МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

ПРОГРАММА

ВСТУПИТЕЛЬНОГО ЭКЗАМЕНА ПО ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ 8D06101 - ИНФОРМАТИКА

Костанай, 2020

Содержание

Введение

Программа вступительного экзамена по специальной дисциплине сформирована в объеме программы предшествующей ступени послевузовского образования (магистратуры).

Основные требования к уровню подготовки поступающих:

Поступающий в докторантуру должен:

иметь представление:

- о методах и путях разработки современного программного и аппаратного обеспечения компьютерных систем;
- об алгоритмических языках и технологиях программирования;
- о приближенных методах для решения прикладных задач, перспективах и тенденциях развития информационных технологий;
- о достижениях отечественной и зарубежной науки и техники в области своей профессиональной деятельности;
- о современных требованиях рынка труда.

знать:

- перспективы и тенденции развития информационных технологий;
- современные средства вычислительной техники, коммуникаций и связи;
- правила, методы и средства подготовки технической документации;
- основы экономики, организации производства и научных исследований, основы трудового законодательства, эргономики;
- современные языки программирования;
- современные технологии программирования и пакеты прикладных программ;
- математические методы и базовые алгоритмы решения прикладных задач;
- визуальное программирование; файл-менеджеры;
- основные модели алгоритмов; методы построения алгоритмов; вычисления сложности работы алгоритмов;
- структуру криптографических сообщений, математические модели текстов и шифров.

уметь:

- формулировать и решать задачи, возникающие в ходе научно-исследовательской и педагогической деятельности и требующие углубленных профессиональных занятий;
- выбирать необходимые методы исследования, модифицировать существующие и разрабатывать новые методы, исходя из задач конкретного исследования;
- обрабатывать полученные результаты, анализировать их с учетом имеющихся данных; работать со специальной литературой и научно-технической информацией;
- разрабатывать различные модули при написании программ; строить собственные компоненты; оформлять компоненты с использованием инструментальных программных средств; создавать обработчики событий;
- разрабатывать алгоритмы для конкретных задач; находить сложность работы алгоритма;
- использовать основные криптографические методы, протоколы и алгоритмы.

иметь навыки:

- работы с программно-аппаратными комплексами, программным обеспечением;
- разработки алгоритмов решения прикладных задач;
- программирования, шифрования данных, в обосновании выбора алгоритмов для шифрования данных.

быть компетентным:

- по всем вопросам, связанными с современными информационными технологиями: в использовании компьютерных систем, языков программирования, программного обеспечения для решения различных задач;
- в методах доказательства корректности алгоритмов для типичных массовых проблем;
- в методах доказательства неразрешимости массовых задач;
- при выборе методов шифрования, применения необходимого математического аппарата и оптимизации процессов шифрования и дешифрования информации.

Настоящая программа предназначена для поступающих в докторантуру по специальности 8D06101 – Информатика.

Вступительный экзамен проводится в форме комплексного экзамена по трем дисциплинам:

1. Технологии разработки программного обеспечения
2. Алгоритмы и их сложность
3. Криптология

Основная часть (содержание дисциплин)

1. Технологии разработки программного обеспечения

Обзор современных технологий разработки программного обеспечения. Организация процесса разработки программного обеспечения. Требования к разработке программного обеспечения. Проектирование программных средств. Тестирование программных средств. Сопровождение программ. Разработка интерфейса. Коллективная разработка программного обеспечения. Экономические аспекты разработки и использования программных продуктов. Объектно-ориентированное программирование. Понятие конструктора и деструктора в языках программирования. Инкрементальный подход в языках программирования. Использование процедур и функций в языках программирования. Понятие модуля в языках программирования. Критерии оценки качества программного обеспечения.

