**Примерный перечень вопросов для экзамена\**

**«Современные информационные системы»**

1. Понятие открытой информационной системы. Свойства открытых информационных систем;
2. Классификация открытых информационных систем;
3. Определение распределённой информационной системы. Клиент-серверная архитектура;
4. Жизненный цикл открытой информационной системы. Основные модели жизненного цикла информационной системы;
5. Техническое задание (ТЗ) и технический проект: структура, базовые понятия, назначение, цели и задачи;
6. Визуальный язык моделирования UML: цели, задачи, назначение. Основные виды диаграмм;
7. Каноническое проектирование информационных систем: основные этапы проектирования. Стандарт ГОСТ 34.601-90;
8. Типовое проектирование информационных систем: цели, задачи, назначение, основные этапы;
9. Модель открытых систем Open-systems environment (OSE). Основные понятия: прикладное обеспечение, прикладная платформа, внешняя среда, API-интерфейс, EEI-интерфейс;
10. Базовая эталонная модель взаимосвязи открытых систем (модель OSI). Краткая характеристика уровней модели OSI;
11. Модель COM и DCOM. Описание и структура COM-объекта. Понятие интерфейса;
12. Формат XML. Структура XML-документа. Сериализация и десериализация;
13. Технология Enterprise JavaBeans (EJB). Стандарт Java Message Service (JMS). Основные понятия технологии EJB (роли EJB, сервер EJB, модель управления сохранением состояния компонентов, модель управления транзакциями);
14. Протокол Simple Object Access Protocol (SOAP). Элементы вызова протокола SOAP. Базовые компоненты SOAP-спецификации. Стек протоколов web-сервисов;
15. Технология распределённых вычислений Common Object Request Broker Architecture (CORBA). Понятие стаба, скелетона, маршалинга. Протокол GIOP.
16. Понятие уязвимости, угрозы, атаки. Подходы к обеспечению информационной безопасности информационной системы;
17. Угроза конфиденциальности, целостности, доступности. Уровни доступа к данным;
18. Идентификация, аутентификация, авторизация, аудит. Принципы обеспечения информационной безопасности информационной системы (системность, комплексность, etc.);
19. Определение политики безопасности информационной системы. Модель политики безопасности;
20. Дискреционная модель доступа: основные понятия, описание, примеры применения;
21. Мандатная модель доступа: основные понятия, описание, примеры применения;
22. Ролевая модель доступа: основные понятия, описание, примеры применения. Администрирование иерархии ролей в ролевой модели доступа;
23. Обеспечения безопасности «облачных систем»: SaaS, PaaS и IaaS –

архитектур;

24) Формальное описание обобщённой модели системы защиты информационной системы;

25) Формальное описание вероятностной модели систем защиты информационной системы;

26) Формальное описание модели безопасности информационной системы, построенной с использованием теории графов;

27) Формальное описание модели безопасности информационной системы, построенной с использованием теории автоматов;

28) Уязвимости канального уровня эталонной модели OSI (ARP, STP);

29) Уязвимости сетевого уровня эталонной модели OSI (ICMP, IPv4, IPv6);

30) Уязвимости транспортного уровня эталонной модели OSI (TCP, UDP) и Уязвимости прикладного уровня эталонной модели OSI (SMTP).