

Министерство образования и науки Российской Федерации
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кубанский государственный университет»
Факультет математики и компьютерных наук

УТВЕРЖДАЮ

Проректор по учебной работе
качеству образования – первый
проректор

Хатуров Т.А.
подпись
«__» _____ 2018 г.



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

**Б1.Б.25 ДОПОЛНИТЕЛЬНЫЕ ДИСЦИПЛИНЫ ДЛЯ УКРУПНЕННЫХ
ГРУПП СПЕЦИАЛИЗАЦИЙ И ДИСЦИПЛИНЫ СПЕЦИАЛИЗАЦИЙ**

Специальность 01.05.01. Фундаментальные математика и механика

Специализация: Математическое моделирование

Форма обучения очная

Квалификация (степень) выпускника Математик. Механик. Преподаватель

Краснодар 2018

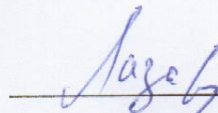
Рабочая программа дисциплины ДОПОЛНИТЕЛЬНЫЕ ДИСЦИПЛИНЫ
ДЛЯ УКРУПНЕННЫХ ГРУПП СПЕЦИАЛИЗАЦИЙ И ДИСЦИПЛИНЫ
СПЕЦИАЛИЗАЦИЙ составлена в соответствии с требованиями ФГОС ВО от
по специальности 01.05.01 ФУНДАМЕНТАЛЬНЫЕ МАТЕМАТИКА И
МЕХАНИКА

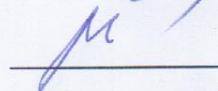
Составители:

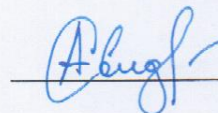
Доктор пед. наук, профессор, зав. кафедрой
теории функций КубГУ

Доктор физ.-мат. наук, профессор кафедры
функционального анализа и алгебры КубГУ

Кандидат физ.-мат. наук, доцент кафедры
математического и компьютерного
моделирования КубГУ

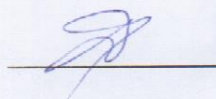
 В.А. Лазарев

 А.В. Рожков

 А.А. Свидлов

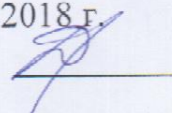
Рабочая программа рассмотрена и утверждена на заседании кафедры функ-
ционального анализа и алгебры протокол № 10 от «10» апреля 2018 г.

Зав. кафедрой функционального анализа
и алгебры кандидат физ.-мат. наук, доцент

 В.Ю. Барсукова

Рабочая программа обсуждена на заседании кафедры (выпускающей) функ-
ционального анализа и алгебры протокол № 10 от «10» апреля 2018 г.

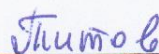
Заведующий кафедрой (выпускающей) Барсукова В.Ю.



Рабочая программа одобрена на заседании учебно-методической комиссии
факультета математики и компьютерных наук «17» апреля 2018 г. протокол
№ 2

Председатель УМК ФМ и КН

кандидат физ.-мат. наук, доцент



Г.Н. Титов

Рецензенты:

Наумова Н.А. доктор технических наук, профессор кафедры прикладной ма-
тематики ФГБОУ ВО «Кубанский государственный технологический уни-
верситет»

Гайденко С.В. кандидат физ.-мат. наук, зав. кафедрой вычислительной мате-
матики и информатики КубГУ

Дисциплина «Дополнительные дисциплины для укрупненных групп специализаций и дисциплины специализаций» рассчитана на четыре семестра (5-8-й)

5 семестр «ПРИМЕНЕНИЕ ТЕОРИИ ФУНКЦИЙ КОМПЛЕКСНОГО ПЕРЕМЕННОГО К ЗАДАЧАМ ФИЗИЧЕСКОГО СОДЕРЖАНИЯ»

Цель дисциплины:

Целью курса Получение обучающимися знаний по теории функций комплексного переменного, необходимых для понимания её приложений к математическим и прикладным дисциплинам (таким, как гидродинамика).

Задачи дисциплины: изучение комплекса методов теории функций, комплексного переменного, применяющихся при решении прикладных задач.

Место дисциплины в структуре ООП ВО

Дисциплина «Дополнительные дисциплины для укрупненных групп специализаций и дисциплины специализаций» относится к базовой части Блока 1 "Дисциплины (модули)" учебного плана.

