1. Безопасность функционирования информационной системы, отказ и сбой, эффективность использования ресурсов

- **Безопасность функционирования** информационной системы (ИС) включает обеспечение конфиденциальности, целостности и доступности данных. Это достигается за счет внедрения мер защиты, таких как шифрование, аутентификация, резервирование и мониторинг.
- **Отказ** — это полная потеря работоспособности системы или её компонентов, что может привести к остановке критических процессов. **Сбой** — это временное нарушение работы системы, которое может быть устранено без полной остановки.
- **Эффективность использования ресурсов** подразумевает оптимизацию использования вычислительных мощностей, памяти, сетевых ресурсов и других компонентов для минимизации затрат и повышения производительности.

2. Система управления ресурсами и взаимоотношениями предприятия, как система с предсказуемым поведением

- Система управления ресурсами и взаимоотношениями предприятия (например, ERP-система) должна быть спроектирована так, чтобы её поведение было предсказуемым. Это достигается за счет:
    - Четко определенных бизнес-процессов.
    - Использования стандартизированных протоколов и интерфейсов.
    - Регулярного тестирования и анализа производительности.
    - Внедрения механизмов автоматического восстановления после сбоев.
- Предсказуемость системы позволяет минимизировать риски и обеспечивать стабильность работы предприятия.

3. Система управления ресурсами и взаимоотношениями предприятия

- Это комплексная система, которая интегрирует управление ключевыми ресурсами предприятия (финансы, персонал, оборудование) и взаимоотношениями с клиентами, поставщиками и партнерами.
- Основные функции:
    - Управление финансами и учет.

    - Управление цепочками поставок.
    - Управление персоналом.
    - Управление взаимоотношениями с клиентами (CRM).
- Такие системы повышают эффективность бизнеса за счет автоматизации процессов и централизации данных.

4. Безопасность функционирования систем и организация резервирования данных

- **Безопасность функционирования** систем включает защиту от внешних угроз (кибератаки) и внутренних рисков (ошибки персонала, сбои оборудования).
- **Организация резервирования данных** — это создание резервных копий критически важной информации для восстановления в случае потери или повреждения данных. Это может включать:
    - Регулярное резервное копирование.
    - Использование RAID-массивов.
    - Развертывание geographically distributed storage (географически распределенных хранилищ).

5. Критический сегмент и безопасность функционирования систем управления ресурсами и взаимоотношениями предприятия

- **Критический сегмент** — это часть системы, отказ которой может привести к остановке ключевых бизнес-процессов. Например, модуль финансового учета в ERP-системе.
- **Безопасность функционирования** таких сегментов обеспечивается за счет:
    - Избыточности (дублирование компонентов).
    - Регулярного мониторинга и тестирования.
    - Защиты от несанкционированного доступа.

6. Зависимость безопасности функционирования системы управления ресурсами и взаимоотношениями предприятия от сетевого окружения

- Сетевое окружение (инфраструктура, протоколы, устройства) напрямую влияет на безопасность системы. Угрозы включают:

    - Атаки на сетевые узлы (DDoS, MITM).
    - Уязвимости в сетевых протоколах.
    - Несанкционированный доступ через слабые точки сети.
- Меры защиты:
    - Использование VPN и шифрования.
    - Внедрение межсетевых экранов (firewalls).
    - Регулярный аудит сетевой безопасности.

7. Зависимость безопасности функционирования системы управления ресурсами и взаимоотношениями предприятия от служебного трафика

- **Служебный трафик** — это данные, передаваемые между компонентами системы (например, между серверами и клиентами).
- Угрозы:
    - Перехват данных.
    - Подмена данных (spoofing).
    - Перегрузка сети (например, из-за атак).
- Меры защиты:
    - Шифрование служебного трафика.
    - Использование защищенных протоколов (HTTPS, TLS).
    - Мониторинг трафика на аномалии.

