

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования

«СЕВЕРО-ВОСТОЧНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ ИМЕНИ М.К. АММОСОВА»
Политехнический институт (филиал) ФГАОУ ВО «Северо-Восточный федеральный университет
имени М.К. Аммосова» в г. Мирном.
Кафедра фундаментальной и прикладной математики

Рабочая программа дисциплины

Б1.О.31 Компьютерная графика

для программы бакалавриата

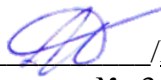
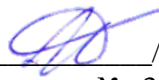

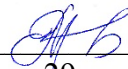
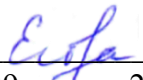
по направлению подготовки

01.03.02. Прикладная математика и информатика

Профиль подготовки: Математическое моделирование и вычислительная математика

Форма обучения: Очная

Автор: Якушев Илья Анатольевич, к.ф.-м.н., доцент кафедры фундаментальной и прикладной математики, МПТИ (ф)СВФУ, Yakushevilya@mail.ru

РЕКОМЕНДОВАНО Заведующий кафедрой фундаментальной и прикладной математики  _____/Гадоев М.Г. протокол № <u>3</u> от «22» февраля 2019 г.	ОДОБРЕНО Заведующий кафедрой фундаментальной и прикладной математики  _____/Гадоев М.Г. протокол № <u>3</u> от «22» февраля 2019 г.	ПРОВЕРЕНО Нормоконтроль в составе ОП пройден Ст.диспетчер УМО  _____/ Баишева О.Ю. «28» марта 2019 г.
Рекомендовано к утверждению в составе ОП Председатель УМС  /Константинова Т.П./ протокол УМС № <u>3</u> от «29» марта 2019 г.		Эксперт УМС  / Егорова М.В. «29» марта 2019 г.

Мирный 2019

АННОТАЦИЯ
к рабочей программе дисциплины
Б1.О.31 Компьютерная графика
Трудоемкость 4 з.е.

1.1. Цель освоения и краткое содержание дисциплины

Цель освоения: Целями преподавания дисциплины являются:

- освоение студентами методов компьютерной геометрии, растровой и векторной графики;
- приобретение навыков самостоятельного изучения отдельных тем дисциплины и решения типовых задач;
- приобретение навыков работы с графическими библиотеками и в современных графических пакетах и системах;
- усвоение полученных знаний студентами, а также формирование у них мотивации к самообразованию за счет активизации самостоятельной познавательной деятельности.

Краткое содержание дисциплины: Области применения компьютерной графики; тенденции построения современных графических систем; стандарты в области разработки графических систем; технические средства компьютерной графики; графические процессоры, аппаратная реализация графических функций; понятие конвейеров ввода и вывода графической информации; системы координат, типы преобразований графической информации; форматы хранения графической информации; принципы построения “открытых” графических систем; 2D и 3D моделирование в рамках графических систем; проблемы геометрического моделирования; виды геометрических моделей их свойства, параметризация моделей; геометрические операции над моделями; алгоритмы визуализации: отсечения, развертки, удаления невидимых линий и поверхностей, закраски; способы создания фотореалистических изображений; основные функциональные возможности современных графических систем; организация диалога в графических системах; классификация и обзор современных графических систем.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Наименование категории (группы) компетенций	Планируемые результаты освоения программы (код и содержание компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения по дисциплине	Оценочные средства
Информационно-коммуникационные технологии для профессиональной деятельности	ОПК-4 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-4.1. Проявляет владение базовыми знаниями по защите информации на рабочем месте и при входе в локальные и глобальные сети. ОПК-4.2. Демонстрирует навыки использования научных и образовательных ресурсов сети Интернет для разработки программ и	Знать: основы безопасности вычислительных систем, необходимые для решения задач профессиональной деятельности. Уметь: применять знания безопасности вычислительных систем для решения задач профессиональной деятельности; Владеть: навыками анализа и оценки архитектуры вычислительных сетей и ее	Выполнение практических заданий, тест, устный опрос

		<p>программной документации с учетом требований информационно й безопасности. ОПК-4.3. Демонстрирует умение использовать основные методы передачи, обработки и хранения информации, от которых зависит компьютерная безопасность. ОПК-4.4. Демонстрирует умение составлять научные обзоры, рефераты и библиографии по тематике научных исследований.</p>	<p>компонентов, информационных процессов, показателей качества и эффективности функционирования , методами защиты информации в компьютерных сетях.</p>	
--	--	--	--	--

