизайна интерфейсов для повышения удобства использования.

2. Организация доступа пользователей:

- Разработайте стратегию управления доступом, определив роли и права доступа для различных категорий пользователей.

- Используйте механизмы аутентификации (логин-пароль, двухфакторная аутентификация, биометрия) для обеспечения безопасного доступа.

- Установите механизмы авторизации для контроля доступа пользователей к различным функциям и данным системы.

3. Интеграция с другими системами:

- Обеспечьте интеграцию с другими информационными системами и сервисами для обмена данными и обеспечения единого пользовательского опыта.

- Разработайте API для возможности интеграции сторонних приложений с вашей информационной системой.

4. Обучение пользователей:

- Проведите обучение пользователей по работе с интерфейсами и доступу к информационной системе.

- Создайте руководства пользователя и видеоуроки для помощи пользователям в освоении системы.

5. Мониторинг и анализ использования:

- Внедрите системы мониторинга использования интерфейсов и доступа к системе для анализа поведения пользователей.

- Проводите регулярный анализ данных о использовании системы для оптимизации интерфейсов и доступа.

6. Обратная связь от пользователей:

- Проводите опросы пользователей и сбор обратной связи о качестве интерфейсов и доступе к системе.

- Используйте полученные данные для улучшения интерфейсов и процессов доступа к информационной системе.

15)Режим оповещения пользователей.

**Ответ:**

Режим оповещения пользователей относится к способу информирования пользователей о различных событиях, акциях, новостях и прочих важных сообщениях от организации, компании или сервиса.

Существует несколько способов режимов оповещения пользователей, включая:

1. Уведомления в приложении или на веб-сайте

2. Электронные письма и рассылки

3. СМС-уведомления

4. Пуш-уведомления на мобильных устройствах

5. Оповещения через социальные сети

Выбор режима оповещения зависит от целей организации, предпочтений пользователей и характера сообщения. Для эффективного оповещения пользователей важно выбрать подходящий способ и частоту отправки сообщений, чтобы не навязывать информацию, но при этом оставаться в фокусе внимания пользователей.

16)Организация мониторинга процессов сопровождения.

**Ответ:**

Мониторинг процесса сопровождения организации можно организовать с помощью следующих шагов:

1. Установить ключевые показатели эффективности (KPI) для оценки процесса сопровождения.

2. Разработать систему сбора и анализа данных.

3. Регулярно отслеживать и анализировать полученные данные.

4. Принимать меры по улучшению процесса сопровождения на основе полученных данных.

5. Внедрить систему обратной связи.

6. Оценивать результаты и планировать дальнейшие действия.

17)Ролевые функции и организация процесса сопровождения.

**Ответ:**

Ролевые функции и организация процесса сопровождения включают в себя следующие ключевые элементы:

1. Определение ролей и обязанностей.

2. Установление коммуникационных каналов.

3. Обучение и поддержка персонала.

4. Управление рисками.

5. Мониторинг и оценка производительности.

6. Постоянное совершенствование.

18)Анализ исходных программ и компонентов программного средства.

**Ответ:**

Анализ исходных программ и компонентов программного средства важен для понимания и определения его архитектуры, структуры, функциональности и возможностей.

19)Программная инженерия и оценка качества.

**Ответ:**

Программная инженерия и оценка качества программного обеспечения тесно связаны между собой. Программная инженерия — это область знаний и практик, направленных на разработку, тестирование, сопровождение и управление программным обеспечением.

20)Реинжиниринг.

**Ответ:**

Реинжиниринг — поэтапное обновление бизнес-процессов в компании целью которого является улучшение показателей компании (применяется, когда идет снижение рентабельности бизнеса).

21)Сохранение и откат рабочей версий системы.

**Ответ:**

Сохранение и откат рабочих версий системы можно сделать средствами Windows и иными программными средствами (Git).

Windows:

Встроенная функция позволяет создавать точки восстановления, к которым можно откатить систему в случае сбоя. Для создания точки восстановления откройте "Панель управления" -> "Система" -> "Защита системы" -> "Создать". При необходимости откатите систему к точке восстановления: "Пуск" -> "Параметры" -> "Обновление и безопасность" -> "Восстановление" -> "Вернуть компьютер в исходное состояние" -> "Выбрать другую точку восстановления".

Git:

Позволяет отслеживать изменения в файлах и коде, а также откатывать к предыдущим версиям. Используется в основном для разработки программного обеспечения, но может применяться и для других целей.

