**Перечень теоретических вопросов к экзамену МДК.06.03 Устройство и функционирование информационной системы**

1. **Классификация информационных систем**

По назначению:

Информационно-управляющие системы

Системы поддержки принятия решений

Информационно-поисковые системы

Информационно-справочные системы

Системы обработки данных

По структуре аппаратных средств:

Однопроцессорные

Многопроцессорные

Многомашинные

Сосредоточенные

С удаленным доступом

Вычислительные сети

По режиму работы:

Пакетная обработка

Индивидуального пользования

Коллективного пользования

По характеру взаимодействия с пользователем:

Диалоговый режим

Интерактивный режим

Режим реального времени

1. **Этапы развития информационных систем**

1. Этап ручной обработки данных (до 1960-х годов):

Данные обрабатывались вручную с использованием бумажных носителей. Этот этап характеризуется высокой трудоемкостью и низкой скоростью обработки информации.

2. Этап автоматизации (1960-е - 1980-е годы):

Появление первых компьютеров и программного обеспечения для автоматизации обработки данных. Начали развиваться базы данных и системы управления ими.

3. Этап интеграции (1980-е - 1990-е годы):

Разработка интегрированных информационных систем, таких как ERP-системы, которые объединяют различные функции и процессы в одной системе. Увеличение использования сетевых технологий.

4. Этап интернета и глобализации (1990-е - 2000-е годы):

Появление веб-технологий и облачных решений. Информационные системы стали доступными через интернет, что позволило расширить их функциональность и доступность.

5. Этап больших данных и аналитики (2000-е - настоящее время):

Развитие технологий обработки больших данных (Big Data) и аналитики. Появление систем, способных обрабатывать и анализировать огромные объемы информации в реальном времени.

6. Этап искусственного интеллекта и автоматизации (настоящее время):

Внедрение технологий искусственного интеллекта и машинного обучения в информационные системы для повышения их эффективности и автоматизации процессов.

1. **Документальные информационные системы**

Документальная ИС – это единое хранилище документов с инструментарием поиска и отбора необходимых документов

Единичным элементом данных неструктурированный наиболее мелкий документ

Основная задача накопление и предоставление пользователю документов, содержание, тематика, реквизиты которых адекватны его информационным потребностям

В зависимости от особенностей реализации хранилище документов и механизмов поиска можно разделить:

Системы на основе индексирования

Семантические навигационные системы

1. **Фактографические информационные системы**

Фактографические ИС накапливают и хранят данные в виде множества экземпляров одного или нескольких типов структурных элементов (информационных объектов)

Каждая из таких структурированных элементов или некоторая их совокупность отражает сведения по какому-либо факту, событию отделенному от всех прочих сведений

Основные признаки:

Простая структура данных

Сложная система взаимосвязей между агрегаторами данных

Организация доступа к данным и их обработка в оперативной и внешней памяти осуществляется через реализацию процессов получивших называние транзакций

Транзакция – последовательная совокупность операций имеющая отдельное смысловое значение по отношению к текущему состоянию БД

Их разделяют на:

Изменяющие состояние БД после завершения транзакции

Изменяющие состояние БД лишь временно с восстановлением исходного состояния данных после завершения транзакции

Совокупность функций СУБД по организации и управлению транзакциями называют монитором транзакций

1. **Геоинформационные системы**

Геоинформационные системы (ГИС) – это специализированные информационные системы, предназначенные для сбора, хранения, обработки, анализа и визуализации пространственных (географических) данных. ГИС позволяют интегрировать различные типы информации, связанные с географическим положением, и представлять их в виде карт, графиков и других визуальных форматов.

Основные компоненты ГИС:

Аппаратное обеспечение

Программное обеспечение

Данные

Методы и технологии

Пользователи

1. **Базовая структура информационной системы**

Аппаратное обеспечение

Программное обеспечение

Данные

Процессы

Пользователи

Сеть

1. **Системная интеграция**

Интеграция ИС – объединение ИС, связывающее множество документов и отношений в данных системах

Стандарт EAI – интеграционная программная структура, объединяющей различного рода приложения, разработанные независимо друг от друга, так чтобы они работали как одно целое, прозрачно для пользователя

1. **Общие подходы к интеграции систем**

В наши дни чаще всего применяются два подхода интеграции по типу «точка-точка» и интеграция по шине сервисов

5 уровней интеграции:

Интеграция бизнес-процессов

Интеграция приложений

Интеграция данных

Интеграция на основе стандартов

Интеграция платформ

1. **Объекты и методы интеграции систем**

Режимы интеграции:

Режим приближенный к реальному времени

Режим реального времени

Промежуточное программное обеспечение – ПО производителей компьютеров, которое приспосабливается под конкретные особенности установки. Слой между сетевыми ОС и приложениями, который помогает справляться с неоднородностью и распределенностью

Ключевые абстракции промежуточного ПО:

Вызовы удаленных процедур

Распределенные транзакции

Промежуточное ПО ориентированное на сообщения

Распределенные транзакции –это последовательность нескольких вызовов удаленных процедур являющихся согласованными, изолированными и долговечными

1. **Программные продукты для интеграции систем**

Существует ряд методов и средств, которые позволяют решить задачу интеграции:

Решения для интеграции данных: импорт данных в разнообразных форматах, их преобразование и очистка от ошибок, исключение дублирующихся записей

Интеграция приложений: обмен сообщениями и событиями между системами

Интеграция бизнес-процессов: выстраивается единая автоматизированная цепочка, в которой человек и машина выполняют свою часть работы, образуя эффективный бизнес-процесс

Система класса MDM

Технология ETL

Платформы класса ECM

Технология BPM

Технология ESB

1. **Основное оборудование системной интеграции**

Серверы:

Физические серверы

Виртуальные серверы

Сетевое оборудование:

Коммутаторы (Switches)

Маршрутизаторы (Routers

Модемы

Хранилища данных

Системы хранения

NAS

Рабочие станции и терминалы:

Персональные компьютеры и ноутбуки

Тонкие клиенты

Устройства ввода-вывода:

Принтеры и сканеры

Мониторы и проекторы

Системы управления и мониторинга:

Системы управления сетью

Системы управления данными

Оборудование безопасности:

Межсетевые экраны

Системы обнаружения и предотвращения вторжений

1. **Особенности информационного обеспечения различных видов АИС**

Автоматизированные информационные системы (АИС) играют ключевую роль в управлении и обработке данных в различных областях. Каждая категория АИС имеет свои особенности информационного обеспечения, которые зависят от целей, задач и специфики работы. Ниже представлены основные виды АИС и их особенности информационного обеспечения.

1. Управленческие информационные системы (УИС)

Описание: Эти системы предназначены для поддержки управленческих процессов на различных уровнях (стратегическом, тактическом и оперативном).

Особенности:

Интеграция данных: Объединение информации из различных источников для формирования единой базы данных.

Аналитические инструменты: Наличие инструментов для анализа данных, построения отчетов и прогнозирования.

Поддержка принятия решений: Предоставление информации в удобном виде для принятия управленческих решений.

2. Системы управления производством (СУП)

Описание: АИС, которые помогают управлять производственными процессами, включая планирование, контроль и оптимизацию.

Особенности:

Мониторинг в реальном времени: Возможность отслеживания производственных процессов в режиме реального времени.

Управление ресурсами: Оптимизация использования материальных, трудовых и финансовых ресурсов.

Интеграция с оборудованием: Связь с производственным оборудованием для автоматического сбора данных.

3. Системы управления проектами (СУП)

Описание: АИС, предназначенные для планирования, выполнения и контроля проектов.

Особенности:

Планирование и графики: Инструменты для создания графиков выполнения задач и распределения ресурсов.

Управление рисками: Механизмы для оценки и управления рисками, связанными с проектом.

Отчетность: Формирование отчетов о ходе выполнения проекта и использовании ресурсов.

4. Системы управления отношениями с клиентами (CRM)

Описание: АИС, которые помогают управлять взаимодействием с клиентами и анализировать данные о клиентах.

Особенности:

Хранение данных о клиентах: Систематизация информации о клиентах, их предпочтениях и истории взаимодействия.

Анализ поведения клиентов: Инструменты для анализа данных о покупках и предпочтениях клиентов.

Автоматизация маркетинга: Возможности для автоматизации маркетинговых кампаний и взаимодействия с клиентами.

5. Системы управления знаниями (СУЗ)

Описание: АИС, которые помогают собирать, хранить и распространять знания внутри организации.

Особенности:

База знаний: Создание и поддержка базы знаний, содержащей информацию и опыт сотрудников.

Поиск и доступ: Удобные инструменты для поиска и доступа к информации.

Системы обмена знаниями: Механизмы для обмена знаниями между сотрудниками и командами.

