**Федеральное государственное автономное образовательное учреждение высшего профессионального образования   
"Национальный исследовательский университет   
"Высшая школа экономики"**

Факультет экономики, менеджмента и бизнес-информатики

Кафедра информационных технологий в бизнесе

**Рабочая программа дисциплины**

**Алгоритмы и структуры данных**

для образовательной программы Программная инженерия

направления подготовки 09.03.04 Программная инженерия

уровень бакалавр

Разработчик программы

Морозенко В.В., к.ф.-м.н., доцент, vmorozenko@hse.ru

Одобрена на заседании кафедры информационных технологий в бизнесе

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_ 2015 г.

И.о. зав. кафедрой Викентьева О.Л.\_\_\_\_\_\_\_

Рекомендована Академическим советом образовательных программ бакалавриата «Бизнес-информатика» и «Программная инженерия» и образовательной программы магистратуры «Информационная аналитика в управлении предприятием»

«\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_ 2015 г., № протокола\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Утверждена «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_ 2015 г.

Академический руководитель образовательной программы

А.О. Сухов \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Пермь, 2015

*Настоящая программа не может быть использована другими подразделениями университета и другими вузами без разрешения подразделения-разработчика программы.*

# Область применения и нормативные ссылки

Настоящая программа учебной дисциплины устанавливает минимальные требования к знаниям и умениям студента и определяет содержание и виды учебных занятий и отчетности.

Программа предназначена для преподавателей, ведущих данную дисциплину, учебных ассистентов и студентов направления подготовки 09.03.04 «Программная инженерия», изучающих дисциплину «Алгоритмы и структуры данных».

Программа разработана в соответствии с:

* Образовательным стандартом федерального государственного автономного образовательного учреждения высшего профессионального образования национального исследовательского университета «Высшая школа экономики» по направлению 09.03.04 Программная инженерия, утвержденным Ученым советом Национального исследовательского университета «Высшая школа экономики», протокол от 30.01.2015 №1;
* Рабочим учебным планом университета по направлению подготовки 09.03.04 Программная инженерия, утвержденным в 2015 г.

# Цели освоения дисциплины

Целями освоения дисциплины «Алгоритмы и структуры данных» являются:

*В области обучения* – получение высшего профессионально профилированного (на уровне бакалавра) образования, позволяющего выпускнику успешно работать в избранной сфере деятельности, обладать универсальными и предметно-специализированными компетенциями, способствующими его социальной мобильности и устойчивости на рынке труда, а именно: изучение основных приемов и методов, используемых при разработке и анализе математических моделей и алгоритмов для решения сложных прикладных задач.

*В области воспитания* – развитие у студентов социально-личностных качеств: целеустремленности, организованности, трудолюбия, ответственности, самостоятельности, гражданственности, эмоционального интеллекта, приверженности этическим ценностям, коммуникативности, умения работать в коллективе, толерантности, повышение их общей культуры и мышления.

Для достижения поставленных целей при изучении дисциплины решаются следующие *задачи:*

* познакомить студентов с основными классами алгоритмов, их математическими моделями;
* дать знания о существующих эффективных алгоритмах для решения наиболее известных задач комбинаторной оптимизации, об их сложности и требованиям к памяти;
* познакомить с классификацией оптимизационных задач и алгоритмов для их решения, особенностями задач комбинаторной оптимизации большой размерности;
* дать представление о методах анализа сложности алгоритмов и доказательства их корректности.

Курс призван повысить общую эрудицию студентов, дать им возможность ориентироваться в данной предметной области, подготовить к применению теоретических знаний при решении различных задач оптимизации, при изучении и разработке средств поддержки принятия решений. Студенты должны получить знания о существующих эффективных алгоритмах, используемых в теории расписаний, методах их разработки и анализа.

# Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины студент должен:

* Знать о различных методах классификации существующих алгоритмов; наиболее известные алгоритмы для работы с различными структурами данных; точные и приближенные подходы к решению типовых задач, возникающих в области программной инженерии; особенности точных, приближенных, эвристических, переборных, «жадных» алгоритмов.
* Уметь анализировать существующие алгоритмы с точки зрения их эффективности и применимости для решения прикладных задач; разрабатывать новые алгоритмы для решения конкретных задач в области программной инженерии; оценивать сложность разработанных алгоритмов и обосновывать их корректность.
* Иметь навыки (приобрести опыт) применения известных и разработки собственных алгоритмов для решения практических задач с учетом требований к точности, времени работы алгоритма и вычислительным ресурсам; формализации и разработки математических моделей и алгоритмов для решения конкретных практических проблем в сфере программной инженерии или их сведения к известным модельным задачам.