1.3. Место дисциплины в структуре ОПОП

Индекс	Наименование дисциплины (модуля), практики	Семестр изучения	Индексы и наименования учебных дисциплин (модулей), практик	
			на которые опирается содержание данной дисциплины (модуля)	для которых содержание данной дисциплины (модуля) выступает опорой
Б1.О.31	Компьютерная графика	4	Б1.О.27 Операционные системы	Б1.О.35 Системы программирования Б1.В.ДВ.08.02 Защита информации

1.4. Язык преподавания: Русский

2. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Выписка из учебного плана:

Код и название дисциплины по учебному плану	Б1.О.31 Компьютерная графика	
Курс изучения	2	
Семестр(ы) изучения	4	
Форма промежуточной аттестации (зачет/экзамен)	Экзамен	
Курсовой проект/ курсовая работа (указать вид работы при наличии в учебном плане), семестр выполнения	-	
Трудоемкость (в ЗЕТ)	4	
Трудоемкость (в часах) (сумма строк 1, 2, 3), в т.ч.:	144	
1. Контактная работа обучающихся с преподавателем (КР):	Объем аудиторной работы (в часах)	В том числе с применением ЭО или ДОТ (в часах)
Объем аудиторной работы (в часах) (1.1.+1.2.+1.3.):	76	
1.1. Занятия лекционного типа (лекции)	36	
1.2. Занятия семинарского типа, всего, в т.ч.:		
- практические занятия (семинары, коллоквиумы)		
- лабораторные работы	36	
- практикумы		
1.3. КСР (контроль самостоятельной работы)	4	
2. Самостоятельная работа обучающихся (СРС) (в часах)	41	
3. Количество часов на экзамен (при наличии экзамена в учебном плане)	27	

3. Содержание дисциплины, структурированное по темам с указанием отведенного на них количества академических часов и видов учебных занятий

3.1. Распределение часов по темам и видам учебных занятий

Тема	Всего часов	Контактная работа, в часах									Часы СРС
		Лекции	из них с применением ЭО и ДОТ	Семинары (практические занятия, коллоквиумы)	из них с применением ЭО и ДОТ	Лабораторные работы	из них с применением ЭО и ДОТ	Практикумы	из них с применением ЭО и ДОТ	КСР (консультации)	
1.Формулы Хартли. Равномерные коды.	12	4				4					4
2.Энтропийный подход к измерению информации	13	4				4				1	4
3.Эффективное кодирование	12	4				4					4
4.Взаимная информация о компонентах сложной системы	13	4				4				1	4
5.Общая характеристика помехоустойчивых кодов	13	4				4					5
6.Коды Хэмминга	14	4				4				1	5
7.Классификация методов защиты	13	4				4					5
8.Использование простейших шифров	14	4				4				1	5
9.Односторонние функции и математические методы защиты	13	4				4					5
Всего часов	117	36				36				4	41

3.2. Содержание тем программы дисциплины

Модуль 1. Измерение информации. Эффективное кодирование

Тема 1.1. Формулы Хартли. Равномерные коды

Единица измерения информации. Формула Хартли в экспоненциальной форме. Формула Хартли в логарифмической форме. Понятие о кодировании. Равномерный код и его длина. Использование равномерных кодов для кодирования информации различного вида (символьная, строковая, цвет, рисунок, аудио и т.д.). Вычисление объема информации в тексте, рисунке, аудиофайле и т.п. в задачах из КИМов ЕГЭ по информатике.

Тема 1.2. Энтропийный подход к измерению информации

Физические системы с конечным числом не равновероятных состояний. Закон распределения для системы. Понятие энтропии. Функция $\eta(x)$ и ее свойства. Максимум энтропии при заданном

количестве состояний. Количество информации в сообщении о состояниях системы – формула Шеннона.

Тема 1.3. Эффективное кодирование

Схема Шеннона для процесса передачи информации. Характеристики источника и канала связи. Первая теорема Шеннона. Понятие о префиксном кодировании. Процедура Шеннона-Фано для построения эффективного префиксного кода. Процедура Хаффмана. Математические основы алгоритмов работы архиваторов (сталкеров).

