ИНСТИТУТ КОМПЬЮТЕРНЫХ НАУК И ТЕХНОЛОГИЙ
ПРОГРАММА
вступительных испытаний в магистратуру
по направлению 09.04.04 «Программная инженерия»

Часть 1: «Методология программной инженерии: Индустриальные технологии разработки ПО»

1. Жизненный Цикл Программ (ЖЦП). Оценка трудоемкости этапов. Разработка и сопровождение программного проекта. Структура функциональных спецификаций (FS).
2. ЖЦП. Отладка и тестирование программного проекта. Структура документа высокоуровневого дизайнера (HLD).
3. ЖЦП. Документирование программного проекта on example of UM structure. Критерии качественной оценки основных моделей ЖЦП.
4. ЖЦП. Каскадная модель разработки программного проекта. Распределение трудоемкости по основным этапам разработки. Структура тестового плана.
5. ЖЦП. Поэтапная модель разработки программного проекта. Распределение трудоемкости по основным этапам разработки. Стандарты кодирования на языках C ANSI или Java. Пример фрагмента кода, разработанного по стандартам
6. ЖЦП. Спиральная модель разработки программного проекта. Распределение трудоемкости по основным этапам разработки. Структура тестового журнала (log файла)
7. ЖЦП. Модель переиспользования и перепроектирования разработки программного проекта. Классификация видов ошибок в программном проекте. Структура тестового плана.
8. ЖЦП. Классификация ПО по сложности разработки. Критерии качественной оценки основных моделей ЖЦП. Структура функциональных спецификаций (FS).
9. Типовой технологический процесс разработки программного продукта в соответствии с ЕСПД: эскизный, технический и рабочий проект. Стандарты кодирования на языках C ANSI или Java. Пример фрагмента кода, разработанного по стандартам.
10. Поколения промышленных ТП. Классификация ПО по сложности разработки. Структура документа высокоуровневого дизайнера (HLD)
11. Сложность разработки ПО и ее источники. Средства борьбы со сложностью: абстракция-свертка, прогнозирование-контроль. Структура тестового журнала (log файла)
12. Модульность как средство борьбы со сложностью программного проекта. Интерфейс, экспорт, импорт, видимость. Структура руководства пользователя.

13. Модульность: интерфейс, экспорт, импорт, видимость. Прочность и сцепление модулей.
    Структура функциональных требований..
14. Документирование программного проекта. Основные требования к разработке документов: Структура руководства пользователя..
15. Тестирование программ. Критерии выбора тестов. Функциональные критерии.
16. Пример программного проекта: Кодирование. Автономная отладка и тестирование. Интеграционное тестирование.
17. Пример программного проекта: Комплексная отладка и тестирование. Системное тестирование. Регрессионное тестирование.
18. Тестирование программ. Стохастические критерии. Модульное тестирование
19. Тестирование программ. Мутационный критерий. Структура системы автоматизации тестирования. Интеграционное тестирование.
20. Тестирование программ. Структурные критерии тестирования. Системное тестирование.
21. Оценка покрытия программы и проекта при тестировании. Издержки тестирования.
    Системное тестирование.
22. Тестирование проекта. Методика интегральной оценки тестированности проекта.
    Регрессионное тестирование.
23. Тестирование комплексов программ. Интеграционное, системное и регрессионное тестирование.
24. Метрики для оценки топологической сложности модулей и их использование для совокупной оценки программного проекта.
25. Метрики для оценки объемной сложности модулей и их использование для совокупной оценки программного проекта.
26. Методы оценки качества ПО: анкеты, рабочие списки, контрольные задачи, распространенные бенчмарки для оценки производительности программного изделия.
27. Количественная оценка объектов с расплывчатыми свойствами: метрики и индикаторы. Использование информационных и топологических метрик для оценки сложности программного модуля.
28. Конструктивные критерии качества ПО. Основные модели программного модуля, используемые для оценки трудоемкости его разработки.
29. Метрики для оценки информационной сложности модулей и их использование для совокупной оценки программного проекта. .
30. Методика оценки характеристики трудоемкости программного проекта.
31. Методика оценки сложности программного проекта.
32. Свойства прогностических оценок качества программного проекта.
33. Основные модели оценки качества модуля программного проекта.
34. Основы эмпирической теории измерений программного обеспечения