В результате освоения дисциплины студент осваивает следующие компетенции:

| Компетенция | Код по ФГОС/ НИУ | Дескрипторы – основные признаки освоения (показатели достижения результата) | Формы и методы обучения, способствующие формированию и развитию компетенции |
| --- | --- | --- | --- |
| Способен формализовать предметную область программного проекта и разработать спецификации для компонентов программного продукта | ПК-6 | Демонстрирует умение обосновывать предлагаемые решения, разрабатывать алгоритмы и программы, реализующие их | Аудиторные занятия проводятся в форме, предполагающей активное участие студентов в работе, обсуждение проблем и анализ решений, предлагаемых студентами и преподавателем на лекциях и практических занятиях |
| Способен проектировать, конструировать и тестировать программные продукты | ПК-10 | Знает и может использовать на практике математический аппарат, формальные средства, лежащие в основе различных методов разработки алгоритмов и программ. | Выполнение практических заданий с использованием языков C# и С++, тестирование разработанных программ с использованием различных методов и средств отладка |
| Четко формулирует задачи, анализирует условия и обоснованно выбирает методы решения, уверенно интерпретирует результаты |
| Способен читать, понимать и выделять главную идею прочитанного исходного кода, документации | ПК-11 | Показывает умение чтения исходного кода алгоритмов, решающих отдельные подзадачи в рамках одной исходной задачи | Получение формальных оценок и сравнение их с результатами, полученными при практической реализации |
| Способен оценивать временную и емкостную сложность программного обеспечения | ПК-13 | Уверенно использует способы формального описания алгоритмов с применением математического аппарата. |
| Может построить оценки и доказать свойства алгоритмов и программ с использованием формальных методов |

# Место дисциплины в структуре образовательной программы

Настоящая дисциплина относится к профессиональному циклу дисциплин, и блоку дисциплин, обеспечивающих базовую подготовку.

Изучение данной дисциплины базируется на следующих дисциплинах:

* Программирование.
* Дискретная математика.
* Информатика, математическая логика и теория алгоритмов.
* Конструирование программного обеспечения.

Для освоения учебной дисциплины, студенты должны владеть следующими знаниями и компетенциями:

* способен вести исследовательскую деятельность, включая анализ проблем, постановку целей и задач, выделение объекта и предмета исследования, выбор способа и методов исследования, а также оценку его качества
* способен работать в команде
* способен применять основные концепции, принципы, теории и факты, связанные с информатикой при решении научно-исследовательских задач;
* способен к формализации в своей предметной области с учетом ограничений используемых методов исследования
* способен моделировать, анализировать и использовать формальные методы конструирования программного обеспечения
* способен использовать различные технологии разработки программного обеспечения
* способен применять основные методы и инструменты разработки программного обеспечения

Основные положения дисциплины должны быть использованы в дальнейшем при изучении следующих дисциплин:

* Конструирование программного обеспечения (продолжение курса).
* Распределенные вычисления.
* Введение в методы трансляции.
* Распознавание образов.
* Современные теории и средства имитационного моделирования.
* Системы поддержки принятия решений.
* Командный проект по программной инженерии.

# Тематический план учебной дисциплины

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | Название раздела | Всего часов | Аудиторные часы | | Самостоя­тельная работа |
| Лекции | Практические занятия |
|  | **Раздел 1. Дополнительные разделы дискретной математики** | **84** | **20** | **20** | **44** |
| 1. | Однородные рекуррентные соотношения и системы соотношений | 8 | 2 | 2 | 4 |
| 2. | Неоднородные рекуррентные соотношения и системы отношений | 12 | 2 | 4 | 6 |
| 3. | Производящие функции | 10 | 2 | 2 | 6 |
| 4. | Методы доказательства оценок сложности рекурсивных алгоритмов | 8 | 2 | 2 | 4 |
| 5. | Простые числа. Асимптотический закон распределения простых чисел | 8 | 2 | 2 | 4 |
| 6. | Модулярная арифметика. Китайская теорема об остатках | 8 | 2 | 2 | 4 |
| 7. | Алгебраические структуры: конечные абелевы группы и поля, кольца целых чисел и вычетов. | 12 | 4 | 2 | 6 |
| 8. | Симметрическая группа подстановок. Теорема Бернсайда | 8 | 2 | 2 | 4 |
| 9. | Цикловой индекс группы подстановок. Теория перечисления Пойя | 10 | 2 | 2 | 6 |
|  | **Раздел 2. Графовые и потоковые алгоритмы** | **52** | **12** | **12** | **28** |
| 10. | Алгоритм поиска максимального паросочетания в двудольном графе | 8 | 2 | 2 | 4 |
| 11. | Алгоритм поиска совершенного паросочетания в двудольном графе | 8 | 2 | 2 | 4 |
| 12. | Венгерский алгоритм для решения задачи о назначении | 10 | 2 | 2 | 6 |
| 13. | Алгоритм поиска максимального потока в сети | 8 | 2 | 2 | 4 |
| 14. | Алгоритм поиска максимального потока минимальной стоимости | 8 | 2 | 2 | 4 |
| 15. | Транспортная задача | 10 | 2 | 2 | 6 |
|  | **Раздел 3. Алгоритмы теории расписаний** | **44** | **10** | **10** | **24** |
| 16. | Алгоритмы теории расписаний для независимых заданий | 8 | 2 | 2 | 4 |
| 17. | Алгоритмы теории расписаний для зависимых единичных заданий | 8 | 2 | 2 | 4 |
| 18. | Алгоритмы теории расписаний для зависимых заданий произвольной длительности | 10 | 2 | 2 | 6 |
| 19. | Алгоритмы теории расписаний для исполнителей с разной производительностью | 10 | 2 | 2 | 6 |
| 20. | Конвейерная задача | 8 | 2 | 2 | 4 |
|  | **Раздел 4. Алгоритмы комбинаторной оптимизации** | **28** | **6** | **6** | **16** |
| 21. | Динамическое программирование | 10 | 2 | 2 | 6 |
| 22. | Дискретная задача оптимального распределения инвестиций | 8 | 2 | 2 | 4 |
| 23. | Метод ветвей и границ | 10 | 2 | 2 | 6 |
| 24. | Сведение задач комбинаторной оптимизации к задачам на потоки | 8 | 2 | 2 | 4 |
|  | **Раздел 5. Криптографические алгоритмы** | **44** | **10** | **10** | **24** |
| 25. | Целочисленные алгоритмы в кольцах вычетов и конечных полях | 8 | 2 | 2 | 4 |
| 26. | Проверка чисел на простоту. Построение больших простых чисел | 8 | 2 | 2 | 4 |
| 27. | Алгоритмы факторизации | 8 | 2 | 2 | 4 |
| 28. | Криптографические системы | 10 | 2 | 2 | 6 |
| 29. | Методы криптоанализа | 10 | 2 | 2 | 6 |
|  | **Раздел 6. Приближенные алгоритмы и эвристики** | **44** | **10** | **10** | **24** |
| 30. | Приближенные алгоритмы и эвристики для решения задачи о рюкзаке | 8 | 2 | 2 | 4 |
| 31. | Приближенные алгоритмы и эвристики для решения задачи коммивояжера | 8 | 2 | 2 | 4 |
| 32. | Генетические алгоритмы | 28 | 6 | 6 | 16 |
|  | ***Всего:*** | **304** | **70** | **70** | **164** |