22)Сохранение и восстановление баз данных.

**Ответ:**

Сохранение баз данных происходит благодаря следующим методам: Миграции – перенос данных из устаревшей в новую программу баз данных.

XML – преобразование исходной информации базы данных в стандартный формат XML.

Эмуляция – воссоздание старой среды с использованием новых технологий и ПО.

Восстановление баз данных происходит благодаря журналу транзакций, который используется для восстановления БД. Возможные варианты: Индивидуальный откат транзакции, Восстановление после внезапного сбоя, Восстановление после внезапной поломки сервера.

23)Обеспечение безопасности функционирования ИС.

**Ответ:**

Обеспечение безопасности функционирования информационной системы — это комплексный процесс, включающий в себя ряд мероприятий и практик для защиты системы от угроз и обеспечения ее эффективного и безопасного функционирования. Основные шаги для обеспечения безопасности функционирования информационной системы: авторизация, защита от вредоносного программного обеспечения (антивирус, брандмауэр), шифрование данных, введение журнала аудита для отслеживания активностей в системе, регулярные обновления для избавления от багов и дыр, обучение пользователей.

24)Организация доступа пользователей к ИС.

**Ответ:**

Давай рассмотрим ключевые аспекты организации доступа пользователей к ИС:  
1. **Идентификация, аутентификация и авторизация:**  
- **Идентификация:** Процесс определения личности пользователя (например, уникальное имя пользователя или идентификатор).  
- **Аутентификация:** Проверка подлинности пользователя (через пароль, биометрические данные и т. д.).  
- **Авторизация:** Определение прав доступа пользователя к определенной информации или функциональности системы.  
2. **Управление ролями и правами доступа:**  
- **Роли пользователей:** Определение уровня доступа для различных категорий пользователей в соответствии с их обязанностями и функциями.  
- **Права доступа:** Назначение конкретных разрешений на доступ к данным и функциональности системы для каждой роли.  
3. **Многоуровневая защита данных:**  
- **Шифрование:** Защита конфиденциальных данных при их передаче или хранении путем преобразования в непонятный для посторонних вид.  
  
- **Управление ключами:** Безопасное управление ключами шифрования для обеспечения доступа только авторизованным пользователям.  
4. **Системы мониторинга и аудита:**  
- **Мониторинг доступа:** Отслеживание действий пользователей в системе для обнаружения аномального поведения или попыток несанкционированного доступа.  
- **Аудитаред:ист:** Зафиксированные действия пользователей, проведенные операции и изменения в системе с целью обеспечения прозрачности и возможности восстановления данных.  
5. **Двухфакторная аутентификация:**  
- **Использование двух (или более) методов аутентификации:** Например, пароль и одноразовый код, чтобы усилить безопасность доступа к системе.  
 6. **Управление сеансами и выход из системы:**  
- **Управление временем сеанса:** Ограничение длительности сеанса пользователя для предотвращения несанкционированной активности.  
- **Безопасный выход из системы:** Убедительное завершение сеанса пользователя для предотвращения несанкционированного доступа при выходе пользователя из системы.

25)Организация сбора данных об ошибках в ИС, Источники сведений.

**Ответ:**

Сбор данных об ошибках в информационной системе (ИС) является важным этапом для обеспечения ее безопасности и надежности. Для этого необходимо использовать соответствующие источники сведений. Вот некоторые из них:

1. Журналы событий (логи) – ведение логов событий и ошибок в ИС помогает выявлять проблемы и аномалии, а также отслеживать действия пользователей и системы.

2. Отчеты об ошибках – внутренние инструменты ИС или сторонние программы могут генерировать автоматические отчеты об ошибках и сбоях.

3. Мониторинг системы – использование специализированных инструментов для мониторинга работы ИС позволяет оперативно реагировать на возникшие проблемы

4. Обращения пользователей – отзывы и жалобы пользователей могут быть ценным источником информации о возможных проблемах в ИС.

5. Анализ уязвимостей – регулярный сканирование и анализ уязвимостей в ИС помогает выявлять потенциальные угрозы и источники ошибок.

6. Системы мониторинга безопасности – использование средств мониторинга безопасности, таких как системы предотвращения вторжений (IDS) и системы обнаружения вторжений (IPS), помогает выявлять и реагировать на аномальное поведение в ИС.