6. Системы электронного документооборота (СЭД)

Описание: АИС, предназначенные для автоматизации процессов создания, обработки и хранения документов.

Особенности:

Управление документами: Возможности для создания, редактирования, согласования и хранения документов.

Автоматизация процессов: Автоматизация процессов согласования и утверждения документов.

Безопасность и доступ: Механизмы для обеспечения безопасности и контроля доступа к документам.

7. Системы управления финансами (СУФ)

Описание: АИС, которые помогают управлять финансовыми потоками и отчетностью.

Особенности:

Бюджетирование: Инструменты для планирования и контроля бюджета.

Финансовая отчетность: Автоматизация формирования финансовых отчетов и анализ данных.

Управление активами: Возможности для учета и управления активами компании.

1. **Особенности программного обеспечения различных видов АИС**

Автоматизированные информационные системы (АИС) различаются по своему назначению, функциональности и архитектуре, что, в свою очередь, определяет особенности их программного обеспечения. Ниже представлены основные виды АИС и их особенности программного обеспечения.

1. Управленческие информационные системы (УИС)

Описание: Эти системы предназначены для поддержки управленческих процессов на различных уровнях.

Особенности ПО:

Интерфейсы для анализа данных: Наличие инструментов для визуализации и анализа данных (графики, диаграммы).

Модели принятия решений: Включение алгоритмов и моделей для поддержки принятия решений.

Интеграция с другими системами: Возможность интеграции с ERP, CRM и другими системами для получения актуальных данных.

2. Системы управления производством (СУП)

Описание: АИС, которые помогают управлять производственными процессами.

Особенности ПО:

Мониторинг в реальном времени: Программное обеспечение для отслеживания производственных показателей и состояния оборудования.

Планирование и оптимизация: Инструменты для планирования производственных процессов и оптимизации ресурсов.

Интерфейсы для взаимодействия с оборудованием: Программные интерфейсы для связи с производственными машинами и системами автоматизации.

3. Системы управления проектами (СУП)

Описание: АИС, предназначенные для планирования и контроля проектов.

Особенности ПО:

Графики и диаграммы: Инструменты для создания диаграмм Ганта и других графиков для визуализации хода проекта.

Управление задачами: Возможности для распределения задач и отслеживания их выполнения.

Отчетность: Функции для автоматического формирования отчетов о ходе выполнения проекта.

4. Системы управления отношениями с клиентами (CRM)

Описание: АИС, которые помогают управлять взаимодействием с клиентами.

Особенности ПО:

База данных клиентов: Хранение и управление данными о клиентах, их предпочтениях и истории взаимодействия.

Автоматизация маркетинга: Инструменты для автоматизации маркетинговых кампаний и рассылок.

Аналитика: Возможности для анализа поведения клиентов и эффективности продаж.

5. Системы управления знаниями (СУЗ)

Описание: АИС, которые помогают собирать и распространять знания внутри организации.

Особенности ПО:

База знаний: Программное обеспечение для создания и управления базой знаний.

Поиск и фильтрация: Инструменты для быстрого поиска информации и фильтрации данных.

Инструменты для совместной работы: Возможности для совместного редактирования и обмена знаниями между сотрудниками.

6. Системы электронного документооборота (СЭД)

Описание: АИС, предназначенные для автоматизации процессов создания и обработки документов.

Особенности ПО:

Управление документами: Функции для создания, редактирования, согласования и хранения документов.

Автоматизация процессов: Возможности для автоматизации процессов согласования и утверждения документов.

Безопасность и контроль доступа: Механизмы для обеспечения безопасности и контроля доступа к документам.

7. Системы управления финансами (СУФ)

Описание: АИС, которые помогают управлять финансовыми потоками и отчетностью.

Особенности ПО:

Бюджетирование: Инструменты для планирования и контроля бюджета.

Финансовая отчетность: Автоматизация формирования финансовых отчетов и анализ данных.

Управление активами: Возможности для учета и управления активами компании.

8. Системы управления персоналом (HRM)

Описание: АИС, которые помогают управлять процессами, связанными с персоналом.

Особенности ПО:

Учет рабочего времени: Инструменты для учета рабочего времени и расчета заработной платы.

Управление кадровыми документами: Возможности для хранения и обработки кадровых документов.

Аналитика по персоналу: Инструменты для анализа данных о сотрудниках и их производительности.

1. **Особенности технического обеспечения различных видов АИС**

Техническое обеспечение автоматизированных информационных систем (АИС) включает в себя аппаратные и программные компоненты, которые обеспечивают функционирование системы. Каждая категория АИС имеет свои особенности технического обеспечения, которые зависят от специфики задач, которые они решают. Ниже представлены основные виды АИС и их особенности технического обеспечения.

1. Управленческие информационные системы (УИС)

Описание: Эти системы предназначены для поддержки управленческих процессов на различных уровнях.

Особенности технического обеспечения:

Серверное оборудование: Высокопроизводительные серверы для обработки больших объемов данных и выполнения аналитических задач.

Системы хранения данных: Использование SAN или NAS для хранения и управления данными.

Сетевое оборудование: Надежные маршрутизаторы и коммутаторы для обеспечения стабильной работы сети.

2. Системы управления производством (СУП)

Описание: АИС, которые помогают управлять производственными процессами.

Особенности технического обеспечения:

Промышленное оборудование: Использование специализированных контроллеров (PLC) и датчиков для мониторинга производственных процессов.

Интерфейсы для связи с оборудованием: Программные и аппаратные интерфейсы для интеграции с производственными системами.

Системы визуализации: Использование SCADA-систем для мониторинга и управления производственными процессами.

3. Системы управления проектами (СУП)

Описание: АИС, предназначенные для планирования и контроля проектов.

Особенности технического обеспечения:

Серверы для хранения данных: Серверы для хранения проектной документации и данных.

Инструменты для совместной работы: Платформы для совместной работы, которые могут включать облачные решения.

Программное обеспечение для планирования: Специализированные программы для создания графиков и управления задачами.

4. Системы управления отношениями с клиентами (CRM)

Описание: АИС, которые помогают управлять взаимодействием с клиентами.

Особенности технического обеспечения:

Базы данных: Использование реляционных баз данных для хранения информации о клиентах.

Интерфейсы API: Наличие API для интеграции с другими системами (например, ERP, маркетинговыми платформами).

Сетевое оборудование: Надежные серверы и сетевые устройства для обеспечения доступа к системе.

5. Системы управления знаниями (СУЗ)

Описание: АИС, которые помогают собирать и распространять знания внутри организации.

Особенности технического обеспечения:

Системы хранения данных: Использование баз данных и хранилищ для хранения знаний и информации.

Инструменты для совместной работы: Платформы для обмена знаниями и совместного редактирования документов.

Системы поиска: Технологии для быстрого поиска и фильтрации информации.

6. Системы электронного документооборота (СЭД)

Описание: АИС, предназначенные для автоматизации процессов создания и обработки документов.

Особенности технического обеспечения:

Серверы для хранения документов: Использование серверов для хранения и управления документами.

Системы сканирования: Оборудование для цифровизации бумажных документов.

Интерфейсы для интеграции: Возможности интеграции с другими системами для автоматизации процессов.

7. Системы управления финансами (СУФ)

Описание: АИС, которые помогают управлять финансовыми потоками и отчетностью.

Особенности технического обеспечения:

Серверы для обработки данных: Высокопроизводительные серверы для обработки финансовых данных.

Базы данных: Использование реляционных баз данных для хранения финансовой информации.

Инструменты для отчетности: Программное обеспечение для автоматизации формирования финансовых отчетов.

8. Системы управления персоналом (HRM)

Описание: АИС, которые помогают управлять процессами, связанными с персоналом.

Особенности технического обеспечения:

Серверы для хранения данных: Серверы для хранения информации о сотрудниках и их документации.

Интерфейсы для интеграции

1. **Особенности сопровождения информационных систем бухгалтерского учета и материально-технического снабжения**

1. Сопровождение информационных систем бухгалтерского учета

1.1. Обновление программного обеспечения

1.2. Поддержка пользователей

1.3. Аудит и контроль

1.4. Интеграция с другими системами

1.5. Адаптация к изменениям

2. Сопровождение информационных систем материально-технического снабжения

2.1. Обновление и модернизация

2.2. Поддержка пользователей

2.3. Анализ и оптимизация процессов

1. **Особенности сопровождения информационных систем управления качеством, технической и технологической подготовки производства**

Сопровождение информационных систем управления качеством и технической и технологической подготовки производства требует комплексного подхода, включающего обновление программного обеспечения, поддержку пользователей, аудит и контроль, интеграцию с другими системами, а также адаптацию к изменениям. Эффективное сопровождение этих систем позволяет обеспечить их надежную работу, соответствие стандартам качества и удовлетворение потребностей бизнеса.