Модуль 2. Помехоустойчивое кодирование

Тема 2.1. Взаимная информация о компонентах сложной системы

Закон распределения сложной системы. Восстановление законов распределения компонент по закону сложной системы. Условные распределения. Виды зависимостей между компонентами и интуитивное представление о количестве информации о недоступной системе в наблюдениях за доступной системой, связанной с недоступной для непосредственного наблюдения. Условная энтропия, полная условная энтропия. Количество взаимной информации.

Тема 2.2. Общая характеристика помехоустойчивых кодов

Зашумленность канала связи. Характеристическая матрица вероятностей преобразования символов в зашумленном канале. Вторая теорема Шеннона. Классификация помехоустойчивых кодов. Обнаруживающие и корректирующие способности помехоустойчивых кодов. Простейшие примеры помехоустойчивых кодов.

Тема 2.3. Коды Хэмминга

Построение кода Хэмминга автоматически обнаруживающего и исправляющего одну ошибку кода. Построение диагностического инструмента – синдрома ошибки. Понятие о кодах BCH (Боуза-Чоудхури-Хоквингема).

Модуль 3. Защита информации

Тема 3.1. Классификация методов защиты

Понятие о защите информации в канале связи от противника. Основные направления борьбы с перехватом информации в канале связи. Стеганографические методы защиты информации. Криптографические методы защиты информации.

Тема 3.2. Использование простейших шифров

Шифры замены, их математические свойства. Методы перестановки, их свойства. Комбинированные методы. Классические шифры (Цезаря, атбаш, сцигаль, четный квадратный, Вижинера, масонов и т.д.).

Тема 3.3. Односторонние функции. Математические методы защиты

Понятие об односторонней функции. Шифр RSA (Райвест, Шамир, Эйдельман). Понятие о хэш-функции. Электронные подписи. Основы безопасной работы в сети Internet.

6. Планы семинарских занятий

На семинарских занятиях рассматриваются следующие проблемы:

- решаются задачи КИМов ЕГЭ по информатике, имеющие тематическое соприкосновение с материалом дисциплины (измерение информации, кодирование, вопросы передачи информации и др.);
- задачи на построение эффективных префиксных кодов по методу Шеннона-Фано с примыкающими задачами (вычисление средней длины бинарного кода на символ входного алфавита, вычисление энтропии источника, аналогичные построения для кодирования блоков по два-три символа входного алфавита);
- задачи на построение эффективных префиксных кодов по методу Хаффмана с примыкающими задачами (вычисление средней длины бинарного кода на символ входного алфавита, вычисление энтропии источника, аналогичные построения для кодирования блоков по два-три символа входного алфавита);
- вычисление количества информации для сложных систем с предварительным построением закона распределения;
- построение кода Хэмминга по заданному информационному сообщению в бинарном коде;
- построение синдрома ошибки по коду Хэмминга и коррекция кода;
- решение задач на использование различных методов шифровки и дешифровки.

Приведем пример некоторых планов практических занятий

Практическое занятие

ТЕМА: "Измерение информации. Равномерное кодирование"

- I. Вопросы для обсуждения
- Единицы измерения информации.
 - Формула Хартли.
 - Формула Шеннона.
 - Энтропийный подход к измерению информации.
 - Длина равномерного кода.
 - Кодирование символов, цвета, текста, рисунков, чисел.
 - Объемы файлов.
- II. Задачи для решения в аудитории (типовые примеры, необходимо расширить списком аналогичных из КИМов ЕГЭ)
1. Состояние морского аквариума контролируется сорока пятью датчиками. Наименьшее количество двоичных разрядов, необходимое для идентификации этих датчиков равно
 2. В велокроссе участвуют 119 спортсменов. Специальное устройство регистрирует прохождение каждым из участников промежуточного финиша, записывая его номер с использованием минимально возможного количества бит, одинакового для каждого спортсмена. Каков информационный объем сообщения, записанного устройством, после того как промежуточный финиш прошли 70 велосипедистов?
 3. В некоторой стране автомобильный номер длиной 6 символов составляют из заглавных букв (используются только 33 буквы) и десятичных цифр в любом порядке. Каждый такой номер в компьютерной программе записывается минимально возможным и одинаковым целым количеством байтов (при этом используют посимвольное кодирование и все символы кодируются одинаковым и минимально возможным количеством битов). Определите объем памяти, отводимый этой программой для записи 125 номеров.
 4. Световое табло состоит из светящихся элементов, каждый из которых может гореть одним из четырех различных цветов. Сколько различных сигналов можно передать при помощи табло, состоящего из пяти таких элементов (при условии, что все элементы должны гореть)?
 5. Скорость передачи данных через ADSL-соединение равна 128000 бит/с. Через соединение передают файл размером 625 Кбайт. Определите время передачи файла в секундах.
 6. В княжестве Блэквайтия имеются автомобили только черного, серого и белого цвета. Информационный объем сообщения "В аварию попал автомобиль не черного цвета" равен $8 - \log_2 5$ бит. Количество информации, содержащееся в сообщении "В аварию попал серый автомобиль", равно 8 бит. Количество бит информации в сообщении "В аварию попал автомобиль белого цвета" равно ____.
- Remark:* Задача № 6 взята из демонстрационного варианта материалов централизованного тестирования по информатике (предшественник ЕГЭ) представленный Центром тестирования при Министерстве образования РФ в 2004 году (тест № 00, задача B2). Авторский ответ к задаче – 6 бит. Разберите решение, найдите правильный ответ и объясните причины многочисленных ошибок централизованного тестирования, возникающих при решении аналогичных задач.
- III. Домашнее задание
- Теория:* Кодирование информации различного вида
- Практика:* Построить таблицу функции $\eta(x)$ с двумя входами (десятые / сотые) с точностью до 0,0001.