# Формы контроля знаний студентов

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Тип контроля | Форма контроля | 1 год | | | | Параметры |
| 1 | 2 | 3 | 4 |
| Текущий (неделя) | Контрольная работа |  | 8 |  |  | Письменная работа 80 мин. |
| Домашнее задание |  |  | 7 | 6 | Письменная работа из одного индивидуального задания |
| Промежуточный | Экзамен |  | \* |  |  | Письменный экзамен 80 мин. |
| Итоговый | Экзамен |  |  |  | \* | Письменный экзамен 80 мин. |

## Критерии оценки знаний, навыков

При выполнении контрольной работы студент должен продемонстрировать знания основных понятий и алгоритмов из соответствующего раздела учебного курса, умения применять указанные алгоритмы для решения предложенных задач и обосновывать корректность полученных решений. Количество задач в контрольных работах – от 6 до 8. Каждая задача оценивается в 1-2 балла, так что общая сумма баллов равна 10.

При выполнении домашних заданий студент должен продемонстрировать знания основных понятий и алгоритмов из соответствующего раздела учебного курса, умения самостоятельно изучать учебную литературу и применять полученные знания при решении предложенных задач.

Оценки по всем формам текущего контроля выставляются по 10-ти балльной шкале.

При выполнении письменной экзаменационной работы студент должен продемонстрировать знания основных понятий и алгоритмов из всего учебного курса, умения применять указанные алгоритмы для решения предложенных задач и обосновывать корректность полученных решений. Работа содержит 1 теоретический вопрос, который оценивается в 2 балла, и 5 практических заданий, каждое из которых оценивается в 1-2 балла, так что общая сумма баллов равна 10.

Промежуточный и итоговый контроль включает как теоретические вопросы, так и практические задания по темам всего курса. Примерный перечень вопросов для подготовки к экзамену по дисциплине приведен в разделе 9.1.

## Порядок формирования оценок по дисциплине

Преподаватель оценивает работу студентов на практических занятиях: студенты работают по карточкам, на которых указаны практические задания. Работа каждого студента оценивается с учетом количества задач, решенных им во время занятия. Оценки за работу на практических занятиях преподаватель выставляет в рабочую ведомость. Оценка по 10-ти балльной шкале за работу на практических занятиях определяется перед промежуточным или итоговым контролем и называется – *Оаудиторная*.

**1,2 модули**

**Оценка за текущий контроль**(*Отекущий*) рассчитывается как взвешенная сумма всех форм текущего контроля.

*Отекущий* = *n1* \**Ок/р.*

при этом *n1 = 1.*

**Накопленная оценка** за текущий контроль учитывает результаты студента по текущему контролю следующим образом:

*Онакопленная*= 2/3\**Отекущий* + 1/3\* О*аудиторная*

Способ округления накопленной оценки текущего контроля: арифметический.

**Результирующая оценка** рассчитывается следующим образом

*Орезультирующая = 0,6\* Онакопленная + 0,4\*·Оэкз*

Способ округления накопленной оценки промежуточного контроля в форме экзамена: арифметический.

**3,4 модули**

**Оценка за текущий контроль** *(Отекущий*) рассчитывается как взвешенная сумма всех форм текущего контроля.

*Отекущий* = *n1·Одз1* + *n2·Одз2,*

при этом *n1 = n2 = 0,5*.

Способ округления оценки за текущий контроль: арифметический.