Эффективный сбор данных об ошибках в ИС требует комплексного подхода и использования различных источников информации. Анализ собранных данных помогает улучшить работу системы, повысить ее безопасность и минимизировать возможные риски.

26)Системы управления производительностью приложения.

**Ответ:**

Системы управления производительностью приложения (Application Performance Management, APM) предназначены для мониторинга, анализа и оптимизации работы приложений с целью обеспечения их высокой производительности, надежности и доступности для пользователей

Ниже приведены основные компоненты и функции систем управления производительностью приложений:

1. Мониторинг производительности: сбор и анализ данных о производительности приложения, включая использование ресурсов (память, процессор), время отклика, объем трафика и другие метрики.

2. Мониторинг транзакций: отслеживание и анализ выполнения транзакций в приложении, выявление узких мест и проблем, связанных с обработкой запросов

3. Мониторинг пользовательского опыта: оценка и анализ пользовательского опыта, включая время загрузки страниц, частоту сбоев и другие аспекты, влияющие на удовлетворенность пользователей.

4. Аналитика и отчетность: предоставление отчетов и аналитики о работе приложения, выявление трендов, аномалий и рекомендации по улучшению производительности

5. Управление нагрузкой: тестирование и анализ производительности приложения под различными нагрузками, выявление проблем и оптимизация ресурсов.

6. Мониторинг инфраструктуры: отслеживание и анализ работы серверов, баз данных, сети и других компонентов инфраструктуры, влияющих на производительность приложения.

Системы управления производительности приложений помогают компаниям эффективно управлять производительностью своих приложений, быстро выявлять и устранять проблемы, обеспечивать стабильную работу системы и улучшать пользовательский опыт.

27)Мониторинг сетевых ресурсов.

**Ответ:**

Мониторинг компьютерной сети — это процесс постоянного отслеживания компьютерной сети на наличие медленных или неисправных компонентов, проверка состояния метрик, в том числе метрик качества предоставления сервиса.

28)Схемы и алгоритмы ошибок, использование баз знаний.

**Ответ:**

В информатике существует несколько различных типов ошибок, которые могут возникнуть при выполнении программ или алгоритмов. Некоторые из них могут быть предотвращены, а другие – только обнаружены и исправлены. Ниже приведены основные типы ошибок, а также способы их обработки:

1. Синтаксические ошибки: возникают при нарушении правил языка программирования. Они обычно обнаруживаются компилятором или интерпретатором и должны быть исправлены до выполнения программы.

2. Логические ошибки: это ошибки в алгоритме или логике программы, которые приводят к неправильным результатам. Их трудно обнаружить, поэтому для поиска логических ошибок используются отладчики и тестирование программы

3. Ошибки времени выполнения: возникают во время выполнения программы из-за различных причин, таких как недоступность ресурсов, некорректные данные ввода и т. д. Для обработки таких ошибок используются исключения и обработка ошибок.

4. Ошибки памяти: возникают при обращении к недопустимым участкам памяти, например, при обращении к уже освобожденной памяти или выходе за пределы массива. Для предотвращения таких ошибок используются специальные инструменты и техники программирования.

Что касается использования баз знаний, они могут быть полезны для распознавания и исправления ошибок в программном обеспечении. Например, база знаний может содержать информацию о типичных проблемах и способах их решения, что позволяет быстро и эффективно идентифицировать, и исправлять ошибки.

Также базы знаний могут применяться для создания экспертных систем, которые могут использоваться для автоматизации процесса анализа и исправления ошибок. Экспертные системы используют знания экспертов в определенной области для принятия решений и решения проблем, включая исправление ошибок в программном обеспечении.

Таким образом, базы знаний могут быть эффективным инструментом для обработки ошибок и повышения качества программного обеспечения. Они помогают быстро выявлять и исправлять проблемы, а также предотвращать их возникновение в будущем.

29)Отчет об ошибках системы: содержание, использование информации.

**Ответ:**

Отчет об ошибках системы

Дата: дата

Расположение: местоположение системы

Описание ошибки

1. Проблема: Система выдает ошибку при попытке доступа к определенной странице/функции/файлу.

Описание: при попытке открыть страницу название страницы система выдает сообщение об ошибке и не позволяет получить доступ к данным.

2. Проблема: Некорректное отображение информации на экране.

Описание: на экране отображается неправильная информация, либо отображение информации смешано или искажено.

3. Проблема: Система периодически выходит из строя или зависает.