Практическое занятие

ТЕМА: "Кодирование информации различного вида"

- I. Вопросы для обсуждения
- Кодирование символьной информации (ASCII, Windows, КОИ, ГОСТ, UNICODE и др.)
 - Кодирование целых чисел, дополнительный код. Кодирование чисел типа Single.
 - Выполнение операций бинарной арифметики с целыми числами (not, and, or, xor, shr, shl, imp, eqv).
 - Кодирование цветов в различных технологиях (RGB, CMYK и др.).
 - Кодирование растровой графики (формат *.bmp).
 - Понятие о кодировании аудиоинформации.

II. Задачи для решения в аудитории (указаны примерные шаблоны решаемых задач, следует наполнить их конкретным содержанием)

1. Известна скорость накопления информации. Найти время необходимое для накопления заданного объема информации (накопление может производиться несколькими объектами).
2. Известен объем сохраняемой информации и плотность ее размещения на носителе конкретного вида. Найти характеристики носителя.
3. Выполнить операции бинарной арифметики над целыми числами.
4. Решение задач из КИМов ЕГЭ по информатике о цвете, заданном тегом bgcolor.
5. Оценка объемов графических растровых файлов и аналогичные задачи.

III. Домашнее задание

Теория: Вопросы эффективного кодирования.

Практика: Задачи, аналогичные задачам, решенным в аудитории.

Практическое занятие

ТЕМА: "Вопросы эффективного кодирования"

I. Вопросы для обсуждения

- Недостатки равномерного кодирования
- Префиксные коды. Недостатки неравномерного кодирования.
- Понятие эффективного кода.
- Алгоритм Шеннона-Фано. Недостатки алгоритма Шеннона-Фано.
- Алгоритм Хаффмана построения эффективного префиксного кода.
- Средняя длина кодовой последовательности на один символ входного алфавита.
- Первая теорема Шеннона.
- Способы уменьшения средней длины кода, использование этих способов в работе архиваторов.

II. Задачи для решения в аудитории (указан универсальный шаблон рассматриваемых задач, наполнить его конкретным содержанием можно используя электронные генераторы задач – специально созданные программы в Delphi /В.Н. Алексеев/)

1. Задан входной алфавит z_1, z_2, \dots, z_n и соответствующие частоты их встречи в исходном тексте:

- а) Найти длину равномерного кода.
- б) Используя таблицу $\eta(x)$ вычислить энтропию исходного текста.
- в) Используя алгоритм Шеннона-Фано построить эффективный префиксный код входного алфавита и вычислить среднюю длину бинарного кода на символ входного алфавита.
- г) Используя алгоритм Хаффмана построить эффективный префиксный код входного алфавита и вычислить среднюю длину бинарного кода на символ входного алфавита.
- е) (для небольших алфавитов – демонстрация принципа работы "сталкеров") Считая для простоты вероятности появления символов независимыми вычислить частоты появления пар символов и построить для них эффективный префиксный код по любому из алгоритмов, после чего вычислить среднюю длину бинарного кода на символ входного алфавита.