**Накопленная оценка** за текущий контроль учитывает результаты студента по текущему контролю следующим образом:

*Онакопленная*= 2/3\**Отекущий* + 1/3\* *Оаудиторная*

Способ округления накопленной оценки текущего контроля: арифметический.

**Результирующая оценка** рассчитывается следующим образом

*Орезультирующая = 0,6\* Онакопленная + 0,4\*·Оэкз*

Способ округления накопленной оценки итогового контроля в форме экзамена: арифметический.

**Результирующая оценка по дисциплине** – это взвешенная сумма результирующих оценок за все модули прохождения дисциплины.

*О* *промежуточная 1* – результирующая оценка за 2 модуль.

*О* *промежуточная 2* – результирующая оценка за 4 модуль.

*О* *результирующая* = *r1*\**Опромежуточная 1* + *r2*\**О* *промежуточная 2*

где *ri* – вес результирующих оценок, при этом *r1* = 0,5, *r2* = 0,5.

Способ округления результирующей оценки по дисциплине: арифметический.

На пересдаче студенту не предоставляется возможность получить дополнительный балл для компенсации оценки за текущий контроль.

На экзамене студент может получить дополнительный вопрос (дополнительную практическую задачу, решить к пересдаче домашнее задание), ответ на который оценивается в 1 балл.

В диплом выставляет результирующая оценка по учебной дисциплине, которая формируется равной результирующей оценке за последний модуль последнего года проведения дисциплины.

# Содержание дисциплины

1. Раздел 1. Дополнительные разделы дискретной математики

Тема 1. Однородные рекуррентные соотношения и системы

Решение однородных систем линейных рекуррентных соотношений с постоянными коэффициентами методом исключения неизвестных и матричным методом (через нахождение собственных значений и собственных векторов матрицы, составленной из коэффициентов).

Количество часов аудиторной работы: 4.

Общий объем самостоятельной работы студента: 4 часа.

Тема 2. Неоднородные рекуррентные соотношения и системы

Решение неоднородных систем линейных рекуррентных соотношений с постоянными коэффициентами методом исключения неизвестных и матричным методом (через нахождение собственных значений и собственных векторов матрицы, составленной из коэффициентов). Примеры задач, приводящих к рекуррентным соотношениям.

Количество часов аудиторной работы: 6.

Общий объем самостоятельной работы студента: 6 часа.

Тема 3. Производящие функции

Полиномиальные и экспоненциальные производящие функции. Нахождение производящих функций для конкретных последовательностей с использованием рядов Тейлора и известных разложений элементарных функций в ряд Маклорена. Решение линейных рекуррентных соотношений с постоянными коэффициентами через производящие функции.

Количество часов аудиторной работы: 4.

Общий объем самостоятельной работы студента: 6 часов.

Тема 4. Методы доказательства оценок сложности рекурсивных алгоритмов

Примеры рекурсивных алгоритмов. Получение рекуррентных соотношений при анализе сложности рекурсивных алгоритмов. Взаимная рекурсия. Решение линейных неоднородных рекуррентных соотношений с постоянными коэффициентами (методом неопределенных коэффициентов) и с переменными коэффициентами (через производящие функции).

Количество часов аудиторной работы: 4.

Общий объем самостоятельной работы студента: 4 часа.

Тема 5. Простые числа. Асимптотический закон распределения простых чисел

Элементарные методы проверки простоты чисел: метод проб, решето Эратосфена, метод Ферма. Числа Мерсенна и Ферма. Теорема Чебышева о распределении простых чисел.

Количество часов аудиторной работы: 4.

Общий объем самостоятельной работы студента: 4 часа.

Тема 6. Модулярная арифметика. Китайская теорема об остатках

Алгоритм Евклида. НОД и НОК. Сравнения. Классы вычетов. Обратный мультипликативный элемент. Функция Эйлера. Малая теорема Ферма. Теорема Эйлера. Алгоритмы модулярной арифметики. Системы сравнений. Китайская теорема об остатках.

Количество часов аудиторной работы: 4.

Общий объем самостоятельной работы студента: 4 часа.

Тема 7. Алгебраические структуры: конечные абелевы группы и поля, кольца целых чисел и вычетов

Группы и подгруппы. Теорема Лагранжа. Циклические группы. Группы подстановок. Разложение подстановок. Кольца и поля. Кольца целых чисел. Сравнения целых чисел по модулю. Классы вычетов и операции над ними.

Количество часов аудиторной работы: 6.

Общий объем самостоятельной работы студента: 6 часов.

Тема 8. Симметрическая группа подстановок. Теорема Бернсайда

Свойства симметрической группы подстановок. Теорема Бернсайда. Подсчет числа неэквивалентных комбинаторных объектов с помощью теоремы Бернсайда.

Количество часов аудиторной работы: 4.

Общий объем самостоятельной работы студента: 4 часа.

Тема 9. Цикловой индекс группы подстановок. Теория перечисления Пойя

Цикловой индекс подстановки и группы подстановок. Теория перечисления Пойа. Первая и вторая теоремы Пойа. Подсчет числа неэквивалентных комбинаторных объектов с помощью теорем Пойа.

Количество часов аудиторной работы: 4.

Общий объем самостоятельной работы студента: 6 часов.