1. **Особенности сопровождения информационных систем поисково-справочных служб, библиотек и патентных ведомств**

**Сопровождение информационных систем поисково-справочных служб, библиотек и патентных ведомств имеет свои особенности, обусловленные спецификой работы этих организаций, типами обрабатываемой информации и требованиями пользователей. Ниже представлены ключевые аспекты сопровождения таких систем.**

1. Сопровождение информационных систем поисково-справочных служб

1.1. Обновление и поддержка базы данных

Регулярное обновление данных: Обеспечение актуальности информации, включая новые записи, изменения и удаления устаревших данных.

Качество данных: Проведение регулярных проверок на корректность и полноту данных.

1.2. Поддержка пользователей

Обучение пользователей: Проведение тренингов для сотрудников и пользователей по эффективному использованию системы.

Техническая поддержка: Обеспечение доступности службы поддержки для решения возникающих вопросов и проблем.

1.3. Интерфейс и удобство использования

Разработка пользовательского интерфейса: Обеспечение интуитивно понятного интерфейса для пользователей, включая возможность настройки под индивидуальные потребности.

Доступность: Обеспечение доступа к системе для различных категорий пользователей, включая людей с ограниченными возможностями.

1.4. Интеграция с другими системами

Совместимость: Обеспечение интеграции с другими информационными системами и ресурсами для расширения функциональности.

Обмен данными: Настройка механизмов обмена данными между различными системами для повышения точности и скорости обработки информации.

1.5. Анализ и отчетность

Мониторинг использования: Анализ статистики использования системы для выявления популярных запросов и улучшения функциональности.

Отчетность: Формирование отчетов о работе системы и ее эффективности.

2. Сопровождение информационных систем библиотек

2.1. Управление библиотечными ресурсами

Обновление каталога: Регулярное обновление и пополнение библиотечного каталога новыми изданиями и ресурсами.

Классификация и индексирование: Поддержка актуальности классификаций и индексов для облегчения поиска информации.

2.2. Поддержка пользователей

Обучение пользователей: Проведение обучающих мероприятий для пользователей по работе с библиотечными системами и ресурсами.

Техническая поддержка: Обеспечение доступности службы поддержки для решения проблем пользователей.

2.3. Интерфейс и удобство использования

Разработка интерфейса: Обеспечение удобного и интуитивно понятного интерфейса для поиска и доступа к ресурсам.

Доступность: Обеспечение доступа к библиотечным ресурсам для различных категорий пользователей.

2.4. Интеграция с другими системами

Совместимость: Интеграция с другими библиотечными системами и ресурсами для расширения функциональности.

Обмен данными: Настройка механизмов обмена данными между библиотечными системами и внешними ресурсами.

2.5. Анализ и отчетность

Мониторинг использования: Анализ статистики использования библиотечных ресурсов для выявления популярных материалов и улучшения обслуживания.

Отчетность: Формирование отчетов о работе библиотеки и ее ресурсах.

3. Сопровождение информационных систем патентных ведомств

3.1. Управление патентными данными

Обновление базы данных: Регулярное обновление информации о патентах, включая новые заявки, изменения и истечения сроков.

Качество данных: Обеспечение точности и полноты данных о патентах и заявках.

3.2. Поддержка пользователей

Обучение пользователей: Проведение обучающих мероприятий для сотрудников и пользователей по работе с патентными системами.

Техническая поддержка: Обеспечение доступности службы поддержки для решения возникающих вопросов и проблем.

3.3. Интерфейс и удобство использования

Разработка интерфейса: Обеспечение удобного интерфейса для поиска и доступа к патентной информации.

Доступность: Обеспечение доступа к патентной информации для различных категорий пользователей.

3.4. Интеграция с другими системами

1. **Особенности сопровождения информационных систем обслуживания многозонного мультимедийного пространства**
2. **Особенности сопровождения информационных систем удаленного управления и контроля объектов**

1. Обновление и модернизация программного обеспечения

1.1. Регулярные обновления

Обновление ПО: Периодическое обновление программного обеспечения для обеспечения совместимости с новыми мультимедийными форматами и стандартами.

Устранение ошибок: Быстрое реагирование на выявленные ошибки и уязвимости в системе.

1.2. Адаптация к новым технологиям

Интеграция новых технологий: Внедрение новых технологий, таких как виртуальная и дополненная реальность, для улучшения пользовательского опыта.

Поддержка новых форматов: Обеспечение поддержки новых мультимедийных форматов и протоколов.

2. Поддержка пользователей

2.1. Обучение и консультации

Обучение персонала: Проведение тренингов для сотрудников, работающих с системой, по использованию мультимедийных технологий и оборудования.

Поддержка пользователей: Обеспечение доступности службы поддержки для решения возникающих вопросов и проблем.

2.2. Интерфейс и удобство использования

Разработка пользовательского интерфейса: Обеспечение интуитивно понятного интерфейса для управления мультимедийным контентом и оборудованием.

Настройка под пользователя: Возможность настройки интерфейса под индивидуальные потребности пользователей.

3. Управление мультимедийным контентом

3.1. Организация контента

Каталогизация: Эффективная организация и каталогизация мультимедийного контента для упрощения поиска и доступа.

Управление правами: Обеспечение управления правами доступа к контенту для различных пользователей и групп.

3.2. Мониторинг и анализ

Анализ использования: Мониторинг статистики использования мультимедийного контента для выявления популярных материалов и улучшения обслуживания.

Обратная связь: Сбор обратной связи от пользователей для улучшения качества контента и обслуживания.

4. Интеграция с другими системами

4.1. Совместимость

Интеграция с другими системами: Обеспечение интеграции с системами управления событиями, CRM и другими для автоматизации процессов.

Обмен данными: Настройка механизмов обмена данными между различными системами для повышения точности и скорости обработки информации.

4.2. Сетевые технологии

Управление сетевой инфраструктурой: Обеспечение надежной работы сетевой инфраструктуры для передачи мультимедийного контента.

Оптимизация потоков данных: Оптимизация потоков данных для обеспечения высокой скорости и качества передачи мультимедийного контента.

5. Безопасность и защита данных

5.1. Защита контента

Управление доступом: Настройка систем управления доступом для защиты мультимедийного контента от несанкционированного доступа.

Шифрование данных: Использование шифрования для защиты данных при передаче и хранении.

5.2. Мониторинг безопасности

Аудит безопасности: Регулярные проверки системы на наличие уязвимостей и угроз безопасности.

Реагирование на инциденты: Разработка и внедрение процедур реагирования на инциденты безопасности.

1. **Особенности сопровождения информационных систем реального времени**

1. Обновление и модернизация программного обеспечения

1.1. Минимизация времени простоя

Планирование обновлений: Обновления должны проводиться в периоды минимальной нагрузки на систему, чтобы избежать сбоев в работе.

Использование "горячих" обновлений: Возможность обновления системы без остановки ее работы (hot swapping) для обеспечения непрерывности процессов.

1.2. Тестирование и валидация

Тестирование обновлений: Перед внедрением обновлений необходимо проводить тщательное тестирование в условиях, приближенных к реальным.

Валидация производительности: Проверка, что обновления не влияют на производительность и временные характеристики системы.

2. Поддержка пользователей

2.1. Обучение и документация

Обучение персонала: Регулярные тренинги для пользователей и администраторов системы по новым функциям и изменениям.

Документация: Поддержка актуальной документации, включая руководства пользователя и технические спецификации.

2.2. Техническая поддержка

Круглосуточная поддержка: Обеспечение доступности службы поддержки 24/7 для быстрого реагирования на инциденты.

Мониторинг системы: Использование систем мониторинга для отслеживания состояния системы в реальном времени и быстрого выявления проблем.

3. Управление производительностью

3.1. Оптимизация ресурсов

Управление нагрузкой: Оптимизация распределения ресурсов для обеспечения необходимой производительности в условиях высокой нагрузки.

Кэширование: Использование кэширования для ускорения доступа к часто запрашиваемым данным.

3.2. Мониторинг производительности

Анализ производительности: Регулярный анализ производительности системы для выявления узких мест и их устранения.

Настройка параметров: Настройка параметров системы для достижения оптимального времени отклика и пропускной способности.

4. Надежность и отказоустойчивость

4.1. Резервирование и дублирование

Резервные копии: Регулярное создание резервных копий данных и конфигураций для восстановления в случае сбоя.

Дублирование компонентов: Использование дублирующих систем и компонентов для обеспечения непрерывности работы.

4.2. Тестирование на отказ

Стресс-тестирование: Проведение стресс-тестов для оценки поведения системы в условиях предельных нагрузок.