III. Домашнее задание

Теория: Помехоустойчивое кодирование

Практика: Решение задач, аналогичных задачам, решенным в аудитории

Практическое занятие

ТЕМА: "Помехоустойчивое кодирование. Защита информации от противника, методы защиты"

I. Вопросы для обсуждения

- Характеристика зашумленности канала.
- Классификация помехоустойчивых кодов.
- Характеристики помехоустойчивых кодов
- Коды с проверкой на четность.
- Рефлективные коды.
- Блочные разделимые коды.
- Код Хэмминга.
- Синдром ошибки в кодах Хэмминга.
- Стеганографические методы защиты информации от противника.

- Простейшие криптографические методы защиты информации.
- Понятие one way function.
- Шифрование с открытым ключом.

II. Задачи для решения в аудитории (расширить список решаемых задач аналогичными задачами)

1. Построить коды Хэмминга для бинарных информационных последовательностей заданной длины.
2. Вычислить синдром ошибки для заданных кодов Хэмминга и исправить ошибку, если синдром не нулевой.
3. Произвести шифровку / дешифровку сообщений заданным способом (решение разнообразных задач на использование шифров).
4. Решение задач из демоверсий ЕГЭ по информатике, связанных с использованием кодирования / шифрования или декодирования / расшифровки.

III. Домашнее задание

Теория: Помехоустойчивое кодирование

Практика: Решение задач, аналогичных задачам, решенным в аудитории

3.3. Формы и методы проведения занятий, применяемые учебные технологии

При проведении занятий применяется игровое проектирование, компьютерная симуляция, дискуссия.

4. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Содержание СРС

№	Наименование раздела (темы) дисциплины	Вид СРС	Трудоемкость (в часах)	Формы и методы контроля
1	1.Формулы Хартли. Равномерные коды.	Выполнение домашних заданий, решение контрольных работ	4	Оценка по БРС
2	2.Энтропийный подход к измерению информации	Выполнение домашних заданий, решение контрольных работ	4	Оценка по БРС
3	3.Эффективное кодирование	Выполнение домашних заданий, решение контрольных работ	4	Оценка по БРС
4	4.Взаимная информация о компонентах сложной системы	Выполнение домашних заданий, решение контрольных работ	4	Оценка по БРС
5	5.Общая характеристика помехоустойчивых кодов	Выполнение домашних заданий, решение контрольных работ	5	Оценка по БРС
6	6.Коды Хэмминга	Выполнение домашних заданий, решение контрольных работ	5	Оценка по БРС
7	7.Классификация методов защиты	Выполнение домашних заданий, решение контрольных работ	5	Оценка по БРС
8	8.Использование простейших шифров	Выполнение домашних заданий, решение контрольных работ	5	Оценка по БРС
9	9.Односторонние функции и математические методы защиты	Выполнение домашних заданий, решение контрольных работ	5	Оценка по БРС
	Всего часов		41	

Лабораторные работы или лабораторные практикумы (при наличии)

№	Наименование раздела (темы) дисциплины	Лабораторная работа или лабораторный практикум	Трудо-емкость (в часах)	Формы и методы контроля
1	1.Формулы Хартли. Равномерные коды.	Лабораторная работа	4	Оценка по БРС
2	2.Энтропийный подход к измерению информации	Лабораторная работа	4	Оценка по БРС
3	3.Эффективное кодирование	Лабораторная работа	4	Оценка по БРС
4	4.Взаимная информация о компонентах сложной системы	Лабораторная работа	4	Оценка по БРС
5	5.Общая характеристика помехоустойчивых кодов	Лабораторная работа	4	Оценка по БРС
6	6.Коды Хэмминга	Лабораторная работа	4	Оценка по БРС
7	7.Классификация методов защиты	Лабораторная работа	4	Оценка по БРС
8	8.Использование простейших шифров	Лабораторная работа	4	Оценка по БРС
9	9.Односторонние функции и математические методы защиты	Лабораторная работа	4	Оценка по БРС
	Всего часов		36	

5. Методические указания для обучающихся по освоению дисциплины

Рейтинговый регламент по дисциплине:

Вид выполняемой учебной работы (контролирующие мероприятия)	Количество баллов (min)	Количество баллов (max)
Изучение конспекта	10	20
Выполнение домашних заданий	30	40
Подготовка доклада	10	20
Подготовка к контрольной работе	10	20
Количество баллов для допуска к экзамену (min-max)	60	100