**Литература по разделу:**

Гагарина Л.Г., Колдаев В.Д. Алгоритмы и структуры данных: учебное пособие. – М.: Финансы и статистика, 2009. – 304 с.

Ахо А., Хопкрофт Дж., Ульман Дж. Структуры данных и алгоритмы. – М.: Вильямс, 2010.

Грэхем Р.Л., Кнут Д.Э., Паташник О. Конкретная математика. Математические основы информатики: пер. с англ. – М.: Вильямс, 2013.

1. Раздел 2. Графовые и потоковые алгоритмы

Тема 10. Алгоритм поиска максимального паросочетания в двудольном графе

Чередующиеся цепи. Метод «волны» для поиска чередующихся цепей. Теорема Бержа. Алгоритм поиска максимального паросочетания с помощью чередующихся цепей.

Количество часов аудиторной работы: 4.

Общий объем самостоятельной работы студента: 4 часа.

Тема 11. Алгоритм поиска совершенного паросочетания в двудольном графе

Чередующееся дерево. Метод «волны» для поиска чередующихся деревьев. Теорема Холла. Алгоритм поиска совершенного паросочетания с помощью чередующихся деревьев.

Количество часов аудиторной работы: 4.

Общий объем самостоятельной работы студента: 4 часа.

Тема 12. Венгерский алгоритм для решения задачи о назначении

Матрица затрат и её свойства. Диагональная редукция матрицы затрат. Венгерский алгоритм для решения задачи о назначении.

Количество часов аудиторной работы: 4.

Общий объем самостоятельной работы студента: 6 часов.

Тема 13. Алгоритм поиска максимального потока в сети

Поток в двухполюсной сети. Величина потока. Разрез сети. Пропускная способность разреза. Теорема Форда-Фалкерсона. Остаточная сеть. Алгоритм поиска максимального потока в двухполюсной сети с помощью остаточной сети.

Количество часов аудиторной работы: 4.

Общий объем самостоятельной работы студента: 4 часа.

Тема 14. Алгоритм поиска максимального потока минимальной стоимости

Стоимость потока в двухполюсной сети. Остаточная сеть. Алгоритм поиска максимального потока минимальной стоимости путем устранения циклов отрицательной стоимости в остаточной сети.

Количество часов аудиторной работы: 4.

Общий объем самостоятельной работы студента: 4 часа.

Тема 15. Транспортная задача

Транспортная задача.

Количество часов аудиторной работы: 4.

Общий объем самостоятельной работы студента: 6 часов.

**Литература по разделу:**

Гагарина Л.Г., Колдаев В.Д. Алгоритмы и структуры данных: учебное пособие. – М.: Финансы и статистика, 2009. – 304 с.

Канцедал С.А. Алгоритмизация и программирование. – М.: Форум: ИНФРА-М, 2010.

Грэхем Р.Л., Кнут Д.Э., Паташник О. Конкретная математика. Математические основы информатики: пер. с англ. – М.: Вильямс, 2013.

1. Раздел 3. Алгоритмы теории расписаний

Тема 16. Алгоритмы теории расписаний для независимых заданий

Построение расписания минимальной стоимости для независимых заданий и одного исполнителя. Построение расписания минимальной длительности с прерываниями для независимых заданий. Ленточная стратегия. Диаграммы Ганта.

Количество часов аудиторной работы: 4.

Общий объем самостоятельной работы: 4 часа.

Тема 17. Алгоритмы теории расписаний для зависимых единичных заданий.

Построение расписания минимальной длительности без прерываний для заданий с графом зависимости в виде ориентированного корневого дерева. Построение расписания минимальной длительности без прерываний с двумя исполнителями для единичных заданий с произвольным орграфом зависимости. Уровневая стратегия.

Количество часов аудиторной работы: 4.

Общий объем самостоятельной работы: 4 часа.

Тема 18. Алгоритмы теории расписаний для зависимых заданий произвольной длительности

Построение расписания минимальной длительности с прерываниями для заданий произвольной длительности с произвольным орграфом зависимости. Уровневая стратегия с лексикографическим упорядочением.

Количество часов аудиторной работы: 4.

Общий объем самостоятельной работы: 6 часов.

Тема 19. Алгоритмы теории расписаний для исполнителей с разной производительностью

Построение расписания минимальной длительности с прерываниями для независимых заданий произвольной длительности и для исполнителей с разной производительностью.

Количество часов аудиторной работы: 4.

Общий объем самостоятельной работы: 6 часов.

Тема 20. Конвейерная задача

Построение расписания минимальной длительности для независимых двухэтапных заданий произвольной длительности и двух исполнителей (конвейерная задача). Алгоритм Джонсона.

Количество часов аудиторной работы: 4.

Общий объем самостоятельной работы: 4 часа.

**Литература по разделу:**

Гагарина Л.Г., Колдаев В.Д. Алгоритмы и структуры данных: учебное пособие. – М.: Финансы и статистика, 2009. – 304 с.

Ахо А., Хопкрофт Дж., Ульман Дж. Структуры данных и алгоритмы. – М.: Вильямс, 2010.

Кормен Т., Лейзерсон Ч., Ривест Р., Штайн К. Алгоритмы: построение и анализ. – М.: Вильямс, 2012.