2. Алгоритмы и их сложность

Понятие алгоритма на интуитивном уровне. Анализ алгоритмов. Машины произвольного доступа (МПД) и вычислимые функции. Алгоритмически сложные проблемы. Характеристики сложности вычислений. Классы сложности и NP и их взаимосвязь. Задачи сложности NP. Сложность алгоритмов, использующих рекурсию. Оптимальность вычислений. Использование технологии графовых моделей в программировании. Задача о коммивояжере. Вычислительные алгоритмы. Сложность итерационных алгоритмов. Технологии графовых моделей.

3. Криптология

Задачи и основные понятия криптологии. Основные требования к криптографическим сообщениям. Криптографические методы. Управление секретными ключами. Управление секретными ключами. Разделение секретов. Криптографическая защита баз данных. Модели шифров. Системы шифрования с открытым ключом. Криптографические протоколы. Цифровые подписи. Криптографические хэш-функции. Протоколы распределения ключей. Псевдослучайные последовательности чисел. Специальные алгоритмы для протоколов. Алгоритмы для протоколов.

1 ТЕХНОЛОГИИ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

1. Обзор современных технологий разработки программного обеспечения
Технология программирования в историческом аспекте. Основные понятия и определения. Классификация программного обеспечения. Особенности создания программного продукта. Принципы работы с требованиями к программному обеспечению. Проблематика проектирования.

2. Организация процесса разработки программного обеспечения
Особенности создания программного продукта. Принципы работы с требованиями к программному обеспечению. Проблематика проектирования.

3. Требования к разработке программного обеспечения
Определение требований к программным продуктам. Выбор архитектуры программного обеспечения. Структура и формат данных. Статические, полустатические и динамические структуры. Модульное программирование. Анализ требований и определение спецификаций при структурном подходе. Анализ требований и определение спецификаций при объектном подходе.

4. Проектирование программных средств
Проектирование программного обеспечения при структурном подходе. Структурная схема разрабатываемого программного обеспечения. Функциональная схема. Метод пошаговой детализации при составлении алгоритмов. Структурные карты Константайна. Структурные карты Джексона. CASE-технологии. Ускорение разработки программного обеспечения. Методология RAD. Проектирование программного обеспечения при объектном подходе. Экстремальное программирование. Суть проектирования. Программирование и тестирование.

5. Тестирование программных средств
Термины и определения. Тестирование «белого ящика» и «черного ящика». Порядок разработки тестов. Автоматизация тестирования. Модульное тестирование. Интеграционное тестирование. Системное тестирование. Эффективность и оптимизация программ. Стиль программирования. Надежность программного обеспечения. Отладка программ.

6. Методика тестирования программных систем
Организация процесса тестирования программного обеспечения. Методика тестирования программных систем. Тестирование элементов. Тестирование интеграции. Тестирование правильности. Системное тестирование. Искусство отладки.

7. Сопровождение программ
Виды программных документов. Пояснительная записка. Руководство пользователя. Руководство системного программиста.

8. Разработка интерфейса
Инструментальные средства разработки программ. Технологии программирования. Защита программных продуктов. Пакеты прикладных программ. Оценка стоимости разработки программного обеспечения. Методы оценки эффективности ПО на этапе эксплуатации.

9. Коллективная разработка программного обеспечения
Пакеты прикладных программ. Система контроля версий Microsoft Visual SourceSafe. Система контроля версий Subversion.

10.Экономические аспекты разработки и использования программных продуктов
Оценка стоимости разработки программного обеспечения. Линейный метод. Метод функциональных точек. Оценка с использованием эмпирических данных. Методы оценки эффективности ПО на этапе эксплуатации.

11. Объектно-ориентированное программирование
Эволюция технологий программирования. Средства объектно-ориентированного программирования. Принцип объектно-ориентированного программирования. Сущность объектно-ориентированного подхода к программированию. Объектно-ориентированный анализ. Пример объектно-ориентированного анализа. Объектно-ориентированное проектирование. Процесс объектно-ориентированного проектирования. Понятие жизненного цикла программных изделий.