Планирование на случай аварий: Разработка и тестирование планов на случай аварий для быстрого восстановления работы системы.

5. Безопасность и защита данных

5.1. Управление доступом

Аутентификация и авторизация: Настройка надежных механизмов аутентификации и авторизации для защиты системы от несанкционированного доступа.

Мониторинг доступа: Ведение журналов доступа и мониторинг действий пользователей для выявления подозрительной активности.

5.2. Защита данных

Шифрование: Использование шифрования для защиты данных как в процессе передачи, так и при хранении.

Обнаружение вторжений: Внедрение систем обнаружения и предотвращения вторжений (IDS/IPS) для защиты от атак.

6. Интеграция с другими системами

6.1. Совместимость

Интерфейсы и API: Обеспечение совместимости с другими системами через стандартизированные интерфейсы и API.

Обмен данными: Настройка механизмов обмена данными между различными системами для повышения эффективности работы.

6.2. Сетевые технологии

Оптимизация сетевой инфраструктуры: Обеспечение надежной и быстрой сетевой инфраструктуры для передачи данных в реальном времени.

Управление трафиком: Использование технологий управления траф

1. **Структура и этапы проектирования информационной систем**

Проектирование информационных систем (ИС) — это сложный и многоэтапный процесс, который включает в себя несколько ключевых этапов и компонентов. Структура проектирования может варьироваться в зависимости от специфики проекта, однако общие этапы и элементы остаются схожими. Ниже представлена типичная структура и этапы проектирования информационных систем.

1. Анализ требований

1.1. Сбор требований

Интервью и опросы: Проведение встреч с заинтересованными сторонами для выявления их потребностей и ожиданий.

Анализ существующих систем: Изучение текущих систем и процессов для выявления недостатков и возможностей для улучшения.

1.2. Документирование требований

Функциональные требования: Определение функций, которые должна выполнять система.

Нефункциональные требования: Определение требований к производительности, безопасности, надежности и удобству использования.

2. Проектирование архитектуры системы

2.1. Определение архитектуры

Выбор архитектурного стиля: Определение подхода к проектированию (например, клиент-сервер, микросервисы, облачные решения).

Модульная структура: Разработка модульной структуры системы, включая основные компоненты и их взаимодействие.

2.2. Проектирование баз данных

Моделирование данных: Создание концептуальной, логической и физической модели данных.

Определение схемы базы данных: Проектирование таблиц, связей и индексов.

3. Проектирование пользовательского интерфейса

3.1. Создание прототипов

Wireframes: Разработка каркасных моделей интерфейса для визуализации структуры и навигации.

Интерактивные прототипы: Создание интерактивных прототипов для тестирования пользовательского опыта.

3.2. Дизайн интерфейса

Графический дизайн: Разработка визуального оформления интерфейса, включая цветовую палитру, шрифты и элементы управления.

Удобство использования: Обеспечение интуитивно понятного и удобного интерфейса для пользователей.

4. Разработка системы

4.1. Кодирование

Выбор технологий: Определение языков программирования, фреймворков и инструментов разработки.

Разработка компонентов: Написание кода для различных модулей и компонентов системы.

4.2. Интеграция

Интеграция модулей: Объединение разработанных компонентов в единую систему.

Тестирование интеграции: Проверка взаимодействия между модулями и системами.

5. Тестирование системы

5.1. Функциональное тестирование

Проверка функциональности: Тестирование всех функций системы на соответствие требованиям.

Тестирование пользовательского интерфейса: Проверка удобства и интуитивности интерфейса.

5.2. Нефункциональное тестирование

Тестирование производительности: Оценка скорости, масштабируемости и надежности системы.

Тестирование безопасности: Проверка системы на уязвимости и соответствие требованиям безопасности.

6. Внедрение системы

6.1. Подготовка к внедрению

Планирование внедрения: Разработка плана по внедрению системы, включая обучение пользователей и миграцию данных.

Тестирование в реальных условиях: Проведение пилотного тестирования системы в реальных условиях.

6.2. Запуск системы

Внедрение: Официальный запуск системы в эксплуатацию.

Поддержка пользователей: Обеспечение технической поддержки и обучения пользователей.

7. Поддержка и сопровождение

7.1. Мониторинг работы системы

Сбор статистики: Мониторинг производительности и использования системы.

Обратная связь от пользователей: Сбор отзывов и предложений по улучшению системы.

7.2. Обновление и модернизация

Регулярные обновления: Внедрение обновлений и улучшений на основе собранной обратной связи.

Поддержка безопасности: Обеспечение актуальности системы в отношении безопасности и защиты данных.

1. **Модели качества информационных систем**

1. Модель ISO/IEC 25010

Модель ISO/IEC 25010 является одной из наиболее известных и широко используемых моделей качества программного обеспечения. Она определяет восемь характеристик качества, которые делятся на две группы: характеристики качества продукта и характеристики качества в процессе.

1.1. Характеристики качества продукта

Функциональность: Степень, в которой система удовлетворяет заявленным требованиям и ожиданиям пользователей.

Надежность: Способность системы выполнять заданные функции при определенных условиях в течение определенного времени.

Удобство использования: Легкость, с которой пользователи могут использовать систему для достижения своих целей.

Эффективность: Способность системы использовать ресурсы (время, память) оптимально.

Поддерживаемость: Легкость, с которой система может быть изменена для исправления дефектов, улучшения производительности или адаптации к изменяющимся требованиям.

Переносимость: Способность системы быть перенесенной с одной среды на другую.

4. Модель McCall

Модель McCall определяет качество программного обеспечения через три основные категории: продукт, процесс и пользователь. Она включает в себя 11 характеристик качества, таких как:

Корректность: Степень, в которой система выполняет заданные функции.

Эффективность: Использование ресурсов.

Удобство использования: Легкость в обучении и использовании.

Надежность: Способность системы работать без сбоев.

Поддерживаемость: Легкость внесения изменений.

1. **Модель качества информационной системы с изменяющимися предметными областями**

4. Метрики качества для изменяющихся предметных областей

Для оценки качества ИС в условиях изменяющихся требований можно использовать следующие метрики:

Время реакции на изменения: Время, необходимое для внесения изменений в систему в ответ на новые требования.

Частота обновлений: Количество обновлений и изменений, внесенных в систему за определенный период.

Уровень удовлетворенности пользователей: Оценка того, насколько система удовлетворяет потребности пользователей в условиях изменений.

Процент успешных изменений: Доля изменений, которые были успешно внедрены без негативного влияния на качество системы.

1. **Иерархическая модель качества информационной системы**

Иерархическая модель качества информационной системы (ИС) представляет собой структурированный подход к оценке и управлению качеством, который делит характеристики качества на несколько уровней. Эта модель позволяет более детально анализировать и управлять качеством системы, а также выявлять области для улучшения. Ниже представлены основные компоненты и уровни иерархической модели качества ИС.

1. Уровни иерархической модели качества

1.1. Высший уровень: Общие характеристики качества

На этом уровне определяются основные характеристики качества, которые являются критически важными для успешного функционирования ИС. К ним могут относиться:

Функциональность: Способность системы выполнять заданные функции и удовлетворять требованиям пользователей.

Надежность: Способность системы работать без сбоев и обеспечивать стабильную работу в течение времени.

Удобство использования: Легкость, с которой пользователи могут взаимодействовать с системой.

Эффективность: Оптимальное использование ресурсов (время, память, вычислительная мощность).

Поддерживаемость: Легкость, с которой система может быть изменена или обновлена.

Переносимость: Способность системы функционировать в различных средах.

1.2. Средний уровень: Подхарактеристики качества

Каждая из общих характеристик может быть разбита на более детализированные подхарактеристики. Например:

Функциональность:

Полнота: Насколько система охватывает все необходимые функции.

Корректность: Насколько правильно система выполняет свои функции.

Совместимость: Способность системы работать с другими системами и компонентами.

Надежность:

Доступность: Время, в течение которого система доступна для использования.

Устойчивость: Способность системы восстанавливаться после сбоев.

Защищенность: Способность системы защищать данные от несанкционированного доступа.

Удобство использования:

Интуитивность: Легкость, с которой пользователи могут понять и использовать интерфейс.

Эффективность: Способность пользователей выполнять задачи с минимальными усилиями.

1.3. Низший уровень: Метрики и показатели качества

На этом уровне определяются конкретные метрики и показатели, которые используются для измерения подхарактеристик. Например:

Для функциональности:

Количество реализованных функций по сравнению с запланированными.

Процент корректных результатов выполнения функций.

Для надежности:

Среднее время безотказной работы (MTBF).

Процент времени, когда система была доступна для пользователей.

Для удобства использования:

Время, необходимое пользователю для выполнения определенной задачи.