8. Безопасность функционирования и функциональная безопасность систем управления ресурсами и взаимоотношениями предприятия

- **Безопасность функционирования** — это защита системы от внешних и внутренних угроз.
- **Функциональная безопасность** — это способность системы корректно выполнять свои функции даже в условиях сбоев или ошибок.
- Оба аспекта важны для обеспечения стабильной работы предприятия. Например, ERP-система должна быть защищена от кибератак (безопасность

функционирования) и иметь механизмы восстановления после сбоев (функциональная безопасность).

9. Безопасность функционирования выделенных сетей хранения данных (СХД)

- **Сети хранения данных (СХД)** — это специализированные сети для хранения и управления большими объемами данных.
- Угрозы:
    - Несанкционированный доступ к данным.
    - Потеря данных из-за сбоев оборудования.
    - Атаки на сетевую инфраструктуру.
- Меры защиты:
    - Использование RAID и резервного копирования.
    - Шифрование данных при передаче и хранении.
    - Регулярный аудит и мониторинг.

10. Безопасность функционирования системы управления ресурсами и взаимоотношениями предприятия при работе отказоустойчивого кластера

- **Отказоустойчивый кластер** — это группа серверов, которые работают вместе для обеспечения высокой доступности системы. Если один сервер выходит из строя, его функции автоматически переходят к другому.
- **Безопасность функционирования** в таких условиях включает:
    - Защиту данных, хранящихся в кластере.
    - Обеспечение целостности данных при переключении между серверами.
    - Защиту от атак на кластерную инфраструктуру.
- Преимущества:
    - Минимизация downtime (времени простоя).
    - Повышение надежности системы.

11. Безопасность функционирования при применении кластеров высокой надежности в компьютерной системе

- **Кластеры высокой надежности** обеспечивают отказоустойчивость за счет дублирования компонентов и автоматического переключения между узлами в случае сбоя.
- **Меры безопасности**:
    - Защита данных в кластере: шифрование данных при передаче и хранении.
    - Контроль доступа: аутентификация и авторизация для предотвращения несанкционированного доступа.
    - Мониторинг и аудит: отслеживание состояния кластера и выявление аномалий.
    - Резервирование: создание резервных копий данных для восстановления в случае сбоя.

12. Безопасность функционирования в системной и программной инженерии

- **Системная инженерия**:
    - Обеспечение безопасности на этапе проектирования системы (security by design).
    - Анализ рисков и угроз на всех этапах жизненного цикла системы.
- **Программная инженерия**:
    - Использование безопасных методов разработки (например, OWASP для веб-приложений).
    - Тестирование на уязвимости (статический и динамический анализ кода).
    - Внедрение механизмов защиты от атак (например, инъекций, XSS).

13. Непрерывность функционирования систем управления ресурсами и взаимоотношениями предприятия (как требования интероперабельности предприятия)

- **Непрерывность функционирования** обеспечивается за счет:
    - Резервирования критических компонентов.
    - Планирования аварийного восстановления (Disaster Recovery Plan, DRP).

    - Регулярного тестирования отказоустойчивости.

- **Интероперабельность** — это способность системы взаимодействовать с другими системами и обмениваться данными. Требования к интероперабельности включают:
    - Использование стандартизированных протоколов (например, SOAP, REST).
    - Обеспечение совместимости форматов данных (например, XML, JSON).
    - Поддержка открытых API для интеграции с внешними системами.

14. Безопасность функционирования систем управления ресурсами и взаимоотношениями предприятия и информационная безопасность

- **Безопасность функционирования** — это обеспечение стабильной работы системы без сбоев и отказов.
- **Информационная безопасность** — это защита данных от несанкционированного доступа, утечек и повреждений.
- Взаимосвязь:
    - Безопасность функционирования зависит от информационной безопасности (например, атака на систему может привести к её отказу).
    - Информационная безопасность обеспечивается за счет мер, таких как шифрование, контроль доступа и резервирование данных.

15. Расчет затрат на производительность и функционирование системы управления ресурсами и взаимоотношениями предприятия

- **Затраты на производительность**:
    - Аппаратные ресурсы (серверы, хранилища данных, сетевые устройства).
    - Программное обеспечение (лицензии, обновления).
    - Энергопотребление и охлаждение.
- **Затраты на функционирование**:
    - Обслуживание системы (администрирование, мониторинг).
    - Обучение персонала.