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

6.1. Показатели, критерии и шкала оценивания

Коды оцениваемых компетенций	Индикаторы достижения компетенций	Показатель оценивания (дескриптор) (по П.1.2.РПД)	Уровни освоения	Критерий оценивания	Оценка
ОПК-4	ОПК-4.1.	Знать: основы	Высокий	Знает: Теоретические основы измерения	отлично

	<p>Проявляет владение базовыми знаниями по защите информации на рабочем месте и при входе в локальные и глобальные сети.</p> <p>ОПК-4.2. Демонстрирует навыки использования научных и образовательных ресурсов сети Интернет для разработки программ и программной документации с учетом требований информационно й безопасности.</p> <p>ОПК-4.3. Демонстрирует умение использовать основные методы передачи, обработки и хранения информации, от которых зависит компьютерная безопасность.</p> <p>ОПК-4.4. Демонстрирует умение составлять научные обзоры, рефераты и библиографии по тематике научных исследований.</p>	<p>безопасности вычислительных систем, необходимые для решения задач профессиональной деятельности.</p> <p>Уметь: применять знания безопасности вычислительных систем для решения задач профессиональной деятельности;</p> <p>Владеть: навыками анализа и оценки архитектуры вычислительных сетей и ее компонентов, информационных процессов, показателей качества и функционирования, методами защиты информации в компьютерных сетях.</p>		<p>информации простых и сложных систем, основы эффективного и помехоустойчивого кодирования, основы работы архиваторов</p> <p>Умеет: Решать задачи из КИМов ЕГЭ, решать задачи по дешифровке, строить эффективные префиксные коды, строить коды Хэмминга и синдром ошибок</p> <p>Владеет: Терминологией и основными понятиями дисциплины, методами</p>	
			<p>Базовый</p>	<p>Знает: Теоретические основы измерения информации простых систем, основы эффективного и помехоустойчивого</p>	<p>хорошо</p>

			кодирования Умеет: Решать задачи из КИМов ЕГЭ, решать задачи по дешифровке, строить эффективные префиксные коды Владеет: Терминологией и основными понятиями дисциплины, некоторыми методами	
		Мини-мальный	Знает: Теоретические основы измерения информации простых систем, основы эффективного кодирования Умеет: Решать задачи из КИМов ЕГЭ, решать задачи по дешифровке Владеет: Терминологией и основными понятиями	удовлетворительно
		Не освоены	Студент не имеет представления об основных понятиях раздела и не умеет приводить примеры	неудовлетворительно

6.2. Типовые контрольные задания (вопросы) для промежуточной аттестации
Темы рефератов и курсовых работ

1. Начальные понятия математической лингвистики.
2. Язык БНФ.
3. Язык РБНФ.
4. Синтаксические диаграммы Вирта.
5. Измерение информации в простейших ситуациях. Формулы Хартли.
6. Понятие о равномерных кодах. Длина равномерных кодов.
7. Схема Шеннона. Простейшие характеристики процесса передачи информации.
8. Энтропия системы с конечным набором не равновозможных состояний.
9. Свойства энтропии. Количество информации.
10. Первая теорема Шеннона.
11. Процедура Шеннона-Фано построения эффективных префиксных кодов.
12. Математические принципы работы архиваторов.
13. Энтропия источника и средняя длина кода на символ входного алфавита.
14. Процедура Хаффмана построения эффективных префиксных кодов.
15. Сложная система. Закон распределения для сложной системы.
16. Восстановление закона распределения компонент по закону распределения сложной системы.
17. Условные распределения. Виды связи между компонентами сложной системы.
18. Полная энтропия сложной системы. Полные условные энтропии компонент.
19. Связь полной энтропии с полными условными энтропиями. Количество информации.
20. Вторая теорема Шеннона.
21. Помехоустойчивые коды. Классификация.
22. Простейшие математические понятия для помехоустойчивых кодов.
23. Обнаруживающие и корректирующие способности m, k кодов.
24. Построение кода Хэмминга.

25. Обнаружение и исправление ошибки в кодах Хэмминга.
26. Общее представление о защите информации.
27. Классификация методов защиты информации. Основной принцип стеганографических методов защиты.
28. Характеристика шифровки методом замены. Примеры шифров замены.
29. Характеристика шифровок методами перестановок. Примеры шифров перестановок.
30. Понятие об односторонней функции. Шифр RSA.