Результаты тестирования удобства использования (например, оценки пользователей).

1. **Стандарты управления качеством**

1. ISO 9001

ISO 9001 — это международный стандарт, который определяет требования к системе менеджмента качества (СМК). Он применяется в любых организациях, независимо от их размера и сферы деятельности. Основные принципы ISO 9001 включают:

Ориентация на клиента: Понимание и удовлетворение потребностей клиентов.

Лидерство: Установление единства целей и направления действий.

Вовлечение людей: Участие сотрудников в процессе управления качеством.

Процессный подход: Управление процессами для достижения желаемых результатов.

Улучшение: Постоянное улучшение процессов и системы управления качеством.

Фактический подход к принятию решений: Принятие решений на основе анализа данных и информации.

Взаимовыгодные отношения с поставщиками: Установление взаимовыгодных отношений с партнерами и поставщиками.

1. **Надежность информационных систем: основные понятия и определения**

Надежность информационных систем (ИС) — это важная характеристика, которая определяет способность системы выполнять свои функции в заданных условиях и в течение определенного времени без сбоев и ошибок. Надежность является критически важной для обеспечения стабильной работы систем, особенно в тех областях, где сбои могут привести к серьезным последствиям, таким как финансовые потери, утечка данных или угроза безопасности.

Основные понятия и определения

Надежность (Reliability): Надежность информационной системы определяется как вероятность того, что система будет выполнять заданные функции в течение определенного времени при заданных условиях эксплуатации. Это означает, что система должна быть способна функционировать без сбоев и ошибок.

Доступность (Availability): Доступность — это мера того, насколько система доступна для пользователей в любой момент времени. Она определяется как отношение времени, в течение которого система функционирует, к общему времени, включая время простоя. Доступность часто выражается в процентах.

[ \text{Доступность} = \frac{\text{Время работы}}{\text{Время работы} + \text{Время простоя}} \times 100% ]

Устойчивость (Robustness): Устойчивость — это способность системы продолжать функционировать корректно в условиях непредвиденных ситуаций, таких как сбои оборудования, ошибки пользователей или внешние воздействия. Устойчивые системы могут адаптироваться к изменениям и сохранять свою функциональность.

Время безотказной работы (Mean Time Between Failures, MTBF): MTBF — это среднее время, в течение которого система работает без сбоев. Этот показатель используется для оценки надежности системы. Чем выше значение MTBF, тем более надежной считается система.

Время восстановления (Mean Time To Repair, MTTR): MTTR — это среднее время, необходимое для восстановления системы после сбоя. Этот показатель важен для оценки доступности системы, так как он показывает, насколько быстро система может быть восстановлена после возникновения проблемы.

Сбой (Failure): Сбой — это событие, при котором система перестает выполнять свои функции или работает некорректно. Сбои могут быть вызваны различными факторами, включая аппаратные и программные ошибки, человеческий фактор и внешние воздействия.

Резервирование (Redundancy): Резервирование — это метод повышения надежности системы путем добавления избыточных компонентов или функций. Например, использование резервных серверов или дублирование данных может помочь обеспечить непрерывность работы системы в случае сбоя основного компонента.

Тестирование надежности: Тестирование надежности — это процесс оценки надежности системы с помощью различных методов, таких как стресс-тестирование, тестирование на отказ и другие. Эти методы помогают выявить слабые места в системе и оценить ее способность справляться с нагрузками.

Управление рисками: Управление рисками включает в себя идентификацию, оценку и минимизацию рисков, связанных с надежностью системы. Это может включать в себя разработку стратегий для предотвращения сбоев, а также планы на случай возникновения инцидентов.

Качество обслуживания (Quality of Service, QoS): QoS — это набор характеристик, которые определяют уровень обслуживания, предоставляемого системой. Надежность является одной из ключевых составляющих QoS, так как она влияет на удовлетворенность пользователей и общую эффективность системы.

1. **Метрики качества информационных систем**
2. **Функциональные метрики**
3. **Метрики надежности**
4. **3. Метрики производительности**
5. **4. Метрики удобства использования**
6. **5. Метрики безопасности**
7. **Показатели надежности в соответствии со стандартами. Обеспечение надежности**

Показатели надежности

Среднее время безотказной работы (MTBF - Mean Time Between Failures):

Определяет среднее время, в течение которого система работает без сбоев. MTBF является важным показателем надежности, так как показывает, как долго система может функционировать до возникновения следующего сбоя.

Формула: [ MTBF = \frac{\text{Общее время работы}}{\text{Количество сбоев}} ]

Среднее время восстановления (MTTR - Mean Time To Repair):

Определяет среднее время, необходимое для восстановления системы после сбоя. MTTR показывает, насколько быстро система может быть восстановлена после инцидента.

Формула: [ MTTR = \frac{\text{Общее время на восстановление}}{\text{Количество сбоев}} ]

Доступность (Availability):

Определяет, насколько система доступна для пользователей в любой момент времени. Доступность часто выражается в процентах и рассчитывается как отношение времени работы к общему времени (включая время простоя).

Формула: [ \text{Доступность} = \frac{MTBF}{MTBF + MTTR} \times 100% ]

Частота сбоев (Failure Rate):

Определяет количество сбоев, происходящих за единицу времени. Частота сбоев может быть использована для оценки надежности системы.

Формула: [ \text{Частота сбоев} = \frac{\text{Количество сбоев}}{\text{Общее время работы}} ]

Вероятность безотказной работы (Reliability):

Определяет вероятность того, что система будет функционировать без сбоев в течение определенного времени. Эта метрика может быть выражена в виде функции надежности.

Формула: [ R(t) = e^{-\lambda t} ] где ( \lambda ) — это коэффициент отказов, а ( t ) — время.

1. **Качество и надежность программных средств**

Качество программных средств

Качество программного обеспечения можно определить как степень соответствия ПО установленным требованиям и ожиданиям пользователей. Качество включает в себя несколько аспектов:

Функциональность:

Способность ПО выполнять заданные функции и задачи. Это включает в себя полноту, корректность и совместимость функциональности.

Надежность:

Способность ПО выполнять свои функции в заданных условиях и в течение определенного времени без сбоев. Надежность включает в себя такие показатели, как MTBF, MTTR и доступность.

Удобство использования:

Насколько легко и удобно пользователям взаимодействовать с ПО. Это включает в себя интуитивность интерфейса, время на обучение и удовлетворенность пользователей.

Производительность:

Эффективность работы ПО, включая время отклика, пропускную способность и использование ресурсов.

Поддерживаемость:

Насколько легко ПО можно модифицировать, исправлять ошибки и обновлять. Это включает в себя документацию, структуру кода и тестирование.

Переносимость:

Способность ПО работать в различных средах и на различных платформах. Это включает в себя адаптацию к новым операционным системам и аппаратным средствам.

Надежность программных средств

Надежность программного обеспечения — это его способность выполнять заданные функции в течение определенного времени без сбоев. Надежность является критически важной для систем, где сбои могут привести к серьезным последствиям. Основные аспекты надежности включают:

Отказоустойчивость:

Способность системы продолжать функционировать в случае возникновения ошибок или сбоев. Это может быть достигнуто через резервирование, обработку ошибок и другие методы.

Время безотказной работы (MTBF):

Среднее время, в течение которого система работает без сбоев. Высокий MTBF указывает на высокую надежность.

Время восстановления (MTTR):

Среднее время, необходимое для восстановления системы после сбоя. Низкий MTTR указывает на эффективные процессы восстановления.

Тестирование на надежность:

Процесс оценки надежности ПО с помощью различных методов, таких как стресс-тестирование, тестирование на отказ и другие.

1. **Методы обеспечения и контроля качества информационных систем**

Методы обеспечения качества

Стандартизация процессов:

Использование стандартов, таких как ISO 9001, CMMI (Capability Maturity Model Integration) и других, помогает установить четкие процессы и процедуры, что способствует повышению качества разработки и управления проектами.

Анализ требований:

Тщательный анализ и документирование требований пользователей и бизнес-процессов на ранних этапах разработки помогают избежать недоразумений и ошибок в дальнейшем. Использование техник, таких как интервью, опросы и прототипирование, может помочь в этом процессе.

Проектирование и архитектура:

Правильное проектирование архитектуры системы и ее компонентов на ранних этапах разработки позволяет избежать многих проблем в будущем. Использование шаблонов проектирования и архитектурных стилей (например, MVC, SOA) может повысить качество системы.

Кодирование и ревью кода:

Следование стандартам кодирования и проведение ревью кода помогают выявить ошибки и улучшить качество кода. Использование инструментов статического анализа кода также может помочь в этом.