    - Резервирование и восстановление данных.
- Методы расчета:
    - Анализ Total Cost of Ownership (TCO).
    - Оценка Return on Investment (ROI) для внедрения новых технологий.

16. Организация безопасности функционирования систем управления ресурсами и взаимоотношениями предприятия при требовании к интероперабельности

- **Интероперабельность** — это способность системы взаимодействовать с другими системами и обмениваться данными.
- **Меры безопасности**:
    - Использование защищенных протоколов (например, HTTPS, TLS).
    - Контроль доступа к API и данным.
    - Шифрование данных при передаче.
    - Регулярный аудит взаимодействия систем для выявления уязвимостей.

17. Безопасность функционирования виртуальных сетей хранения данных (СХД) информационных систем

- **Виртуальные СХД** — это системы хранения данных, построенные на основе виртуализации.
- **Меры безопасности**:
    - Шифрование данных при передаче и хранении.
    - Контроль доступа к виртуальным хранилищам.
    - Резервирование данных для восстановления в случае сбоя.
    - Мониторинг и аудит для выявления аномалий.

18. Проектирование информационных систем управления ресурсами предприятия. Определение параметров безопасности функционирования системы по этапам ЖЦ

- **Этапы жизненного цикла (ЖЦ)**:
    1. **Анализ требований**: определение угроз и рисков.

2. **Проектирование**: внедрение мер безопасности (например, шифрование, контроль доступа).
3. **Разработка**: использование безопасных методов программирования.
4. **Тестирование**: проверка на уязвимости и отказоустойчивость.
5. **Эксплуатация**: мониторинг и обновление системы.
6. **Вывод из эксплуатации**: безопасное удаление данных.

19. Выбор хранения данных при проектировании информационных и телекоммуникационных систем управления ресурсами и взаимоотношениями предприятия

- **Критерии выбора**:
  - Объем данных: выбор между локальными хранилищами и облачными решениями.
  - Скорость доступа: использование SSD или высокопроизводительных сетей.
  - Надежность: резервирование и отказоустойчивость.
  - Безопасность: шифрование данных и контроль доступа.
- Примеры решений:
  - Локальные СХД (например, NAS, SAN).
  - Облачные хранилища (например, AWS S3, Azure Blob Storage).

20. Структура вспомогательных систем SAP системы управления ресурсами и взаимоотношениями предприятия

- **SAP** — это комплексная ERP-система для управления ресурсами предприятия.
- **Вспомогательные системы**:
  - **SAP NetWeaver**: платформа для интеграции и разработки приложений.
  - **SAP Business Warehouse (BW)**: система для аналитики и отчетности.
  - **SAP Solution Manager**: инструмент для управления жизненным циклом системы.
  - **SAP Fiori**: пользовательский интерфейс для доступа к функциям SAP.

- **Безопасность**:
    - Контроль доступа на основе ролей (Role-Based Access Control, RBAC).
    - Шифрование данных и защита соединений.
    - Регулярное обновление и патчинг системы.

1. ГОСТы по информационной безопасности

- **ГОСТ Р 50922-2006**
  "Защита информации. Основные термины и определения".
  Описывает основные понятия в области защиты информации.
- **ГОСТ Р 57580-2017**
  "Безопасность финансовых услуг. Требования к защите информации".
  Применим для систем управления ресурсами, связанных с финансовыми операциями.
- **ГОСТ Р ИСО/МЭК 27001-2022**
  "Информационная безопасность, cybersecurity и защита privacy. Системы менеджмента информационной безопасности. Требования".
  Стандарт для построения системы управления информационной безопасностью (СМИБ).
- **ГОСТ Р ИСО/МЭК 27033-1-2014**
  "Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей".
  Описывает подходы к защите сетевой инфраструктуры.
- **ГОСТ Р ИСО/МЭК 27033-3-2017**
  "Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии".
  Полезен для анализа сетевого окружения.