Описание: при использовании системы возникают сбои, и система периодически выходит из строя, либо зависает и требует перезагрузки.

Действия по решению проблемы:

1. Попытаться обновить страницу/файл и повторить попытку доступа.

2. Проверить правильность ввода данных и корректность отображения информации.

3. Перезагрузить систему или выполнить обновление программного обеспечения.

Если описанные выше действия не помогли решить проблему, рекомендуется обратиться к администратору системы или технической поддержке для дальнейших инструкций и помощи.

Будьте внимательны при использовании системы и следите за появлением ошибок, чтобы своевременно решать возникающие проблемы.

31)Пользовательская документация: “Руководство программиста”, “Руководство системного администратора”.

Руководство программиста — это эксплуатационно-техническая документация, которая необходима, когда система предоставляет возможность написания, редактирования или использования программного кода.

Руководство программиста содержит информацию, которая помогает разработчику воспользоваться возможностями системы. В документе могут быть указаны:

* назначение, структура входных и выходных данных программных функций;
* возможности по созданию программного кода, особенности его интерпретации и компиляции;
* синтаксические особенности используемого языка программирования;
* возможные правила и ограничения при работе с программным кодом;
* различные инструкции по работе с программой.

Состав типового руководства программиста регламентируется ГОСТ 19.504.

Руководство системного администратора — это документ, который раскрывает информацию о комплексе технических средств, необходимых для работы программного обеспечения, а также описывает процесс и особенности установки, настройки и поддержки работоспособности ПО.

Согласно стандарту ГОСТ 19.503-79, руководство системного администратора должно содержать следующие разделы:

* Общие сведения о программе.
* Структура программы.
* Настройка программы.
* Проверка программы.
* Дополнительные возможности.
* Сообщения системному программисту.

В зависимости от особенностей документа допускается объединять отдельные разделы или вводить новые.

30)Методы и инструменты тестирования приложения.

**Ответ:**

Методы тестирования приложения: Тестирование белого ящика (Полный доступ к исходному коду для его анализа), Тестирование черного ящика (тестирование проводиться на внешних проявлениях), Тестирование серого ящика (тестирование имеет частичный доступ к исходному коду иди знает некоторые детали), Ручное тестирование (Тестировщик самостоятельно взаимодействует с программой), Автоматическое тестирование (Тестирование набором тестовых сценариев разработанных тестировщиком).

31)Пользовательская документация: “Руководство программиста”, “Руководство системного администратора”.

**Ответ:**

1. Руководство программиста:

- Описание архитектуры и основ функционирования системы: Подробное описание структуры информационной системы, включая компоненты, модули, их взаимодействие и данные, с которыми они работают.

- Инструкции по разработке и поддержке кода: Рекомендации по организации разработки, стандартам кодирования, тестированию и сопровождению приложений.

- Использование инструментов и технологий: Обзор используемых программных средств, инструментов разработки, фреймворков, библиотек и способы их применения в рамках системы.

- Отладка и устранение проблем: Инструкции по поиску и исправлению ошибок, отладке программного кода, оптимизации и улучшению производительности приложений.

2. Руководство системного администратора:

- Управление системой: Информация о настройке, конфигурации и управлении аппаратными и программными компонентами информационной системы.

- Мониторинг и обслуживание: Инструкции по мониторингу состояния системы, выявлению и устранению сбоев, выполнению планового обслуживания и резервному копированию.

- Безопасность и доступ: Рекомендации по обеспечению безопасности данных, контролю доступа, настройке антивирусной защиты и другим аспектам обеспечения информационной безопасности.

- Работа с пользователями: Инструкции по обучению пользователей работе с системой, решению типовых проблем, предоставлению технической поддержки.

32)Выявление аппаратных ошибок ИС.

**Ответ:**

Методы выявления аппаратных ошибок ИС

1. Встроенные средства диагностики

Самотестирование при включении (POST): проверяет основные компоненты системы (память, процессор, видеокарту) при запуске.

Тесты памяти: проверяют наличие ошибок в оперативной памяти.

Тесты жесткого диска: проверяют ошибки чтения/записи на жестком диске.

Тесты процессора: проверяют работоспособность процессора и кэша.

2. Программные инструменты диагностики

memtest86+: Расширенный инструмент тестирования памяти.

HD Tune: Инструмент для тестирования жестких дисков.

Prime95: Инструмент для тестирования процессора и кэша.