1. Раздел 4. Алгоритмы комбинаторной оптимизации

Тема 21. Динамическое программирование

Принцип Бэллмана и метод динамического программирования. Примеры и оценка сложности алгоритмов комбинаторной оптимизации, основанных на методе динамического программирования.

Количество часов аудиторной работы: 4.

Общий объем самостоятельной работы: 6 часов.

Тема 22. Дискретная задача оптимального распределения инвестиций

Полиномиальный алгоритм оптимального дискретного распределения инвестиций на основе метода динамического программирования. Комбинаторная оценка его сложности.

Количество часов аудиторной работы: 4.

Общий объем самостоятельной работы: 4 часа.

Тема 23. Метод ветвей и границ

Метод ветвей и границ. Алгоритмы для решения задачи о рюкзаке и задачи коммивояжера на основе метода ветвей и границ. Алгоритм Литтла.

Количество часов аудиторной работы: 4.

Общий объем самостоятельной работы: 6 часов.

Тема 24. Сведение задач комбинаторной оптимизации к задачам на потоки

Возможность сведения некоторых задач комбинаторной оптимизации к задачам на потоки. Решение задач о кратчайших путях в графе, о максимальном паросочетании и задачи о назначении с помощью потоковых алгоритмов.

Количество часов аудиторной работы: 4.

Общий объем самостоятельной работы: 4 часа

**Литература по разделу:**

Гагарина Л.Г., Колдаев В.Д. Алгоритмы и структуры данных: учебное пособие. – М.: Финансы и статистика, 2009.

Канцедал С.А. Алгоритмизация и программирование. – М.: Форум: ИНФРА-М, 2010.

Кормен Т., Лейзерсон Ч., Ривест Р., Штайн К. Алгоритмы: построение и анализ. – М.: Вильямс, 2012.

Сигал И.Х., Иванова А.П. Введение в прикладное дискретное программирование: модели и вычислительные алгоритмы: Учеб. пособие. – М.: ФИЗМАТЛИТ, 2002.

1. Раздел 5. Криптографические алгоритмы

Тема 25. Целочисленные алгоритмы в кольцах вычетов и конечных полях

Булевы криптофункции. Сложение, вычитание, умножение, обращение, деление в кольце целых чисел. Сложность операций. Быстрое возведение в степень.

Количество часов аудиторной работы: 4.

Общий объем самостоятельной работы студента: 4 часа.

Тема 26. Проверка чисел на простоту. Построение больших простых чисел

Методы проверки чисел на простоту: критерий Вильсона, тест на основе малой теоремы Ферма, тест Соловея-Штрассена, тест Рабина-Миллера. Построение больших простых чисел.

Количество часов аудиторной работы: 4.

Общий объем самостоятельной работы студента: 4 часа.

Тема 27. Алгоритмы факторизации

Методы факторизации: метод Полларда, факторизация Ферма, алгоритм Диксона, метод квадратичного решета.

Количество часов аудиторной работы: 4.

Общий объем самостоятельной работы студента: 4 часа.

Тема 28. Криптографические системы

Криптографическая система RSA. Протокол Диффи-Хеллмана. Выбор параметров системы RSA.

Количество часов аудиторной работы: 4.

Общий объем самостоятельной работы: 6 часов.

Тема 29. Методы криптоанализа

Частотный анализ. Стойкость RSA против метода повторного шифрования. Поиск секретного ключа *d* и факторизация модуля *N*.

Количество часов аудиторной работы: 4.

Общий объем самостоятельной работы: 6 часов.

**Литература по разделу:**

Гагарина Л.Г., Колдаев В.Д. Алгоритмы и структуры данных: учебное пособие. – М.: Финансы и статистика, 2009.

Домашев А.В. и др. Программирование алгоритмов защиты информации: Учеб. пособие. – 2-е изд., исправл. и доп. – М.: Издатель Молгачева С.В., Издательство «Нолидж»Ю, 2002.

1. Приближенные алгоритмы и эвристики

Тема 30. Приближенные алгоритмы и эвристики для решения задачи о рюкзаке

Эвристики и приближенный алгоритм для задачи о рюкзаке с гарантированной погрешностью. Точный полиномиальный алгоритм для задачи о сверхвозрастающем рюкзаке.

Количество часов аудиторной работы: 4.

Общий объем самостоятельной работы студента: 4 часа.

Тема 31. Точные и приближенные алгоритмы для решения задачи коммивояжера

Эвристики для решения задачи коммивояжера. Приближенный алгоритм Кристофидиса для евклидовой задачи коммивояжера с гарантированной точностью.

Количество часов аудиторной работы: 4.

Общий объем самостоятельной работы студента: 4 часа.

Тема 32. Генетические алгоритмы

Общая схема и параметры генетического алгоритма. Операторы скрещивания, мутации и отбора. Решение задачи коммивояжера, задачи о рюкзаке и непрерывной задачи об оптимальном распределении инвестиций с помощью генетического алгоритма. Криптоанализ шифра с помощью генетического алгоритма.

Количество часов аудиторной работы: 12.

Общий объем самостоятельной работы студента: 16 часов.