12. Метрики объектно-ориентированных программных систем
Использование метрик Чидамбера-Кемерера. Метрики Лоренца и Кидда. Набор метрик Фернандо Абреу.

13. Понятие конструктора и деструктора в языках программирования
Понятие конструктора и деструктора. Наследование в объектно-ориентированном программировании.

14. Инкрементальный подход в языках программирования
Понятие языка программирования. Понятие инкрементального программирования. Важные моменты в инкрементальном подходе к языкам программирования.

15. Использование процедур и функций в языках программирования
Понятие процедуры. Понятие функции. Объявление процедур и функций. Рекурсивная функция. Прямая и косвенная рекурсия.

16. Понятие модуля в языках программирования
Понятие модуля. Область видимости имён: локальная переменная, глобальная переменная. Передача параметров: по значению и по ссылке.

17. Критерии оценки качества программного обеспечения
Понятие программного обеспечения. Качество программного обеспечения. Критерии оценки качества программного обеспечения: гибкость, простота, эффективность, уменьшение затрат.

Список экзаменационных вопросов

1. Обзор современных технологий разработки программного обеспечения
2. Организация процесса разработки программного обеспечения
3. Требования к разработке программного обеспечения
4. Проектирование программных средств
5. Тестирование программных средств
6. Методика тестирования программных систем
7. Виды программных документов. Пояснительная записка. Руководство пользователя. Руководство системного программиста.

8. Инструментальные средства разработки программ. Защита программных продуктов. Пакеты прикладных программ.
9. Коллективная разработка программного обеспечения
10. Экономические аспекты разработки и использования программных продуктов
11. Объектно-ориентированное программирование. Средства объектно-ориентированного программирования. Принцип объектно-ориентированного программирования.
12. Метрики объектно-ориентированных программных систем
13. Понятие конструктора и деструктора в языках программирования
14. Инкрементальный подход в языках программирования
15. Использование процедур и функций в языках программирования
16. Понятие модуля в языках программирования
17. Критерии оценки качества программного обеспечения

Список рекомендуемой литературы

1. Гагарина Л. Г., Кокорева Е. В., Виснадул Б. Д. Технология разработки программного обеспечения: учебное пособие / под ред. Л. Г Гагариной. — М: ИД «ФОРУМ»: ИНФРА-М, 2016. — 400 с.: ил. — (Высшее образование).
2. Орлов С.А. Технологии разработки программного обеспечения. СПб.: Питер, 2002. 464 с.
3. Кокарева Е.В., Гагарина Л.Г., Виснадул Б.Д. Технологии разработки программного обеспечения. ИНФРА – М, издательский дом Форум, 2008г.
4. Браудэ Э. Технологии разработки программного обеспечения. СПб.: Питер, 2004. 656 с.
5. Сергушичева А.П. Технологии разработки программного обеспечения: Методические указания к выполнению лабораторной работы №4 «Применение CASE – средств при разработке программного обеспечения». – Вологда: ВоГТУ, 2007. – 31 с.
6. Орлов С.А. Принципы объектно-ориентированного и параллельного программирования на языке Ada 95. Рига: TSI, 2001. 327 с.
7. Ambler, S.W. The Object Primer. 2nd ed. Cambrige University Press, 2001. 541 pp.
8. Beck, K, Fowler, M.Planning Extreme Programming. Addison – Wesley, 2001. 156 pp.
9. Boehm, B.W. etal. Software Cost Estimation with Cocomo II. Prentice Hall, 2011. 502 pp.
10. Fowler, M. The New Methodology http://www.martinfoler.com, 2001
11. Дин Леффингуэлл, Дон Уидриг. Принципы работы с требованиями к программному обеспечению. М.: Вильяме, 2002.
12. Липаев В. В. Проектирование программных средств. М.: Высшая школа, 1990.
13. Майерс Г. Искусство тестирования программ. М.: Финансы и статистика, 1982.
14. Брукс Ф. Мифический человеко-месяц, или Как создаются программные системы. СПб.: Символ-Плюс, 1999.
15. Роберт Дж. Орберг. COM+ технология. Основы и программирование М.: Вильяме, 2000. 478 с.
16. Аджиев В. // Открытые системы. 1998. № 1.
17. Батенко Л. П. // Менеджмент и менеджер. 2003. № 3.
18. Алистэр Коуберн, Лори Вильяме. Парное программирование: преимущества и недостатки.
19. Жоголев Е. А. Введение в технологию программирования (конспект лекций). М.: ДИАЛОГ-МГУ, 1994.
20. Страуструп Б. Язык программирования C++. Киев: ДиаСофт, 1993.
21. Модели и структуры данных / В. Д. Далека, А. С. Деревянко, О. Г. Кравец, Л. Е. Тимановская. Харьков: ХГПУ, 2000.