FurMark: Инструмент для тестирования видеокарты.

3. Мониторинг системы

Журналы событий: записывают ошибки и предупреждения, которые могут указывать на аппаратные проблемы.

Мониторинг температуры: Чрезмерная температура может указывать на проблемы с охлаждением или аппаратные сбои.

Мониторинг напряжения: Нестабильное напряжение может привести к аппаратным ошибкам.

4. Физическая проверка

Визуальный осмотр: Проверка на наличие повреждений компонентов, таких как вздутые конденсаторы или потемневшие области на плате.

Очистка: Удаление пыли и мусора, которые могут вызвать перегрев или короткие замыкания.

Переустановка компонентов: Переустановка памяти, процессора или видеокарты может устранить плохие контакты.

5. Стресс-тестирование

Стресс-тесты памяти: Запуск тестов памяти в течение длительного периода времени для выявления скрытых ошибок.

Стресс-тесты процессора: Запуск ресурсоемких задач для проверки стабильности процессора.

Стресс-тесты жесткого диска: Запись и чтение больших объемов данных для проверки надежности диска.

6. Замена компонентов

Замена памяти: Установка новой оперативной памяти может устранить ошибки памяти.

Замена процессора: Установка нового процессора может устранить проблемы с процессором или кэшем.

Замена видеокарты: Установка новой видеокарты может устранить проблемы с графикой или отображением.

33)Техническое обслуживание аппаратных средств.

**Ответ:**

Техническое обслуживание аппаратных средств включает в себя ряд действий, направленных на поддержание и оптимальную работу компьютерного оборудования. Вот некоторые основные аспекты технического обслуживания аппаратных средств:

1. Регулярная чистка: Аппаратные средства, такие как компьютеры, принтеры, серверы и другие устройства, нуждаются в регулярной чистке. Это включает удаление пыли, грязи и других загрязнений, которые могут накапливаться внутри и на поверхности устройств. Чистка помогает предотвратить перегрев и повреждение компонентов.

2. Обновление программного обеспечения: Регулярное обновление драйверов и программного обеспечения для аппаратных средств помогает устранить ошибки, улучшить совместимость и обеспечить более стабильную работу устройств. Это может включать обновление BIOS, драйверов видеокарты, аудио-драйверов и других компонентов.

3. Проверка на наличие обновлений прошивки: Некоторые аппаратные устройства, такие как маршрутизаторы, коммутаторы и другие сетевые устройства, имеют прошивку, которую можно обновлять. Обновление прошивки может улучшить безопасность, исправить ошибки и добавить новые функции. Регулярная проверка наличия обновлений прошивки и их установка являются важной частью технического обслуживания сетевого оборудования.

4. Резервное копирование данных: Регулярное создание резервных копий данных является неотъемлемой частью технического обслуживания аппаратных средств. Это важно для предотвращения потери данных в случае сбоев оборудования, атак хакеров или случайного удаления информации. Резервные копии могут быть созданы на внешних носителях, в облачном хранилище или на других компьютерах.

5. Проверка и замена неисправных компонентов: В процессе технического обслуживания может возникнуть необходимость в проверке и замене неисправных компонентов. Это могут быть неисправные жесткие диски, оперативная память, блоки питания и другие элементы. Регулярная проверка аппаратных средств на наличие неисправностей помогает предотвратить поломки и сбои в работе.

6. Мониторинг и анализ производительности: Техническое обслуживание аппаратных средств также включает мониторинг и анализ производительности. Это может включать проверку загрузки процессора, использования оперативной памяти, дискового пространства и сетевого трафика. Мониторинг позволяет выявить проблемы производительности и принять меры для их устранения.

7. Физическая безопасность: Техническое обслуживание аппаратных средств также включает обеспечение физической безопасности устройств. Это может включать установку защитных замков, контроль доступа к серверным помещениям, регулярную проверку наличия повреждений и т.д.

Важно отметить, что конкретные действия по техническому обслуживанию аппаратных средств могут различаться в зависимости от типа устройств и их конфигурации. Руководство системного администратора может содержать подробные инструкции и рекомендации по техническому обслуживанию конкретных систем и устройств.

34)Базовая структура ИС.

**Ответ:**

Структура информационных систем (ИС) состоит из отдельных частей, называемых подсистемами. Среди основных подсистем ИС обычно выделяют: Информационное обеспечение, Техническое обеспечение, Математическое обеспечение, Программное обеспечение, Организационное обеспечение, Правовое обеспечение.