35. Принципы разработки спецификаций программного проекта. Диаграммы, использующиеся в процессе разработки спецификаций. (UML)
36. Потоковые диаграммы, диаграммы описания данных и их использование в процессе проектирования. (MSC)
37. Основные требования к разработке документов: Требования к проекту (FS), Проектные спецификации (HLD). Разработка MSC спецификации для тестового сценария
38. Поведенческая спецификация программного проекта средствами языка UML.
39. Поведенческая спецификация программного проекта средствами языка MSC.
40. Поведенческая спецификация программного проекта средствами языка SDL.
41. Ручное и автоматизированное тестирование. Пример тестового набора и тестирующей программы на языке C или C++.
42. Ручное и автоматизированное тестирование. Пример спецификации тестового сценария на языке MSC или UML.
43. Ручное и автоматизированное тестирование. Пример тестовой процедуры
44. Организационная структура программистского коллектива и оценка ее эффективности. Сборочная технология программирования.
45. Программистская бригада: распределение ролей. Оценка вклада отдельного программиста в работу коллектива. Классификация программистских организаций по уровню качества выпускаемого продукта.
46. Методы контроля качества программного проекта в соответствии с процессом. ISO 9000.
47. Методы управления степенью совершенства процесса и инструментальные средства поддержки. Методы контроля качества программного проекта в соответствии с процессом. CMMI
48. Сборочная ТП. Особенности жизненного цикла сборочной ТП. Требования к модулям и интерфейсам.
49. Средства поддержки сборочной ТП в САПР ПО на базе языков C/C++ и Java. Эффективность сборочной ТП.
50. Быстрое программирование (agile programming). Особенности жизненного цикла. Средства поддержки ТП в САПР ПО). Эффективность
51. Аспектное программирование. Особенности жизненного цикла. Требования к модулям и интерфейсам. Средства поддержки в САПР ПО. Эффективность
52. ТП управляющих систем. Сложность проектирования программных систем с ресурсными ограничениями. Целевая компиляция, сборка автономных систем, натурные испытания и сопровождение на объекте.
    ТП отказоустойчивых систем. Надежность программных комплексов.
53. ТП отказоустойчивых распределенных систем. Методы нейтрализации ошибок, адаптации структуры, восстановления состояния. Надежность программных комплексов
54. ТП распределенных систем и сетей. Особенности разработки ПО распределенных систем со статическим и динамическим распределением

функций. Методы повышения надежности /корректности и устойчивости/ ПО распределенных систем.

Часть 2: «Методы и средства защиты компьютерной информации»

1. Безопасность информационных технологий. Основные понятия.

Информационная безопасность, безопасность информации, безопасность информационных технологий.
Конфиденциальность, целостность, доступность.
Угрозы безопасности информационных технологий (ИТ).
Модель нарушителя.
Уязвимости информационных систем и пути нанесения ущерба.
Взаимосвязь основных понятий безопасности ИТ. Управление рисками.
Меры противодействия угрозам безопасности: законодательные, морально этические, организационные, физические, технические.
Основные принципы построения системы защиты АС.

2. Шифрсистемы.

Основные понятия. Классификация криптосистем.
Классификация шифрсистем. Простые шифры.
Теоретико-информационная оценка криптостойкости шифрсистем. Совершенно безопасные системы.
Ненадежность шифров и расстояние единственности.
Практическая стойкость шифра. Современные методы и технологии криптоанализа.
Требования к современным шифрам (диффузия, конфузия, практическая реализуемость). Итерированные блочные шифры. Выбор основных параметров.
Требования к шифрам первого поколения. Сеть Фейстела.
Блочный шифр ГОСТ 28147-89. Основные характеристики. Математическая модель и архитектура.
Требования к шифрам второго поколения. Блочный шифр AES. Основные характеристики. Математическая модель и архитектура.
Сравнительный анализ современных блочных шифров.
Протоколы шифрования. ГОСТ 28147-89. Режим простой замены. Математическая модель, особенности и области применения.
Протоколы шифрования. ГОСТ 28147-89. Режим гаммирования. Математическая модель, особенности и области применения.
Протоколы шифрования. ГОСТ 28147-89. Режим гаммирования с обратной связью. Математическая модель, особенности и области применения.

Сравнительный анализ протоколов шифрования ГОСТ 28147-89 и стандартов США.

3. Обеспечение имитостойкости.

Имитостойкость.
Способы контроля целостности сообщения.
Хэш-функция. Требования к криптографической хэш-функции. Криптостойкость хэш-функций.
Архитектура хэш-функции. Функция сжатия.
Стандарт функции хэширования ГОСТ Р34.11-94. Основные характеристики и математическая модель. Сравнительные характеристики современных хэш-функций.
Стандарт функции хэширования SHA-1. Основные характеристики и математическая модель. Сравнительные характеристики современных хэш-функции.
Протокол контроля целостности с использованием хэш-функции. Область применения.
Коды аутентификации сообщения. Математическая модель. Достоинства и недостатки. Область применения.
HMAC. Математическая модель и основные характеристики. Протокол контроля целостности. Область применения.
Шифрование с контролем целостности. Показатели эффективности. Стандарт блочного шифрования ГОСТ 28147-89, режим выработки имитовставки. Математическая модель и основные характеристики. Протокол контроля целостности.
Сравнительный анализ протоколов контроля целостности.
Методы защиты от навязывания ранее переданных, задержанных или переадресованных сообщений.