2 АЛГОРИТМЫ И ИХ СЛОЖНОСТЬ

1. Понятие алгоритма на интуитивном уровне
Интуитивное понятие алгоритма и его свойства. Меры эффективности алгоритма. Классы алгоритмов. Полиномиальные и экспоненциальные алгоритмы.

2. Анализ алгоритмов
Принципы разработки алгоритмов. Реализация и эмпирический анализ. Анализ алгоритмов. Алгоритмическая модель машины Тьюринга. Вычисление функций на машине Тьюринге.

3. Машины произвольного доступа (МПД) и вычислимые функции
Алгоритмическая модель МПД. Вычисление функций на МПД. Тезиз Черча. Принципы построения дискретных моделей. Выбор алгоритма решения задач. Анализ устойчивости по Фон-Нейману. Тезиз Черча для частично рекурсивных функций.

4. Алгоритмически сложные проблемы
Построение алгоритма совместного решения системы уравнений. Особенности программирования.

5. Характеристики сложности вычислений
Алгоритмы решений системы уравнений. Функции временной и емкостной сложности. Нижние оценки временной сложности на машинах Тьюринга.

6. Классы сложности и NP и их взаимосвязь
Подмножества множеств. Генерирование подмножества множеств. NP – полные задачи. Теорема Кука.

7. Задачи сложности NP
Основные NP полные задачи. Сильная NP полнота. Класс co- NP. Структура классов NP и co- NP. Применение теории NP-полноты к разработке приближенных алгоритмов.

8. Сложность алгоритмов, использующих рекурсию
Моделирование и реализация алгоритма решения двумерных задач. Рекурсивный алгоритм обращения матрицы.

9. Оптимальность вычислений
Реализация алгоритмов при использовании неравномерной разностной сетки. Оптимальность вычислений. Способы оптимизации вычислений

10. Использование технологии графовых моделей в программировании
Использование технологии графовых моделей в программировании. Сведение модели алгоритма решения задачи к графовой

11. Основные алгоритмы на графах
Поиск в глубину в графе. Поиск в ширину в графе. Кратчайший путь в графе. Максимальный поток в графе. Минимальное остовное дерево графа.

12. Задача о коммивояжере
Алгоритмы с гарантированной оценкой точности для задачи коммивояжера. Метод ветвей и границ.

13. Вычислительные алгоритмы
Пересечение отрезков, вычисление углов многоугольника. Основные алгоритмы решения геометрических задач.

14. Сложность итерационных алгоритмов
Разработка итерационных алгоритмов. Принципы построения дискретных моделей. Выбор алгоритма решения задач.

15. Технологии графовых моделей
Лабиринты, алгоритмы поиска путей в лабиринте: поиск с возвратом, волновой метод.

16. Разработка эффективных алгоритмов
Метод разделяй и властвуй. Динамическое программирование.