В билет на зачете включается теоретический вопрос и два практических задания.

Типы практических заданий

1. Решение заданий из КИМов ЕГЭ по информатике (системы счисления, логика, алгоритмы, задания на кодирование, вычисление объема информации и т.п.);
2. Построение эффективных префиксных кодов по методу Шеннона-Фано. Определение средней длины бинарного кода на символ входного алфавита;
3. Построение эффективных префиксных кодов по методу Хаффмана. Определение средней длины бинарного кода на символ входного алфавита;
4. Построение кода Хэмминга по информационной части сообщения.
5. Вычисление синдрома ошибки в коде Хэмминга.
6. Использование простейших методов шифрования.

6.3. Методические материалы, определяющие процедуру оценивания

Оценивание отдельных контрольных точек учебного процесса осуществляется по технологии рейтинговой оценки с использованием идеи сведения многокритериальной оптимизационной задачи к однокритериальной за счет декомпозиции контрольной точки (естественное разложение по заданиям) с использованием весовых коэффициентов, учитывающих важность задания в комплексной подготовке профессионального учителя информатики.

Дисциплина "Основы информатики" призвана решать задачу подготовки студентов направления подготовки "Прикладная математика и информатика" с дополнительной специальностью информатика к преподаванию информатики в средней общеобразовательной школе с учетом уровневой и профильной дифференциаций образования. Важность дисциплины обусловлена также тем, что элементы теоретических основ информатики могут быть использованы на различных этапах обучения информатике в школе (равномерные коды, измерение информации, алгоритмы работы архиваторов, кодирование информации различного вида и т.д.). Особую ценность приобретают знания этой дисциплины при подготовке наиболее "продвинутых" школьников к сдаче испытаний в формате ЕГЭ.

При изучении дисциплины следует перед каждым очередным практическим или лекционным занятием повторять соответствующий материал по конспектам лекций, отмечая непонятые и/или непонятные положения. Рекомендуется проведение самостоятельной работы в читальном зале во внеучебное время. Используйте ресурсы Internet

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

№	Автор, название, место издания, издательство, год издания учебной литературы, вид и характеристика иных информационных ресурсов	Наличие грифа, вид грифа	МПТИ СВФУ, кафедральная библиотека и кол-во экземпляров в библиотеке МПТИ (ф) СВФУ	Электронные издания: точка доступа к ресурсу (наименование ЭБС, ЭБ СВФУ)
Основная литература				
1	Петров М.Н., Компьютерная графика + CD, учебник, СПб.: Питер, 2011	МО	17	
2	Пантюхин П.Я., Компьютерная графика. : В 2-х частях. Ч : 1, учебное пособие, М.: Форум: Инфра-м, 2012	МО	17	
3	Григорьева И.В., Компьютерная графика, учебное пособие, М.: Прометей, 2012	УМО	17	http://biblioclub.ru/index.php?page=book_red&id=211721
Дополнительная литература				
1	Машихина Т.П., Компьютерная графика, учебное пособие, Волгоград : ВИБ, Вузовское образование, 2009		17	http://www.iprb ookshop.ru/1132 8.html
2	Перемитина Т.О., Компьютерная графика, учебное пособие, Томск : ТГУСУиР, Эль Контент, 2012		17	http://www.iprb ookshop.ru/1394 0.html

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее сеть-Интернет), необходимых для освоения дисциплины

1. ЭБС «Университетская библиотека онлайн» www.biblioclub.ru
2. ЭБС IPRbooks <http://www.iprbookshop.ru/>
3. Научная электронная библиотека <http://elibrary.ru>

9. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Класс ЭВМ, мультимедиа проектор и интерактивная доска

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

10.1. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

При осуществлении образовательного процесса по дисциплине используются следующие информационные технологии:

- использование на занятиях электронных изданий (чтение лекций с использованием слайд - презентаций, электронного учебного пособия);
- использование специализированных и офисных программ, информационных (справочных) систем;
- Организация взаимодействия с обучающимися посредством электронной почты и СДО Moodle.

10.2. Перечень программного обеспечения

MS Office, Delphi. Программы для чтения источников в формате pdf, djvu.

10.3. Перечень информационных справочных систем

Консультант, Гарант