Требования к уровню освоения дисциплины

Изучение данной учебной дисциплины направлено на формирование у обучающихся общепрофессиональных и профессиональных компетенций (ОПК-1, ПК-5)

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	владеть
1.	<i>ОПК-1</i>	Готовностью использовать фундаментальные знания в области, комплексного анализа в будущей профессиональной деятельности	теоретические основы применения методов теории функций комплексного переменного к задачам гидродинамики	Применять стандартные методы теории функций комплексного переменного к прикладным задачам	навыками применения средств теории функций комплексного переменного
2.	<i>ПК-5</i>	способностью использовать методы математического и алгоритмического моделирования при решении теоретических и прикладных задач	основные приемы моделирования с помощью методов теории функций комплексного переменного к задачам гидродинамики	Решать задачи в области гидродинамики с помощью теории функций комплексного переменного	Навыками построения моделей на базе функций комплексного переменного

2 Структура и содержание дисциплины

2.1 Распределение трудоемкости дисциплины по видам работ

Общая трудоемкость дисциплины «Применение теории функций комплексного переменного к задачам физического содержания» составляет 4 зачетные единицы (144 ч., из них контактных 80,2 ч.: аудиторной нагрузки 72 ч. (36 ч лекций, 36 ч. лабораторных занятий), 8 ч. КСР, 0,2 ч. ИКР, 63,8 ч. самостоятельной работы).

Вид учебной работы		Всего часов	Семестры 5-й
Аудиторные занятия (всего)		144	144
В том числе:			
Занятия лекционного типа		36	36
Занятия семинарского типа (семинары, практические занятия)		36	36
Иная контактная работа:			
Контроль самостоятельной работы (КСР)		8	8
Промежуточная аттестация (ИКР)		0,2	0,2
Самостоятельная работа, в том числе		63,8	63,8
Проработка учебного (теоретического) материала		20	20
Выполнение домашних заданий (решение задач)		30	30
Подготовка к текущему контролю		13,8	13,8
Контроль:			
Подготовка к экзамену			
Общая трудоемкость	час.	144	144
	в том числе контакт-ная работа	80,2	80,2
	зач. ед	4	4

2.2 Структура дисциплины:

Разделы дисциплины, изучаемые в 5 семестре

№	Наименование разделов (тем)	Количество часов				
		Всего	Аудиторная работа			Вне аудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
1.	Гидродинамическая интерпретация функций комплексного переменного.	28	4		4	20
2.	Конформные отображения.	48	14		14	20
3.	Гидродинамические представления, связанные с функциями комплексного переменного	59,8	18		18	23,8
	<i>Итого по дисциплине:</i>		36	-	36	63,8

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа

№ п/п	Наименование раздела	Содержание раздела	Форма текущего контроля
1	Гидродинамическая интерпретация функций комплексного переменного.	Гидродинамическая интерпретация функций комплексного переменного. Гидродинамические представления, связанные с функциями комплексного переменного.	Проверка домашнего задания .

2	Конформные отображения.	Свойство конформности. Картографическая задача: конформное отображение сферы на плоскость. Геометрический смысл производной. Чертёжное воспроизведение конформного отображения. Понятие об основной теореме Римана по поводу конформного отображения. Уравнение Лапласа. Гармонические функции. Их применение. Некоторые свойства линий постоянного модуля и линий постоянного	Проверка домашнего задания
3	Гидродинамические представления, связанные с функциями комплексного переменного	Вихрь и источник под свободной поверхностью жидкости при малых числах Фруда. Диполь под свободной поверхностью жидкости при малых числах Фруда. Обтекание суперкавитирующей пластинки в канале.	Проверка домашнего задания

2.3.2 Занятия семинарского типа не предусмотрены

2.3.3 Лабораторные занятия.