2. ГОСТы по резервированию данных

- **ГОСТ Р 53647.4-2012**
  "Менеджмент непрерывности бизнеса. Руководство по восстановлению после сбоев".
  Описывает подходы к резервированию и восстановлению данных.
- **ГОСТ Р 55892-2013**
  "Технологии информационные. Резервное копирование данных. Общие

требования".
Устанавливает требования к организации резервного копирования.

3. ГОСТы по управлению ресурсами и ERP-системам

- **ГОСТ Р 53647.1-2009**
  "Менеджмент непрерывности бизнеса. Часть 1. Практическое руководство".
  Полезен для обеспечения стабильности работы систем управления ресурсами.

- **ГОСТ Р 55062-2012**
  "Системы менеджмента качества. Руководство по применению ГОСТ Р ИСО 9001 в сфере информационных технологий".
  Применим для систем управления ресурсами и взаимоотношениями.

4. ГОСТы по сетевым технологиям и безопасности

- **ГОСТ Р 54325-2011**
  "Информационная технология. Защита информации. Требования к защите информации в сетях передачи данных".
  Описывает требования к защите данных в сетях.

- **ГОСТ Р 57583-2017**
  "Информационная технология. Методы и средства обеспечения безопасности. Безопасность виртуализации".
  Полезен для защиты виртуальных сред, используемых в системах управления ресурсами.

5. ГОСТы по функциональной безопасности

- **ГОСТ Р 51904-2002**
  "Программное обеспечение встроенных систем. Общие требования к разработке и документированию".
  Применим для обеспечения функциональной безопасности.

- **ГОСТ Р 54531-2011**
  "Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью".
  Полезен для критических сегментов систем управления.

6. ГОСТы по отказоустойчивости и кластеризации

- **ГОСТ Р 55062-2012**
  "Системы менеджмента качества. Руководство по применению ГОСТ Р ИСО

9001 в сфере информационных технологий".
Полезен для обеспечения отказоустойчивости.

- **ГОСТ Р 56939-2016**
  "Информационная технология. Методы и средства обеспечения безопасности. Обеспечение отказоустойчивости информационных систем".
  Описывает подходы к созданию отказоустойчивых систем.

7. ГОСТы по хранению данных (СХД)

- **ГОСТ Р 55892-2013**
  "Технологии информационные. Резервное копирование данных. Общие требования".
  Применим для организации резервирования в СХД.
- **ГОСТ Р 56938-2016**
  "Информационная технология. Методы и средства обеспечения безопасности. Безопасность систем хранения данных".
  Описывает требования к защите данных в СХД.

8. ГОСТы по критическим сегментам

- **ГОСТ Р 56939-2016**
  "Информационная технология. Методы и средства обеспечения безопасности. Обеспечение отказоустойчивости информационных систем".
  Полезен для защиты критических сегментов.
- **ГОСТ Р 55062-2012**
  "Системы менеджмента качества. Руководство по применению ГОСТ Р ИСО 9001 в сфере информационных технологий".
  Применим для управления критическими процессами.

11. Безопасность функционирования при применении кластеров высокой надежности в компьютерной системе

- **ГОСТ Р 56939-2016**
  "Информационная технология. Методы и средства обеспечения безопасности. Обеспечение отказоустойчивости информационных систем".
  Описывает подходы к созданию отказоустойчивых систем, включая кластеры.
- **ГОСТ Р 55062-2012**
  "Системы менеджмента качества. Руководство по применению ГОСТ Р ИСО

9001 в сфере информационных технологий".
Полезен для обеспечения качества и надежности кластерных систем.

12. Безопасность функционирования в системной и программной инженерии

- **ГОСТ Р ИСО/МЭК 12207-2010**
  "Информационная технология. Процессы жизненного цикла программных средств".
  Описывает процессы разработки и обеспечения безопасности программного обеспечения.

- **ГОСТ Р 56938-2016**
  "Информационная технология. Методы и средства обеспечения безопасности. Безопасность систем хранения данных".
  Применим для проектирования безопасных систем.