Тестирование:

Разработка и выполнение различных видов тестов (юнит-тесты, интеграционные тесты, системные тесты, тесты на приемку) на всех этапах разработки помогает выявить и устранить ошибки. Автоматизация тестирования может повысить эффективность и скорость тестирования.

Управление изменениями:

Эффективное управление изменениями в проекте, включая контроль версий и документацию, помогает предотвратить возникновение новых проблем и поддерживать высокое качество.

Обучение и развитие команды:

Обучение сотрудников и повышение их квалификации способствуют улучшению навыков и знаний, что, в свою очередь, повышает качество разработки.

Методы контроля качества

Аудиты и проверки:

Проведение регулярных аудитов и проверок процессов разработки и тестирования помогает выявить несоответствия и области для улучшения. Это может включать как внутренние, так и внешние аудиты.

Метрики и показатели качества:

Использование метрик, таких как количество дефектов, время на исправление ошибок, покрытие тестами и другие, позволяет количественно оценивать качество системы и выявлять проблемы.

Обратная связь от пользователей:

Сбор и анализ обратной связи от пользователей после внедрения системы помогает выявить проблемы и области для улучшения. Это может включать опросы, интервью и анализ пользовательского опыта.

Мониторинг и анализ производительности:

Постоянный мониторинг производительности системы в реальном времени позволяет выявлять проблемы и узкие места, которые могут повлиять на качество работы системы.

Тестирование на этапе эксплуатации:

Проведение тестирования в условиях реальной эксплуатации (например, A/B тестирование, нагрузочное тестирование) помогает оценить качество системы и ее соответствие требованиям пользователей.

Управление рисками:

Идентификация и оценка рисков, связанных с качеством, позволяет заранее разработать стратегии их минимизации и управления.

1. **Достоверность информационных систем**

Основные аспекты достоверности

Точность данных:

Данные должны быть корректными и соответствовать реальности. Это включает в себя правильность ввода данных, а также их обработку и хранение.

Актуальность данных:

Данные должны быть обновлены и соответствовать текущему состоянию дел. Устаревшая информация может привести к ошибочным выводам и решениям.

Полнота данных:

Данные должны быть полными и содержать всю необходимую информацию для выполнения задач. Неполные данные могут привести к искажению анализа и принятию неверных решений.

Неподверженность изменениям:

Достоверность данных также зависит от их защиты от несанкционированных изменений. Это включает в себя контроль доступа, а также механизмы аудита и отслеживания изменений.

Источники данных:

Достоверность информации зависит от надежности источников данных. Использование проверенных и авторитетных источников данных повышает уровень достоверности.

1. **Эффективность информационных систем**

Эффективность информационных систем (ИС) — это характеристика, отражающая способность системы достигать поставленных целей и задач с минимальными затратами ресурсов, времени и усилий. Эффективность ИС является важным аспектом, который влияет на производительность организации, качество принимаемых решений и удовлетворенность пользователей. Рассмотрим основные аспекты, связанные с эффективностью информационных систем.

Основные аспекты эффективности информационных систем

Производительность:

Производительность ИС определяется скоростью обработки данных, временем отклика системы и количеством выполняемых операций за единицу времени. Высокая производительность позволяет пользователям быстрее получать необходимую информацию и выполнять задачи.

Экономичность:

Эффективность ИС также включает в себя соотношение затрат на разработку, внедрение и эксплуатацию системы к получаемым результатам. Экономичные системы обеспечивают максимальную отдачу от инвестиций.

Удобство использования:

Удобство интерфейса и простота взаимодействия с системой влияют на эффективность работы пользователей. Интуитивно понятные интерфейсы и доступность необходимых функций способствуют повышению производительности.

Гибкость и адаптивность:

Эффективные ИС способны адаптироваться к изменяющимся требованиям бизнеса и быстро реагировать на изменения внешней среды. Это может включать возможность интеграции с другими системами и масштабируемость.

Качество данных:

Эффективность ИС зависит от качества обрабатываемых данных. Достоверные, актуальные и полные данные способствуют более точному анализу и принятию решений.

Поддержка бизнес-процессов:

ИС должны эффективно поддерживать ключевые бизнес-процессы организации, обеспечивая автоматизацию, оптимизацию и улучшение этих процессов.

1. **Безопасность информационных систем**

Основные аспекты безопасности информационных систем

Конфиденциальность:

Защита информации от несанкционированного доступа. Это включает в себя использование шифрования, контроля доступа и аутентификации пользователей.

Целостность:

Обеспечение точности и полноты данных. Меры по поддержанию целостности включают в себя механизмы проверки данных, резервное копирование и контроль версий.

Доступность:

Гарантия того, что информация и ресурсы доступны для авторизованных пользователей в нужное время. Это может включать в себя защиту от атак, таких как DDoS, а также обеспечение надежности систем и резервирования.

Аутентификация:

Процесс проверки подлинности пользователей и устройств, которые пытаются получить доступ к системе. Это может включать в себя пароли, биометрические данные и многофакторную аутентификацию.

Авторизация:

Определение прав доступа пользователей к различным ресурсам и данным в системе. Это позволяет ограничить доступ к конфиденциальной информации только для тех, кто имеет на это право.

Управление рисками:

Идентификация, оценка и управление рисками, связанными с безопасностью информации. Это включает в себя анализ угроз и уязвимостей, а также разработку стратегий по их минимизации.

1. **Виды угроз информационной безопасности**

Вредоносное ПО:

Вирусы, черви, трояны и другие виды вредоносного программного обеспечения могут нанести ущерб системам и данным.

Атаки на сеть:

Атаки, такие как DDoS (распределенный отказ в обслуживании), могут привести к недоступности систем и сервисов.

Несанкционированный доступ:

Попытки злоумышленников получить доступ к системам и данным без разрешения.

Утечка данных:

Утечка конфиденциальной информации может произойти как в результате атак, так и из-за человеческих ошибок.

Социальная инженерия:

Методы манипуляции людьми для получения конфиденциальной информации, такие как фишинг и предлог.

1. **Построения системы информационной безопасности**

Этапы построения системы информационной безопасности

Анализ и оценка рисков:

Идентификация активов: Определение всех информационных активов, включая данные, программное обеспечение, оборудование и сети.

Оценка угроз и уязвимостей: Анализ потенциальных угроз (вредоносное ПО, атаки, ошибки пользователей) и уязвимостей (недостатки в программном обеспечении, недостаточная защита).

Оценка рисков: Определение вероятности возникновения угроз и их потенциального воздействия на организацию.

Разработка политики безопасности:

Определение целей и задач: Установление целей безопасности, таких как защита конфиденциальности данных и обеспечение доступности систем.

Создание политики безопасности: Документ, описывающий правила и процедуры, касающиеся безопасности информации, включая управление доступом, использование паролей, обработку данных и реагирование на инциденты.

Проектирование архитектуры безопасности:

Выбор технологий и инструментов: Определение необходимых технологий для защиты информации, таких как шифрование, файрволы, системы обнаружения вторжений (IDS) и антивирусное ПО.

Разработка архитектуры: Создание схемы, описывающей, как различные компоненты безопасности будут взаимодействовать друг с другом.

Внедрение мер безопасности:

Настройка систем и инструментов: Установка и конфигурация программного обеспечения и оборудования для обеспечения безопасности.

Обучение сотрудников: Проведение тренингов для сотрудников по вопросам безопасности, чтобы повысить их осведомленность о рисках и методах защиты.

Мониторинг и аудит:

Постоянный мониторинг: Использование систем мониторинга для отслеживания активности в сети и выявления подозрительных действий.

Аудит безопасности: Регулярные проверки и оценки системы безопасности для выявления уязвимостей и несоответствий.

Реагирование на инциденты:

Разработка плана реагирования: Создание плана действий на случай инцидентов безопасности, включая процедуры уведомления, расследования и восстановления.

Тестирование плана: Проведение учений и тестов для проверки готовности к реагированию на инциденты.

Обновление и улучшение:

Регулярный пересмотр политики и мер безопасности: Обновление политики безопасности и мер защиты в соответствии с изменениями в бизнесе, технологиях и угрозах.

Анализ инцидентов: Изучение произошедших инцидентов для выявления причин и предотвращения их повторения.

1. **Основы законодательства в области обеспечения информационной безопасности**

Россия

Федеральный закон от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации":

Устанавливает правовые основы для обеспечения информационной безопасности, защиты информации и прав граждан в этой области.

Федеральный закон от 6 апреля 2011 года № 63-ФЗ "Об электронной подписи":

Регулирует использование электронной подписи, которая является важным инструментом для обеспечения безопасности электронных документов.

Федеральный закон от 28 декабря 2013 года № 390-ФЗ "О безопасности":

Определяет основные принципы государственной политики в области безопасности, включая информационную безопасность.