35)Основное оборудование системной интеграции.

**Ответ:**

1. Сетевое оборудование:

- Маршрутизаторы и коммутаторы: для управления и маршрутизации сетевого трафика.

2. Системы хранения данных:

- Хранилища данных (SAN): для централизованного и высокопроизводительного хранения данных.

3. Серверное оборудование:

- Серверы: для обработки данных, хранения информации и выполнения специфических функций.

4. Устройства управления системой:

- Устройства мониторинга и управления: для контроля и администрирования работы системы.

5. Программное обеспечение:

- Системы управления интеграцией (ESB): для обеспечения взаимодействия и интеграции компонентов системы.

6. Оборудование для обеспечения информационной безопасности:

- Средства аутентификации и авторизации: для защиты доступа к системе.

7. Оборудование для резервного копирования и восстановления:

- Устройства резервного копирования: для сохранения данных и обеспечения возможности восстановления в случае необходимости.

36)Особенности информационного, программного и технического обеспечения различных видов АИС.

**Ответ:**

Техническое обеспечение АИС включает в себя аппаратное обеспечение (компьютеры, серверы, сетевое оборудование), операционные системы, средства связи и другие технические средства, необходимые для функционирования системы.

Различные виды АИС могут иметь различные особенности информационного, программного и технического обеспечения в зависимости от их целей и специфики. Например, бухгалтерские АИС будут содержать специализированные программы для учета финансовых операций, а медицинские АИС - программы для хранения и обработки медицинских данных пациентов.

37)Особенности сопровождения ИС управление качеством, технической и технологической подготовки производства.

**Ответ:**

Ниже приведены основные особенности сопровождения ИС в контексте управления качеством и подготовки производства:

1. Управление качеством:

- Оценка и контроль качества информационной системы. Это включает в себя мониторинг работы системы, анализ отклонений, выявление и устранение ошибок, обновление программного обеспечения.

2. Техническая подготовка производства:

- Обеспечение работоспособности и совместимости аппаратного и программного обеспечения.

3. Технологическая подготовка производства:

- Анализ требований бизнес-процессов и определение необходимых изменений в информационной системе.

Сопровождение ИС включает в себя комплексный подход к управлению качеством, технической и технологической подготовке производства с целью обеспечения эффективной работы системы и повышения конкурентоспособности предприятия.

38)Особенности сопровождения ИС поисковосправочных служб, библиотек и патентных ведомств.

**Ответ:**

Поисково-справочные службы:

- Обновление информации: важно поддерживать актуальность и точность информации в базе данных или поисковой системе для обеспечения достоверных результатов.

- Улучшение интерфейсов и поисковых функций: Непрерывное развитие пользовательского интерфейса и алгоритмов поиска для увеличения эффективности и комфорта пользователей.

- Защита данных: Обеспечение безопасности и конфиденциальности хранимой информации, особенно при работе с чувствительными данными пользователей.

- Техническая поддержка: Гарантирование бесперебойной работы системы, своевременное обнаружение и устранение сбоев для непрерывной доступности информации.

39)Особенности сопровождения ИС управления “Умный дом”.

**Ответ:**

Ниже приведены основные особенности сопровождения ИС управления "Умный дом":

1. Мониторинг и обновление устройств

2. **Интеграция новых устройств**

3. **Безопасность**

4. **Управление энергопотреблением**

5. **Поддержка пользователей**:  
Обучение пользователей работе с системой "Умный дом" и ее возможностями.

6. **Анализ данных и оптимизация процессов**

40)Особенности сопровождения ИС обслуживания многозонного мультимедийного пространства.

**Ответ:**

Сопровождение ИС обслуживания многозонного мультимедийного пространства охватывает весь комплекс мероприятий, направленных на обеспечение непрерывной и эффективной работы ИС. Основная цель сопровождения ИС - обеспечить бесперебойную работу системы и удовлетворение потребностей пользователей.

Особенности:

- Управление многозонностью: возможность управления и настройки каждой зоны отдельно, а также координация работы между зонами.

- Поддержка различных типов мультимедийных компонентов: поддержка всех компонентов системы, их настройка, мониторинг и управление.

- Масштабируемость: способность эффективного управления и поддержки системы на большой площади.

- Мониторинг и управление: возможность мониторинга работы компонентов системы и их управление.