**Литература по разделу:**

Гагарина Л.Г., Колдаев В.Д. Алгоритмы и структуры данных: учебное пособие. – М.: Финансы и статистика, 2009.

Гладков Л.А., Курейчик В.В., Курейчик В.М. Генетические алгоритмы / Под ред. В.М.Курейчика. – 2-е изд., исправл. и доп. – М.: ФИЗМАТЛИТ, 2010.

# Образовательные технологии

На практических занятиях студенты работают в мини-группах по 3-4 человека в компьютерном классе. Задача группы, как правило, разработать программный продукт на основе одного из алгоритмов, изучаемых в данном курсе, подготовить набор тестов и выполнить тестирование разработанного программного продукта на этом наборе тестов.

## Методические рекомендации преподавателю

На лекциях рекомендуется иллюстрировать материал примерами, показывающими все этапы решения задачи: формализацию и построение математической модели, разработку алгоритма, доказательство его корректности, нахождение его сложности, написание программы, её отладку и тестирование, выполнение программы на реальных входных данных.

На практических занятиях используются следующие методы обучения и контроля усвоения материала: разработка алгоритмов для конкретных задач и их практическая реализация в виде программного продукта с последующей отладкой и тестированием.

При оценке выполненных заданий особое внимание рекомендуется обратить на оценки разработанных программ (получение теоретических оценок, сравнение проведенных экспериментов с результатами, полученными различными способами).

## Методические указания студентам

Студенту рекомендуется следующая схема выполнения домашних заданий:

* проработать конспект лекций;
* проанализировать основную и дополнительную литературу, рекомендованную по изучаемому разделу;
* проанализировать варианты решений, предложенные преподавателем на практических занятиях;
* при затруднениях сформулировать вопросы к преподавателю.

При подготовке рекомендуется использовать электронные учебные материалы, имеющиеся в медиатеке.

Выполненные задания должны сопровождаться данными анализа результатов (теоретическими оценками, сравнением результатов, полученных различными способами).

# Оценочные средства для текущего контроля и аттестации студента

## Тематика заданий текущего контроля

Примерные задания для контрольной работы:

1. Решить систему рекуррентных уравнений



1. Решить рекуррентное уравнение

.

1. С помощью полиномиальной производящей функции решить рекуррентное уравнение

.

1. Используя первую теорему Пойа, найти количество различных раскрасок *граней* плоского графа (включая *внешнюю грань*) с помощью трех красок

а) с группой автоморфизмов *на плоскости*;

б) с группой автоморфизмов *в пространстве*.

1. Вершины графа раскрашивают в два цвета так, что 2 вершины оказываются покрашенными в один цвет, а остальные 4 – в другой цвет. Используя вторую теорему Пойа, найти число различных (с точностью до автоморфизма *в пространстве*) раскрасок вершин графа.

Примерные задания для домашнего задания №1:

1. Найти максимальный поток минимальной стоимости в двухполюсной сети:

|  |  |  |
| --- | --- | --- |
| *Дуга* | *Пропускная способность* | *Стоимость* |
| *s → 1* | 2 | 1 |
| *s → 2* | 4 | 2 |
| *s → 3* | 3 | 4 |
| *1 → 3* | 1 | 2 |
| *1 → 4* | 2 | 2 |
| *2 → 4* | 2 | 3 |
| *2 → t* | 1 | 3 |
| *3 → t* | 3 | 2 |
| *4 → t* | 3 | 1 |

1. Составить минимальное расписание без прерываний для 3 исполнителей и системы заданий с отношением предшествования, заданного орграфом. Ответ записать в виде диаграммы Ганта.

3

2

1

4

3

3

2

4

2

Примерные задания для домашнего задания №2:

1. С помощью венгерского алгоритма решить задачу о назначении для заданной матрицы стоимостей работ:



1. С помощью алгоритма Литтла решить задачу коммивояжера для матрицы расстояний:

3



1. На основе метода ветвей и границ разработать алгоритм и написать программу, а также подготовить набор тестов и проверить с их помощью программу для решения задачи о рюкзаке. Требуется найти такой вариант заполнения рюкзака, при котором суммарная стоимость положенных в него предметов является максимально возможной. Тестовый вариант задачи: имеется рюкзак, вместимость которого равна 11, а веса и стоимости предметов указаны в таблице:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| *Вес* | 2 | 3 | 6 | 4 | 5 |
| *Стоимость* | 6 | 7 | 8 | 9 | 10 |