13. Непрерывность функционирования систем управления ресурсами и взаимоотношениями предприятия (как требования интероперабельности предприятия)

- **ГОСТ Р 53647.4-2012**
  "Менеджмент непрерывности бизнеса. Руководство по восстановлению после сбоев".
  Описывает подходы к обеспечению непрерывности функционирования.

- **ГОСТ Р ИСО/МЭК 19793-2014**
  "Информационная технология. Открытые распределенные обработки. Использование UML для спецификации систем".
  Полезен для обеспечения интероперабельности.

14. Безопасность функционирования систем управления ресурсами и взаимоотношениями предприятия и информационная безопасность

- **ГОСТ Р ИСО/МЭК 27001-2022**
  "Информационная безопасность, cybersecurity и защита privacy. Системы менеджмента информационной безопасности. Требования".
  Основной стандарт для построения системы информационной безопасности.

- **ГОСТ Р 50922-2006**
  "Защита информации. Основные термины и определения".
  Описывает основные понятия в области защиты информации.

15. Расчет затрат на производительность и функционирование системы управления ресурсами и взаимоотношениями предприятия

- **ГОСТ Р 55062-2012**
  "Системы менеджмента качества. Руководство по применению ГОСТ Р ИСО 9001 в сфере информационных технологий".
  Полезен для оценки затрат и качества.

- **ГОСТ Р ИСО/МЭК 19761-2016**
  "Информационная технология. Оценка затрат на программное обеспечение. Метод COSMIC".
  Описывает методы расчета затрат на разработку и эксплуатацию ПО.

16. Организация безопасности функционирования систем управления ресурсами и взаимоотношениями предприятия при требовании к интероперабельности

- **ГОСТ Р ИСО/МЭК 27033-1-2014**
  "Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей".
  Описывает подходы к защите сетевой инфраструктуры.

- **ГОСТ Р ИСО/МЭК 19793-2014**
  "Информационная технология. Открытые распределенные обработки. Использование UML для спецификации систем".
  Полезен для обеспечения интероперабельности.

17. Безопасность функционирования виртуальных сетей хранения данных (СХД) информационных систем

- **ГОСТ Р 56938-2016**
  "Информационная технология. Методы и средства обеспечения безопасности. Безопасность систем хранения данных".
  Описывает требования к защите данных в СХД.

- **ГОСТ Р 55892-2013**
  "Технологии информационные. Резервное копирование данных. Общие требования".
  Применим для организации резервирования в виртуальных СХД

18. Проектирование информационных систем управления ресурсами предприятия. Определение параметров безопасности функционирования системы по этапам ЖЦ

- **ГОСТ Р ИСО/МЭК 12207-2010**
  "Информационная технология. Процессы жизненного цикла программных средств".
  Описывает процессы разработки и обеспечения безопасности.

- **ГОСТ Р 56939-2016**
  "Информационная технология. Методы и средства обеспечения безопасности. Обеспечение отказоустойчивости информационных систем".
  Полезен для проектирования безопасных систем.

19. Выбор хранения данных при проектировании информационных и телекоммуникационных систем управления ресурсами и взаимоотношениями предприятия

- **ГОСТ Р 55892-2013**
  "Технологии информационные. Резервное копирование данных. Общие требования".
  Описывает подходы к организации хранения данных.

- **ГОСТ Р 56938-2016**
  "Информационная технология. Методы и средства обеспечения безопасности. Безопасность систем хранения данных".
  Применим для выбора безопасных решений хранения.

20. Структура вспомогательных систем SAP системы управления ресурсами и взаимоотношениями предприятия

- **ГОСТ Р ИСО/МЭК 27001-2022**
  "Информационная безопасность, cybersecurity и защита privacy. Системы менеджмента информационной безопасности. Требования".
  Полезен для обеспечения безопасности SAP-систем.

- **ГОСТ Р 55062-2012**
  "Системы менеджмента качества. Руководство по применению ГОСТ Р ИСО 9001 в сфере информационных технологий".
  Применим для управления качеством SAP-систем.