Список экзаменационных вопросов

1. Понятие алгоритма на интуитивном уровне.
2. Эмпирический анализ алгоритмов. Алгоритмическая модель машины Тьюринга.
3. Машины произвольного доступа (МПД) и вычислимые функции.
4. Алгоритмически сложные проблемы.
5. Характеристики сложности вычислений.
6. Классы сложности и NP и их взаимосвязь.
7. Задачи сложности NP.
8. Сложность алгоритмов, использующих рекурсию.
9. Способы оптимизации вычислений. Реализация алгоритмов при использовании неравномерной разностной сетки.
10. Использование технологии графовых моделей в программировании.
11. Основные алгоритмы на графах. Поиск в глубину в графе. Поиск в ширину в графе. Кратчайший путь в графе.
12. Задача о коммивояжере.
13. Вычислительные алгоритмы.
14. Комбинаторика. Размещения. Перестановки. Перестановки с повторениями. Сочетания. Сочетания и бином Ньютона.
15. Сложность итерационных алгоритмов.
16. Технологии графовых моделей
17. Разработка эффективных алгоритмов с использованием метода разделяй и властвуй

Список рекомендуемой литературы

1. Алгоритмы. Руководство по разработке», Стивен Скиена,2-е издание, 720 стр., БХВПетербург, 2011
2. Кузюрин, С.А. Фомин. Курс лекций «Сложность алгоритмов» (2013).
3. Sipser M. Introduction to the Theory of Computation. Boston, Mass.: Thomson Course Technology, 2016 (pp. 368–380).
4. Arora S. and Barak B. Computational Complexity: A Modern Approach. Cambridge University Press, 2017 (Chapter 7).
5. Кормен Томас. Алгоритмы: построение и анализ. М.: Вильямс, 2005.
6. M.T. Goodrich, R.Tamassia. Data structures and Algorithms in Java., Prentice Hall. 2005. – 695 p.
7. Р.Сейджвик. Фундаментальные алгоритмы на С.- СПб: ООО «ДиаСофтЮП», 2003. – 1136с.

8. S. Baase. Computer Algorithms. Introduction to Design and Analysis. 2nd edition, Prentice Hall. 2001
9. J.Hastad Notes for the course advanced algorithms
10. Абрамов С.А. Лекции о сложности алгоритмов, - М.: МЦНМОб 2009.
11. Кузюрин Н.Н., Фомин С.А. Эффективные алгоритмы и сложность вычислений, - М.: МФТИ, 2007.
12. Шурыгин В.А. Сложностный метод теории алгоритмов. – М.: ЛИБРОКОМ, 2009.
13. Окулов С.М. Программирование в алгоритмах. - М.:БИНОМ. Лаборатория знаний, 2002. - 341с.
14. Ахо А., Хопкрофт Д., Ульман Д. Структуры данных и алгоритмы.: Пер. с англ.:Учебное пособие. –М.:Издательский дом «Вильямс», 2000. – 384с.
15. Культин Н. Turbo Pascal в задачах и примерах. – СПб.: БХВ-Петербург, 2000. – 256с.
16. Кирюхин В. М., Лапунов А. И., Окулов С. М. Задачи по информатике (международные олимпиады 1989-1996). М.: ABF, 1996.

3 КРИПТОЛОГИЯ

1. Задачи и основные понятия криптологии
Симметричные и асимметричные шифросистемы. Понятие о криптографических протоколах. Организация секретной связи, задачи криптоаналитика.

2. Методы теории информации в криптологии
Количество информации по Шеннону и его свойства. Шенноновские модели криптосистем. Теоретико-информационные оценки стойкости симметричных криптосистем.

3. Основные требования к криптографическим сообщениям
Конфиденциальность. Целостность. Аутентичность.

4. Криптографические методы
Предварительное распределение ключей. Пересылка ключей. Открытое распределение ключей. Схема разделения.

5. Управление секретными ключами
Обмен ключами. Формальный анализ протоколов проверки подлинности и обмена ключами.

6. Управление секретными ключами. Разделение секретов
Разделение секрета. Совместное использование секрета.

7. Криптографическая защита баз данных
Криптографическая защита баз данных. Типы алгоритмов и криптографические режимы.