Федеральный закон от 27 декабря 2018 года № 533-ФЗ "О внесении изменений в отдельные законодательные акты Российской Федерации":

Устанавливает требования к защите персональных данных и информации, обрабатываемой в информационных системах.

1. **Защита информации в информационных системах и компьютерных сетях**

Основные аспекты защиты информации

Конфиденциальность:

Защита информации от несанкционированного доступа. Это включает в себя использование шифрования, контроля доступа и аутентификации пользователей.

Целостность:

Обеспечение точности и полноты данных. Меры по поддержанию целостности включают в себя механизмы проверки данных, резервное копирование и контроль версий.

Доступность:

Гарантия того, что информация и ресурсы доступны для авторизованных пользователей в нужное время. Это может включать в себя защиту от атак, таких как DDoS, а также обеспечение надежности систем и резервирования.

1. **Обеспечение безопасности**

1. Физическая безопасность

Физическая безопасность направлена на защиту объектов, людей и информации от физических угроз, таких как кража, вандализм, террористические акты и природные катастрофы. Основные меры включают:

Контроль доступа: Использование систем контроля доступа (карты, биометрия) для ограничения доступа к защищаемым объектам.

Системы видеонаблюдения: Установка камер для мониторинга и записи событий на территории.

Охрана: Привлечение охранных служб для патрулирования и защиты объектов.

Защита от стихийных бедствий: Разработка планов эвакуации и защиты от природных катастроф (пожары, наводнения и т.д.).

2. Информационная безопасность

Информационная безопасность направлена на защиту данных и информационных систем от несанкционированного доступа, утечек, повреждений и других угроз. Основные меры включают:

Шифрование данных: Защита информации с помощью криптографических методов.

Аутентификация и авторизация: Использование паролей, двухфакторной аутентификации и других методов для подтверждения личности пользователей и ограничения их прав доступа.

Мониторинг и аудит: Постоянный мониторинг систем на предмет подозрительной активности и проведение регулярных аудитов безопасности.

Обучение сотрудников: Повышение осведомленности сотрудников о рисках и методах защиты информации.

1. **Вертикальная интеграция. Интеграция «многие ко многим» (звезда, спагетти)**

Вертикальная интеграция — это стратегия, при которой компания расширяет свои операции на несколько уровней цепочки поставок. Это может включать в себя как интеграцию вверх (поглощение поставщиков), так и интеграцию вниз (поглощение дистрибьюторов или розничных продавцов). Основные цели вертикальной интеграции:

Интеграция «многие ко многим» — это подход, при котором несколько участников могут взаимодействовать друг с другом в различных комбинациях. Это может быть реализовано через различные модели, такие как «звезда» и «спагетти».

В модели «звезда» все участники (например, компании, системы или пользователи) подключены к центральному узлу или серверу. Этот узел управляет взаимодействиями и обменом данными между участниками.

Модель «спагетти» характеризуется более сложной и запутанной сетью взаимодействий между участниками. В этой модели нет четкой структуры, и участники могут взаимодействовать друг с другом напрямую, без центрального узла.

1. **Интеграция платформ. Интеграция данных. Интеграция приложений**

Интеграция платформ — это процесс объединения различных технологических платформ и систем, чтобы они могли работать вместе как единое целое. Это может включать в себя интеграцию облачных платформ, локальных систем, мобильных приложений и других технологий.

Интеграция данных — это процесс объединения данных из различных источников и систем, чтобы создать единое представление информации. Это может включать в себя извлечение, трансформацию и загрузку (ETL) данных, а также их синхронизацию и консолидацию.

Интеграция приложений — это процесс объединения различных программных приложений, чтобы они могли взаимодействовать друг с другом и обмениваться данными. Это может включать в себя как интеграцию на уровне пользовательского интерфейса, так и на уровне бэкенда.

1. **Классы продуктов для интеграции систем: реализующие идеологию SOA, реализующие идеологию Messaging (промежуточное ПО), корпоративные шины сервисов**

Service-Oriented Architecture (SOA) — это архитектурный стиль, который позволяет создавать системы, состоящие из независимых сервисов, которые могут взаимодействовать друг с другом через стандартизированные интерфейсы.

Messaging — это подход к интеграции, основанный на обмене сообщениями между различными системами и приложениями. Промежуточное ПО (middleware) обеспечивает надежную и асинхронную передачу сообщений, что позволяет системам взаимодействовать друг с другом без необходимости прямого соединения.

Корпоративная шина сервисов (Enterprise Service Bus, ESB) — это архитектурный паттерн, который обеспечивает интеграцию различных приложений и сервисов в рамках организации. ESB служит центральной точкой для маршрутизации, трансформации и управления сообщениями между сервисами.

1. **Жизненный цикл проекта по созданию информационной системы**
2. Инициация проекта
3. Планирование
4. Проектирование
5. Разработка
6. Внедрение
7. Эксплуатация и поддержка
8. Завершение проекта
9. **Модели жизненного цикла проекта информационной системы**

Водопадная модель — это линейная и последовательная модель, где каждый этап должен быть завершен перед переходом к следующему. Этапы включают: анализ требований, проектирование, разработка, тестирование, внедрение и поддержку.

Итеративная модель предполагает повторение циклов разработки, где каждый цикл включает в себя все этапы жизненного цикла. На каждом итеративном цикле система постепенно улучшается и дорабатывается.

Спиральная модель сочетает в себе элементы итеративной и водопадной моделей. Проект проходит через несколько итераций (спиралей), каждая из которых включает в себя этапы планирования, анализа рисков, разработки и тестирования.

1. **Критерии показателя качества**
2. Функциональное качество
3. Нефункциональное качество
4. Удобство использования
5. Поддерживаемость
6. Совместимость
7. Экономические показатели
8. **Стандарты оценки качества информационных систем**

1. ISO/IEC 25010

Описание: Стандарт ISO/IEC 25010 определяет модель качества программного обеспечения и включает в себя восемь характеристик качества, которые делятся на две категории: функциональные и нефункциональные.

Функциональные характеристики:

Соответствие требованиям

Полнота

Корректность

Удобство использования

Нефункциональные характеристики:

Производительность

Надежность

Безопасность

Поддерживаемость

Совместимость

1. **Показатели экономической эффективности системы. Показатели прагматической эффективности**

**Общая стоимость владения (TCO):**

**Срок окупаемости (Payback Period)**:

**Внутренняя норма доходности (IRR)**:

**Показатели прагматической эффективности**

**Прагматическая эффективность фокусируется на практической полезности системы и ее влиянии на бизнес-процессы. Основные показатели включают:**

**Увеличение производительности:**

**Описание: Измеряет, насколько система улучшает производительность сотрудников или процессов. Это может быть выражено в увеличении объема выполненной работы или сокращении времени на выполнение задач.**

**Снижение затрат:**

**Описание: Оценка экономии, достигнутой за счет автоматизации процессов, уменьшения ошибок и повышения эффективности работы.**

**Улучшение качества:**

**Описание: Измеряет, насколько система способствует повышению качества продукции или услуг. Это может включать снижение количества дефектов, улучшение удовлетворенности клиентов и т.д.**

**Скорость принятия решений:**

**Описание: Оценка того, как система влияет на скорость и качество принятия решений в организации. Это может быть связано с доступом к актуальной информации и аналитическим инструментам.**

**Уровень удовлетворенности пользователей:**

**Описание: Оценка удовлетворенности конечных пользователей системой. Это может быть измерено через опросы, отзывы и другие методы.**

**Гибкость и адаптивность:**

**Описание: Способность системы адаптироваться к изменениям в бизнес-процессах и требованиям пользователей. Это может включать возможность интеграции с другими системами и легкость в обновлении.**

1. **Экономическая и информационная безопасность. Составляющие информационной безопасности**

Экономическая безопасность организации включает в себя защиту ее финансовых интересов, активов и ресурсов от различных угроз, таких как мошенничество, экономические кризисы, конкуренция и другие риски.

Информационная безопасность (ИБ) — это защита информации и информационных систем от несанкционированного доступа, использования, раскрытия, разрушения или изменения.

Составляющие информационной безопасности

Информационная безопасность состоит из нескольких ключевых компонентов:

Конфиденциальность:

Защита информации от несанкционированного доступа. Это включает в себя использование шифрования, контроля доступа и других методов для обеспечения того, чтобы только авторизованные пользователи могли получить доступ к чувствительной информации.

Целостность:

Обеспечение точности и полноты данных. Это включает в себя защиту от несанкционированного изменения данных, а также использование механизмов проверки целостности, таких как контрольные суммы и хеширование.

Доступность:

Гарантия того, что информация и системы доступны для авторизованных пользователей, когда это необходимо. Это включает в себя защиту от атак, таких как DDoS, а также обеспечение резервного копирования и восстановления данных.