- Резервирование и отказоустойчивость: обеспечение непрерывной работы системы при отказе компонентов с помощью резервирования и автоматического переключения на резервные системы.

- Обновление и модернизация: возможность обновления и модернизации компонентов системы, включая замену устаревших компонентов и обновление программного обеспечения.

41)Особенности сопровождения ИС удаленного управления и контроля объектов.

**Ответ**:

Дистанционное управление и контроль: возможность управления и мониторинга объектов удаленно, без необходимости физического присутствия на месте.

- Мониторинг состояния объектов: система позволяет отслеживать различные параметры и состояние объектов, такие как температура, влажность, энергопотребление и другие.

- Автоматизация процессов: возможность автоматизировать определенные процессы и задачи на объектах, что позволяет сократить человеческую ошибку и повысить эффективность работы.

- Удаленное обновление и настройка: возможность обновлять программное обеспечение и настраивать систему удаленно, без необходимости физического доступа к объектам.

- Аналитика и отчетность: система предоставляет возможность анализировать данные и создавать отчеты о работе объектов, что помогает в принятии решений и оптимизации работы.

- Безопасность и защита данных: система обеспечивает защиту данных и информации от несанкционированного доступа, используя различные механизмы шифрования и аутентификации.

42)Особенности сопровождения ИС реального времени.

**Ответ:**

1. Высокая требовательность к надежности: ИС реального времени обычно используются в критических сферах, таких как авиация, медицина или промышленность, где любая ошибка может иметь серьезные последствия.

2. Быстрая реакция на изменения: ИС реального времени должны быть готовы к быстрой адаптации к изменяющимся условиям и требованиям. Сопровождение должно включать механизмы для быстрой реакции на изменения и внесения необходимых корректировок.

3. Высокая производительность: ИС реального времени должны обеспечивать высокую производительность и отзывчивость, чтобы обрабатывать данные и выполнять операции в режиме реального времени. Сопровождение должно включать мониторинг и оптимизацию производительности системы.

4. Сложность отладки: Отладка ИС реального времени может быть сложной из-за их сложности и специфики работы. Сопровождение должно включать инструменты и методы для эффективной отладки и исправления ошибок.

5. Зависимость от внешних факторов: ИС реального времени могут быть зависимы от внешних факторов, таких как сетевая задержка или оборудование. Сопровождение должно учитывать эти факторы и предусматривать меры для минимизации их влияния на работу системы.

43)Модели качества ИС. Стандарты управления качеством.

**Ответ:**

Модели:

1. Модель качества ISO 9126: это международный стандарт, который определяет атрибуты качества ИС: функциональность, надежность, используемость, эффективность, удобство сопровождения и переносимость.

2. Модель качества ISO 25010: Эта модель является обновленной версией ISO 9126 и включает в себя восемь атрибутов качества информационных систем: функциональность, надежность, используемость, эффективность, безопасность, сопровождаемость, переносимость и совместимость.

3. Модель качества CMMI: это модель управления качеством, которая оценивает и улучшает процессы разработки и сопровождения информационных систем. Она включает пять уровней зрелости, от начинающего до оптимального, и охватывает различные аспекты, такие как управление проектами, инженерия требований, разработка и тестирование.

Стандарты:

1. ISO 9001: это международный стандарт, который устанавливает требования к системе управления качеством. Он охватывает различные аспекты, такие как управление процессами, удовлетворение потребностей клиентов, улучшение процессов и контроль качества.

2. ITIL (Information Technology Infrastructure Library): это набор рекомендаций и методологий для управления IT-сервисами. Он включает в себя различные практики, такие как управление инцидентами, проблемами, изменениями и конфигурациями, которые помогают обеспечить высокое качество работы информационных систем.

3. Six Sigma: это методология, которая стремится уменьшить дефекты и несоответствия в процессах. Она использует статистические методы и инструменты для анализа данных и улучшения процессов, что приводит к повышению качества информационных систем.

44)Надежность ИС: основные понятия и определения.

**Ответ:**

Надежность ИС – это свойство сохранять заданные характеристики при определенных условиях эксплуатации. Показатели надежности ИС: Безотказность, Долговечность, Ремонтопригодность, Сохраняемость.

45)Метрики качества.

**Ответ:**

Метрики качества — это измерения, которые помогают нам оценить производительность, надежность и общее качество наших продуктов. Они дают ценную информацию о пользовательском опыте, стабильности продукта и соблюдении стандартов.