8. Модели шифров
Шифрсистема RSA. Шифрсистема Диффи Хеллмана. Шифрсистема Эль Гамаля.

9. Системы шифрования с открытым ключом
Шифрсистема Мак Эллиса. Шифрсистемы на основе алгоритма «проблема рюкзака»

10. Криптографические протоколы

Элементы протоколов. Основные протоколы. Промежуточные протоколы. Развитые протоколы. Эзотерические протоколы. Доказательства с нулевым знанием.

11. Цифровые подписи
Цифровые подписи на основе шифрсистем с открытыми ключами. Цифровая подпись Фиата-Шамира. Цифровая подпись Эль Гамаля.

12. Криптографические хэш-функции
Функции хэширования и целостность данных. Ключевые функции хэширования. Бесключевые функции хэширования.

13. Криптографические алгоритмы.
Стандарт шифрования данных DES . Блочные шифры. Объедение блочных шифров. Генераторы псевдослучайных последовательностей и потоковые шифры. Генераторы настоящих случайных последовательностей.

14. Протоколы распределения ключей
Передача ключей с использованием симметричного шифрования. Двусторонние протоколы. Трехсторонние протоколы. Передача ключей с использованием асимметричного шифрования.

15. Псевдослучайные последовательности чисел
Простейшие алгоритмы генерации. Рекуррентные двоичные последовательности. Последовательности максимальной длины. Анализ псевдослучайных последовательностей.

16. Специальные алгоритмы для протоколов
Криптография с несколькими открытыми ключами. Алгоритмы разделения секрета. Подсознательный канал.

17. Алгоритмы для протоколов
Бросание «Честной монеты». Однонаправленные сумматоры. Раскрытие секретов «все или ничего». Квантовая криптография

Список экзаменационных вопросов

1. Симметричные и асимметричные шифросистемы. Понятие о криптографических протоколах.
2. Количество информации по Шеннону и его свойства. Шенноновские модели криптосистем.
3. Основные требования к криптографическим сообщениям
4. Предварительное распределение ключей. Пересылка ключей. Открытое распределение ключей.
5. Обмен секретными ключами. Формальный анализ протоколов проверки подлинности и обмена ключами.
6. Управление секретными ключами. Разделение секретов
7. Криптографическая защита баз данных
8. Модели шифров: шифрсистема RSA, шифрсистема Диффи Хеллмана.
9. Системы шифрования с открытым ключом
10. Криптографические протоколы
11. Цифровые подписи на основе шифрсистем с открытыми ключами. Цифровая подпись Фиата-Шамира.
12. Криптографические хэш-функции

13. Стандарт шифрования данных DES . Блочные шифры. Объедение блочных шифров.
14. Протоколы распределения ключей
15. Псевдослучайные последовательности чисел
16. Специальные алгоритмы для протоколов
17. Алгоритмы для протокола бросание «Честной монеты». Раскрытие секретов «все или ничего».

Список рекомендуемой литературы

1. А.В.Черемушкин. Лекции по арифметическим алгоритмам в криптографии. - М.: МЦНМО, 2015.
2. Фомичев В.М. Дискретная математика и криптология. – М.: ДИАЛОГ-МИФИ, 2003.
3. Тилберг К.Х.А. Основы криптологии. Профессиональное руководство. – М.: Мир, 2007.
4. Нечаев В.И. Элементы криптографии. Основы теории защиты информации. М.: Высшая школа, 1999.
5. Шнайер Б. Прикладная криптография. – СПб: Питер, 2005.
6. Казарин О.В. Теория и практика защиты программ. – М.: Высшая школа, 2000.
7. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. – Спб.: Питер, 2000.
8. W. Stallings. CryptographyandNetworksecurity. PrinciplesandPractice. SecondEdition. Upper Saddle River, NJ: Prentice Hall, 1999.
9. J. JaworskiandP. Perrone. Java Security Handbook.- SAMS Publishing, 2000.