№ п/п	Наименование раздела	Содержание раздела	Форма текущего контроля
1	Гидродинамическая интерпретация функций комплексного переменного.	Гидродинамическая интерпретация функций комплексного переменного. Гидродинамические представления, связанные с функциями комплексного переменного.	Проверка домашнего задания.
2	Конформные отображения.	Свойство конформности. Картографическая задача: конформное отображение сферы на плоскость. Геометрический смысл производной. Чертёжное воспроизведение конформного отображения. Понятие об основной теореме Римана по поводу конформного отображения. Уравнение Лапласа. Гармонические функции. Их применение. Некоторые свойства линий постоянного модуля и линий постоянного	Проверка домашнего задания Контрольная работа
3	Гидродинамические представления, связанные с функциями комплексного переменного	Вихрь и источник под свободной поверхностью жидкости при малых числах Фруда. Диполь под свободной поверхностью жидкости при малых числах Фруда. Обтекание суперкавитирующей пластинки в канале.	Проверка домашнего задания. Контрольная работа

3. Образовательные технологии: активные и интерактивные формы, лекции, лабораторные занятия, контрольные работы, реферативные доклады (по некоторым темам в виде презентации). В течение семестра студенты решают задачи, указанные преподавателем, к каждому лабораторному занятию.

Использование компьютерных технологий

Применение на занятии компьютерных технологий позволяет студентам при рассмотрении определенных тем курса более глубоко освоить соответствующие понятия. В

этой связи определенные лекционные и лабораторные занятия преподавателю целесообразно проводить в виде презентации. Также в виде презентации в соответствии с темой лабораторного занятия студенты могут излагать подготовленные ими некоторые свои реферативные доклады

К образовательным технологиям также относятся интерактивные методы обучения. Интерактивность подачи материала по дисциплине предполагает не только взаимодействия вида «преподаватель - студент» и «студент - преподаватель», но и «студент - студент». Все эти виды взаимодействия хорошо достигаются при изложении материала на занятиях в ходе дискуссий, а также на лабораторных занятиях в ходе изложения студентами реферативных докладов (возможно в виде презентации).

Се- местр	Вид занятия	Используемые интерактивные образовательные тех- нологии	Количе- ство ча- сов
5	Лаборатор- ные занятия	«Гидродинамическая интерпретация функций комплексного переменного.– <i>занятие - дискуссия</i>	4
		Доклады студентов по теме «Гидродинамиче- ские представления, связанные с функциями комплексного переменного»	14
Итого:			18

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций со студентом при помощи электронной информационно-образовательной среды ВУЗа.

Таблица 4 – типовые задания для самоподготовки студентов

Перечень компетенций	Л	ЛЗ	Формы контроля
ОПК-1		+	Самостоятельная работа с доступом к источникам информации, зачет
ОПК-1 ПК-5	+		Обзор литературы, зачет
ОПК-1		+	Отчеты по практическим заданиям
ОПК-1	+	+	Дискуссия, зачет
ОПК-1	+		зачет
ПК-5	+	+	Собеседование, зачет
ПК-5	+	+	консультация
ОПК-1 ПК-5	+		Презентация, зачет

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа,

Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа,

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Учебная деятельность проходит в соответствии с графиком учебного процесса. Процесс самостоятельной работы контролируется во время аудиторных занятий и индивидуальных консультаций.

Оценочными средствами дисциплины являются средства текущего контроля (контрольные работы, ответ у доски и проверка домашних заданий) и итоговая аттестация (зачет). Зачет выставляется по результатам работы в семестре с учетом выполнения домашних заданий и итоговой контрольной работы.

Контрольные работы оцениваются по пятибалльной системе. Зачет оценивается по системе: зачтено, не зачтено. На лабораторных занятиях контроль осуществляется при ответе у доски и при проверке домашних заданий.

Самостоятельная работа студента включает в себя повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным занятиям, к контрольным работам и к зачету. Такой вид СРС контролируется в ходе проверки домашних заданий, заданий контрольных работ и в ходе зачета. Контроль осуществляется во время консультаций (вызывных или по желанию студента), а также на лабораторных занятиях.