46)Показатели надежности в соответствии со стандартами.

**Ответ:**

Показатели надежности в информационных системах являются критериями, которые определяют степень устойчивости и надежности работы системы. Они позволяют оценить, насколько система способна обеспечить непрерывную работу, защитить данные от потерь и повреждений, а также обеспечить доступность и конфиденциальность информации.

Перечислим основные показатели надежности в соответствии со стандартами в сопровождении информационных систем:

1. Доступность (Availability): это показатель, определяющий время, в течение которого информационная система доступна для использования

2. Надежность (Reliability): это показатель, который характеризует степень вероятности безотказной работы информационной системы в течение определенного времени.

3. Устойчивость к отказам (Fault tolerance): это способность информационной системы продолжать работу при возникновении отказов в отдельных компонентах или подсистемах. Это включает в себя резервирование, дублирование и другие методы обеспечения непрерывности работы.

5. Защищенность (Security): это показатель, оценивающий степень защиты информации от несанкционированного доступа, изменения или уничтожения. Включает в себя аутентификацию, авторизаию, шифрование и другие меры безопасности.

6. Производительность (Performance): это показатель, характеризующий скорость и эффективность работы информационной системы при выполнении различных операций и задач.

47)Методы обеспечения и контроля качества ИС.

**Ответ:**

Под контролем ИС понимают процессы, обеспечивающие обнаружение ошибок в их функционировании, вызванных отказами аппаратуры, ошибками в программах или другими причинами.

Средства контроля ИС подразделяются на аппаратные, программные и смешанные. Они характеризуются тремя основными параметрами: полнотой (глубиной) контроля, временем обнаружения ошибки и сложностью.

Полнота контроля оценивается как доля отказов, обнаруживаемых в результате контроля, от общего их количества.

Время обнаружения ошибки (время контроля) определяется как интервал времени от момента возникновения ошибки до момента ее обнаружения.

Сложность средств контроля характеризуется массой, размерами, стоимостью, потребляемой энергией, памятью и другими параметрами аппаратных средств.

Классификация методов и средств контроля правильности функционирования информационных систем:

1) По характеру контроль в ИС подразделяется на:

- Оперативный контроль осуществляется в ходе решения задач и позволяет в процессе их решения немедленно обнаруживать ошибку.

- Тестовый контроль осуществляется в специально отведенные промежутки времени на основе решения специальных, тестовых задач.

2) По способу организации различают контроль прямой, обратный и

Смешанный

48)Виды интеллектуальных систем и области их применения.

**Ответ:**

Интеллектуальные системы — это системы, способные обрабатывать информацию и принимать решения, используя методы искусственного интеллекта. Они могут быть применены в различных областях, включая сопровождение информационных систем.

Вот некоторые виды интеллектуальных систем и области их применения в сопровождении информационных систем:

1.Системы мониторинга и аналитики: обнаружение аномалий, прогнозирование отказов, анализ производительности.

2. Системы автоматизации рутинных задач: управление резервными копиями, планирование обновлений, мониторинг производительности.

3.Системы поддержки принятия решений: анализ данных, предсказание проблем, оптимальные стратегии обслуживания.

4.Системы управления конфигурацией: автоматическое выявление изменений, контроль версий, управление изменениями.

5.Системы диагностики и решения проблем: диагностика проблем, предложение решений, автоматическое исправление ошибок.

49)Архитектура интеллектуальных ИС.

**Ответ:**

Архитектура интеллектуальных информационных систем (ИС) — это структура и организация компонентов, процессов и данных, которые обеспечивают реализацию и функционирование интеллектуальных технологий и методов в рамках информационной системы.

50)Типовая схема функционирования интеллектуальной системы.

**Ответ:**

1. Мониторинг: интеллектуальная система собирает данные о работе информационных систем.

2. Анализ: Данные анализируются для выявления проблем и трендов.

3. Диагностика: Интеллектуальная система проводит диагностику проблем и сбоев.

4. Прогнозирование: предсказывает возможные неисправности и сбои.

5. Принятие решений: принимает решения по оптимизации работы информационных систем.

6. Управление: автоматически управляет информационными системами.

7. Обратная связь: получает обратную связь и обучается для улучшения своих функций.

Такая схема позволяет интеллектуальной системе эффективно сопровождать информационные системы, повышая их надежность и производительность.