4. Криптография с открытым ключом

Требования к преобразованиям в криптографии с открытым ключом. Вычислительно простые и вычислительно сложные проблемы.
Необратимые преобразования с лазейкой и их применение в криптографии с открытым ключом..
Система открытого шифрования RSA. Математическая модель. Протокол применения. Анализ криптостойкости.
Сравнительный анализ шифрования с секретным ключом и открытого шифрования.

5. Электронная цифровая подпись (ЭЦП).

Модель нарушителя и требования к ЭЦП. Сравнение с графической подписью.
ЭЦП RSA, математическая модель, анализ криптостойкости, протокол применения. ЭЦП ElGamal, математическая модель, анализ криптостойкости. Сравнение ЭЦП ElGamal и ЭЦП RSA. ЭЦП DSA, математическая модель, анализ криптостойкости. Математические основы криптографии на эллиптических кривых (ЭК).
ЭЦП на ЭК (ГОСТ Р34.10-2001), математическая модель, анализ криптостойкости, протокол применения.
Сравнительные характеристики ЭЦП (RSA, DSA, ГОСТ Р34.10-2001 (ECDSA)).
Хэш-функции в протоколах цифровой подписи.

6. Управление криптографическими ключами.

Жизненный цикл ключей и функции управления ключами.
Криптографические генераторы псевдослучайных последовательностей (требования, принципы построения, примеры).
Генерация больших простых чисел. Тест Ферма.
Управление ключами в криптосистемах с секретным ключом, сравнительный анализ протоколов децентрализованного и централизованного управления ключами.
Управление ключами в криптосистемах с открытым ключом. Сертификат открытого ключа. Удостоверяющий центр и его функции. Протоколы сертификации и кросс-сертификации.
Гибридные криптосистемы на основе открытого шифрования и открытого распределения ключей системы.

7. Аутентификация субъектов.

Идентификация и аутентификация. Классификация схем аутентификации. Требования к протоколу аутентификации.
Парольная защита. Достоинства и недостатки (уязвимости). Методы усиления парольной защиты.
Аутентификация с использованием криптографических методов. Примеры протоколов.
Аутентификация с нулевой передачей знаний. Протокол Fiat-Shmir, математическая модель, протокол применения, анализ стойкости.
Биометрическая аутентификация. Статические и динамические биометрические образы. Биометрические механизмы. Биометрическая аутентификация и криптографические механизмы.

8. Разграничение доступа.

Политика безопасности и схема разграничения доступа. Избирательное управление доступом. Математическая модель. Достоинства и недостатки.
Полномочное управление доступом. Математическая модель. Особенности применения и реализации. Ролевая модель управления доступом. Математическая модель. Достоинства и недостатки.
Контроль информационных потоков для обеспечения конфиденциальности (модель Bell-LaPadule). Достоинства и недостатки.
Реализация разграничения доступа в современных ОС.

9. Безопасность компьютерных сетей.

Уязвимости IP-сетей, сетевых ОС и прикладных сервисов. Типовые сетевые атаки. Защищенный сетевой протокол IPSec, Архитектура: протоколы безопасности (TSP, AH) и режимы их использования, ассоциация безопасности и протокол согласования ее параметров (ISAKMP), БД политик безопасности.
Защищенный транспортный протокол SSL, архитектура и принципы работы. Межсетевые экраны (МЭ). Основные функции. Типы МЭ. Построение и применение правил фильтрации. Конфигурация МЭ.

10. Оценочные стандарты безопасности информационных технологий.

Нормативные стандарты. «Оранжевая книга» Концепция, основные понятия. Достоинста и недостатки.
Руководящие документы Гостехкомиссии : «Показатели защищенности от НСД к информации», «Классификация АС и требования по защите информации». Концепция, основные понятия, принципы применения, достоинства и недостатки.
ГОСТ ISO/IEC 15408 «Общий критерий оценки безопасности информационных технологий». Концепция документа. Основные понятия: требования безопасности (функциональные и доверия) и их структуризация, уровни доверия, профиль защиты). Принципы применения.

Часть 3: «Сети ЭВМ и коммуникации»

1. Сетевые операционные системы.
2. Telnet
3. Служба DNS
4. Протокол SMTP
5. Протоколы POP3 и IMAP
6. Протокол HTTP

7. Протокол FTP
8. Протокол ICMP. PING
9. Протокол ICMP. TRACEROUTE
10. Сети. LAN. Топология сетей. Модель OSI
11. Ethernet. Формат кадра. CSMA/CD
12. Auto-Negotiation
13. 10-Gigabit Ethernet
14. Физическая среда СКС. Витая пара
15. Физическая среда СКС. Оптоволоконный кабель
16. Технологии уплотнения по длине волны. DWDM. CWDM
17. Электропитание по сети Ethernet. PoE
18. Коммутаторы. Протокол STP
19. LAG. VLAN. Switch Fabric
20. Маршрутизаторы. Статическая и динамическая маршрутизация
21. Удаленный доступ к локальной сети.VPN