Аутентификация:

Процесс проверки идентичности пользователей и систем. Это может включать в себя использование паролей, биометрических данных, токенов и других методов.

Авторизация:

Определение прав доступа пользователей к различным ресурсам и данным. Это включает в себя управление ролями и правами доступа.

Управление рисками:

Идентификация, оценка и минимизация рисков, связанных с информационными активами. Это включает в себя регулярные аудиты безопасности и анализ уязвимостей.

Обучение и осведомленность:

Обучение сотрудников основам информационной безопасности и повышению их осведомленности о возможных угрозах и методах защиты.

Инцидент-менеджмент:

Процессы, связанные с обнаружением, реагированием и восстановлением после инцидентов безопасности. Это включает в себя разработку планов реагирования на инциденты и проведение учений.

Соответствие и аудит:

Обеспечение соблюдения стандартов и нормативных требований в области информационной безопасности. Это включает в себя регулярные проверки и аудит систем безопасности.

1. **Классификация автоматизированных информационных систем реального времени**

Системы обработки данных: Обрабатывают и храня ят данные в реальном времени, обеспечивая быструю реакцию на события.

Системы управления: Используются для управления технологическими процессами, например, в промышленности, где требуется синхронизация действий и контроль за состоянием оборудования.

Системы мониторинга: Предназначены для наблюдения за состоянием объектов и процессов, например, в системах безопасности или здравоохранения.

Системы поддержки принятия решений: Помогают пользователям принимать решения на основе анализа данных в реальном времени, часто применяются в бизнесе и финансах.

1. **Особенности сопровождения информационных систем управления «Умный дом»**

1. Многоуровневая архитектура

Системы «Умный дом» часто имеют многоуровневую архитектуру, включающую:

Устройства и датчики: Различные устройства (освещение, термостаты, камеры, замки и т.д.) и датчики (движения, температуры, влажности и т.д.) должны быть правильно интегрированы и настроены.

Контроллеры: Центральные контроллеры или хабы, которые управляют взаимодействием между устройствами и обеспечивают связь с пользователем.

Пользовательский интерфейс: Мобильные приложения или веб-интерфейсы, через которые пользователи могут управлять системой.

2. Обновления и поддержка

Регулярные обновления: Необходимость в регулярных обновлениях программного обеспечения для обеспечения безопасности и добавления новых функций. Это может включать обновления прошивки для устройств и обновления приложений.

Совместимость: Обеспечение совместимости новых устройств с уже установленными компонентами системы. Это может потребовать тестирования и настройки.

3. Безопасность

Защита данных: Системы «Умный дом» обрабатывают личные данные пользователей, поэтому важно обеспечить защиту информации от несанкционированного доступа и утечек.

Шифрование: Использование шифрования для передачи данных между устройствами и контроллерами, а также для хранения данных.

4. Пользовательская поддержка

Обучение пользователей: Обучение пользователей правильному использованию системы, включая настройку сценариев и автоматизаций.

Техническая поддержка: Обеспечение доступной технической поддержки для решения проблем, возникающих у пользователей.

5. Интеграция с другими системами

Интеграция с IoT: Системы «Умный дом» часто интегрируются с другими IoT-устройствами и сервисами, такими как голосовые помощники (например, Amazon Alexa, Google Assistant).

Совместимость с протоколами: Поддержка различных протоколов связи (Zigbee, Z-Wave, Wi-Fi, Bluetooth и т.д.) для обеспечения взаимодействия между устройствами.

6. Мониторинг и диагностика

Мониторинг состояния: Постоянный мониторинг состояния устройств и системы в целом для выявления и устранения проблем.

Диагностика: Использование инструментов для диагностики и устранения неполадок, что может включать удаленный доступ для технической поддержки.

7. Адаптация к изменениям

Изменения в потребностях пользователей: Системы должны быть гибкими и адаптироваться к изменяющимся потребностям пользователей, включая добавление новых устройств и функций.

Тренды и технологии: Учет новых технологий и трендов в области домашней автоматизации, таких как искусственный интеллект и машинное обучение, для улучшения функциональности системы.

Заключение

1. **Режимы и уровни интеграции**

Интеграция на уровне данных:

Обмен данными между системами осуществляется через общие форматы или базы данных. Это может включать использование ETL-процессов (Extract, Transform, Load) для извлечения данных из одной системы, их преобразования и загрузки в другую.

Интеграция на уровне приложений:

Приложения взаимодействуют друг с другом через API (Application Programming Interface) или другие интерфейсы. Это позволяет системам обмениваться данными и вызывать функции друг друга.

Интеграция на уровне процессов:

Системы интегрируются на уровне бизнес-процессов, что позволяет автоматизировать и оптимизировать рабочие процессы. Это может включать использование BPM (Business Process Management) систем для управления и координации процессов между различными системами.

Интеграция на уровне пользовательского интерфейса:

Объединение различных интерфейсов в единый пользовательский интерфейс, что позволяет пользователям взаимодействовать с несколькими системами через одну точку доступа.

Уровни интеграции

Технический уровень:

На этом уровне осуществляется интеграция на уровне сетевой инфраструктуры и протоколов. Это включает в себя использование стандартов и технологий, таких как TCP/IP, HTTP, SOAP, REST и других.

Информационный уровень:

Интеграция данных и информации между системами. Это может включать использование общих форматов данных (например, XML, JSON) и стандартов обмена данными.

Функциональный уровень:

Интеграция функциональности различных систем. Это может включать использование API для вызова функций одной системы из другой, а также создание интеграционных решений, которые объединяют функциональность нескольких систем.

Организационный уровень:

Интеграция бизнес-процессов и организационных структур. Это включает в себя координацию действий различных подразделений и систем для достижения общих бизнес-целей.

Стратегический уровень:

Интеграция на уровне стратегического управления и планирования. Это включает в себя использование интегрированных систем для поддержки принятия решений и стратегического планирования на уровне всей организации.

**Типовые практические задания**

1. **Разработка технического задания на сопровождение информационной системы**

Техническое задание на сопровождение информационной системы

1. Введение

1.1. Наименование проекта: Сопровождение информационной системы [Название системы].

1.2. Заказчик: [Наименование организации].

1.3. Исполнитель: [Наименование исполнителя или команды].

1.4. Дата составления: [Дата].

1.5. Цель документа: Определение требований и условий сопровождения информационной системы.

2. Описание информационной системы

2.1. Общее описание: Краткое описание функциональности и назначения информационной системы.

2.2. Архитектура системы: Описание архитектуры системы, включая используемые технологии, базы данных, интерфейсы и интеграции.

2.3. Пользователи системы: Определение категорий пользователей и их ролей в системе.

3. Цели и задачи сопровождения

3.1. Цели сопровождения:

Обеспечение бесперебойной работы системы.

Поддержка пользователей.

Обновление и модернизация системы.

3.2. Задачи сопровождения:

Мониторинг состояния системы.

Проведение регулярных обновлений программного обеспечения.

Обеспечение безопасности данных.

Обучение пользователей.

Техническая поддержка и устранение неполадок.

4. Требования к сопровождению

4.1. Технические требования:

Описание необходимых ресурсов (серверы, сети, программное обеспечение).

Требования к безопасности (шифрование, аутентификация).

4.2. Функциональные требования:

Описание функций, которые должны быть доступны пользователям.

Условия для интеграции с другими системами.

4.3. Нефункциональные требования:

Производительность системы (время отклика, количество пользователей).

Уровень доступности (например, 99.9% времени работы).

5. Организация работы

5.1. Состав команды сопровождения: Определение ролей и обязанностей членов команды.

5.2. Процессы сопровождения:

Описание процессов мониторинга, обновления и поддержки.

Регламент работы с инцидентами и запросами пользователей.

5.3. Планирование и отчетность:

Частота отчетов о состоянии системы.

Форматы отчетов и их содержание.

6. Сроки и этапы выполнения

6.1. Этапы сопровождения:

Начальный этап: анализ текущего состояния системы.

Этап регулярного сопровождения: мониторинг, обновления, поддержка.

Этап оценки и улучшения: анализ эффективности работы системы.

6.2. Сроки выполнения: Указать сроки для каждого этапа.

7. Бюджет

7.1. Оценка затрат: Описание предполагаемых затрат на сопровождение системы (зарплаты, оборудование, лицензии и т.д.).

8. Заключение

8.1. Подписи сторон: Место для подписей заказчика и исполнителя.

Примечания

Техническое задание должно быть согласовано с заинтересованными сторонами и может быть изменено в процессе работы в зависимости от новых требований или условий.

Важно учитывать специфику конкретной информационной системы и потребности организации при разработке ТЗ.