## Вопросы для оценки качества освоения дисциплины

1. Однородные системы линейных рекуррентных соотношений с постоянными коэффициентами, их решение методом исключения неизвестных, примеры.
2. Однородные системы линейных рекуррентных соотношений с постоянными коэффициентами, их решение матричным методом, примеры.
3. Неоднородные рекуррентные соотношения, пример нахождения хроматического многочлена для графа-цикла.
4. Полиномиальные производящие функции, примеры полиномиальных производящих функций для простейших последовательностей.
5. Решение рекуррентных соотношения с переменными коэффициентами с помощью полиномиальных производящих функций, примеры.
6. Операции над полиномиальными производящими функциями, свертка.
7. Экспоненциальные производящие функции, вывод верхней оценки для сложности вычисления детерминанта «по определению» и разложением по строке.
8. Симметрическая группа подстановок, теорема Бернсайда, задача об ожерелье на плоскости и в пространстве.
9. Разложение подстановки в произведение циклов, цикловой индекс подстановки и группы подстановок, первая теорема Пойа.
10. Вторая теорема Пойа, задача об окраске граней куба.
11. Задача о числе неэквивалентных химических деревьев и о числе различных булевых функций от *n* аргументов.
12. Максимальное паросочетание, теорема Бержа, алгоритм чередующихся цепей, метод «волны» для поиска чередующихся цепей в двудольном графе.
13. Совершенное паросочетание, теорема Холла, метод «волны» для поиска чередующихся деревьев, поиск совершенного паросочетания в двудольном графе.
14. Потоки в сетях, задача о максимальном потоке, разрез сети, теорема Форда–Фолкерсона.
15. Остаточная сеть, её использование для поиска максимального потока в двухполюсной сети.
16. Задача о максимальном потоке минимальной стоимости, остаточная сеть, метод удаления циклов отрицательной стоимости в остаточной сети.
17. Задача о назначениях, венгерский алгоритм.
18. Полиномиальные алгоритмы из теории расписаний: построение расписания минимальной стоимости для независимых заданий и одного исполнителя.
19. Полиномиальные алгоритмы из теории расписаний: построение расписания минимальной длительности для единичных заданий с древовидным графом предшествования.
20. Полиномиальные алгоритмы из теории расписаний: построение расписания минимальной длительности с прерываниями для независимых заданий.
21. Задача о рюкзаке. Метод ветвей и границ для точного решения задачи о рюкзаке (два способа ветвления).
22. Задача о рюкзаке. Приближенный алгоритм для задачи о рюкзаке с гарантированной погрешностью.
23. Задача коммивояжера. Метод ветвей и границ, алгоритм Литтла.
24. Задача коммивояжера. Приближенные алгоритмы. Алгоритм Кристофидиса.
25. Точные и «жадные» алгоритмы и эвристики.
26. Общая схема, операторы и параметры генетического алгоритма. Решение задачи коммивояжера с помощью генетического алгоритма.
27. Оценка эффективности комбинаторного алгоритма, полиномиальные и экспоненциальные алгоритмы, их принципиальные отличия.
28. Нижние оценки сложности комбинаторных алгоритмов. Методы их доказательства. Оптимальные алгоритмы сортировки и поиска.
29. Элементарные методы проверки простоты чисел: метод проб, решето Эратосфена, метод Ферма.
30. Алгоритм Евклида. НОД и НОК, их свойства.
31. Сравнения, их свойства. Классы вычетов. Полная система вычетов. Обратный мультипликативный элемент.
32. Функция Эйлера. Малая теорема Ферма. Теорема Эйлера.
33. Системы линейных сравнений. Китайская теорема об остатках.
34. Криптографическая система RSA. Выбор параметров системы RSA.
35. Возможные атаки на криптосистему RSA.

# Учебно-методическое и информационное обеспечение дисциплины

## Базовый учебник

Гагарина Л.Г., Колдаев В.Д. Алгоритмы и структуры данных: учебное пособие. – М.: Финансы и статистика, 2009.

## Основная литература

1. Канцедал С.А. Алгоритмизация и программирование. – М.: Форум: ИНФРА-М, 2010.
2. Грэхем Р.Л., Кнут Д.Э., Паташник О. Конкретная математика. Математические основы информатики: пер. с англ. – М.: Вильямс, 2013.

## Дополнительная литература

1. Ахо А., Хопкрофт Дж., Ульман Дж. Структуры данных и алгоритмы. – М.: Вильямс, 2010.
2. Гладков Л.А., Курейчик В.В., Курейчик В.М. Генетические алгоритмы / Под ред. В.М.Курейчика. – 2-е изд., исправл. и доп. – М.: ФИЗМАТЛИТ, 2010.
3. Домашев А.В. и др. Программирование алгоритмов защиты информации: Учеб. пособие. – 2-е изд., исправл. и доп. – М.: Издатель Молгачева С.В., Издательство «Нолидж»Ю, 2002.
4. Кормен Т., Лейзерсон Ч., Ривест Р., Штайн К. Алгоритмы: построение и анализ. – М.: Вильямс, 2012.
5. Левитин А.В. Алгоритмы: введение в разработку и анализ. – М.: Вильямс, 2006.
6. Сигал И.Х., Иванова А.П. Введение в прикладное дискретное программирование: модели и вычислительные алгоритмы: Учеб. пособие. – М.: ФИЗМАТЛИТ, 2002.

## Справочники, словари, энциклопедии

Не предусмотрены.

## Программные средства

Для успешного освоения дисциплины, студент использует следующие программные средства:

* Microsoft Visual Studio 2010/2013.
* Microsoft Office.

## Дистанционная поддержка дисциплины

Дистанционная поддержка курса предусмотрена в рамках информационной образовательной среды LMS.

# Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий используется компьютер с установленным программным обеспечением для демонстрации презентаций и проектор. Практические занятия проводятся в компьютерных классах с установленным программным обеспечением, перечисленным выше.