4.1 Фонд оценочных средств для проведения текущей аттестации

Примерные задания для контрольных работ

1. На какую область в плоскости w функция $w = \frac{1}{1-z}$ отображает круг $|z| < 1$? Как отображаются, в частности: а) окружности $|z| = r (0 < r < 1)$ и б) радиусы $\arg z = \theta (0 \leq \theta \leq 2\pi)$?
2. Доказать, что функция $w = \frac{z-a}{1-\bar{a}z}$ ($|a| < 1$) отображает круг $|z| < 1$ на круг $|w| < 1$, причем точка $z = a$ переходит в точку $w = 0$. Выяснить, во что превращаются окружности $|z| = r (0 < r < 1)$ и радиусы $\arg z = \theta (0 \leq \theta < 2\pi)$. Убедиться, что такими же свойствами обладает и более общая функция $w = \frac{e^{i\omega}(z-a)}{1-\bar{a}z}$.
3. Функция $w = e^z$ отображает полосу $-\infty < x < +\infty, -\pi < y \leq +\pi$ на всю плоскость w . Как отображаются при этом: а) отрезок $x = x_0, -\pi < y \leq \pi$ б) прямая $y = y_0 (-\pi < y_0 < \pi)$ в) окружность $r = r_0 (0 < r_0 < \pi)$, г) луч $\theta = \theta_0 (-\pi < \theta_0 \leq \pi)$?
4. Дать гидродинамическое истолкование течений, определяемых характеристическими функциями: а) z^2 , б) $\ln \frac{z+1}{z-1}$, в) $\ln(z^4 - 1)$, г) $i \ln z$, д) e^z , е) $\ln \operatorname{tg} z$.
5. Как изменяется картина течения при переходе от характеристической функции $f(z)$ к одной из следующих: а) $-f(z)$, б) $if(z)$, в) $-if(z)$?
6. Характеристическая функция имеет вид:

$$f(z) = \ln \frac{z}{(z+1)^\alpha (z-1)^\beta} \quad (\alpha, \beta > 0; \alpha + \beta = 1).$$

Установить, каковы источники и каковы стоки; определить соответствующие мощности. Имеются ли точки покоя?
7. Построить течение с источниками равной мощности в точках $+1, -1, +i, -i$ и со стоком учетверенной мощности в точке $z = 0$.
8. Показать, что следующая характеристическая функция способна также давать картину обтекания кругового цилиндра": $f(z) = z + \frac{1}{z} + 2i\mu \ln z \quad (0 < \mu < 1)$. Найти точки покоя.

9. Уяснить себе следующую гидродинамическую интерпретацию теоремы : если характеристическая функция имеет вид $f(z) = \ln P(z)$, где $P(z)$ — многочлен, имеющий лишь простые корни, то внутри всякого замкнутого контура, ортогонального к линиям тока, содержится число точек покоя, на единицу меньшее, чем число источников. Внести уточнения, относящиеся к случаю многочлена с кратными корнями.

10. Для случая течения с характеристической функцией вида $f(z) = \ln P(z)$, где $P(z)$ — произвольный многочлен, целесообразно говорить о „стоке на бесконечности". Надлежащим образом дав определение „мощности стока на бесконечности", уяснить себе следующую гидродинамическую интерпретацию основной теоремы алгебры: *Мощность стока на бесконечности равна сумме мощностей источников, находящихся на конечном расстоянии.*

Критерии оценивания по промежуточной аттестации

Зачет выставляется по результатам работы студента в течение семестра. Отметка «зачтено» выставляется студентам, которые регулярно посещали занятия, выполняли домашние работы, написали контрольные работы на положительные оценки. Отметка «незачтено» выставляется студентам, которые пропустили более 60 % занятий и написали контрольные работы на неудовлетворительные оценки.

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

5.1 Основная литература:

1. Попов, В.Н. Прикладные вопросы теории функций комплексного переменного : учебное пособие / В.Н. Попов ; - Архангельск : ИПЦ САФУ, 2013. - 164 с. : ил. - Библиогр. в кн. - ISBN 978-5-261-00850-7 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=436400>

2. Привалов, И.И. Введение в теорию функций комплексного переменного [Электронный ресурс] : учебник / И.И. Привалов. — Электрон. дан. — Санкт-Петербург : Лань, 2009. — 432 с. — Режим доступа: <https://e.lanbook.com/book/322> .

5.2 Дополнительная литература:

1. Лаврентьев, М.А. Методы теории функций комплексного переменного : учебное пособие / М.А. Лаврентьев, Б.В. Шабат. - Изд. 3-е, испр. - Москва : Наука, 1965. - 716 с. : ил. ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=464237>

6. Методические указания для обучающихся по освоению дисциплины

По курсу предусмотрено проведение лекционных занятий, на которых дается основной систематизированный материал, лабораторных занятий, в ходе которых студентами приобретаются и закрепляются основные практически навыки решения различных задач, в том числе с применением полученных теоретических знаний.

Важнейшим этапом курса является самостоятельная работа по дисциплине. Самостоятельная работа студентов является неотъемлемой частью процесса подготовки. Под самостоятельной работой понимается часть учебной планируемой работы, которая выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Самостоятельная работа направлена на усвоение системы научных и профессиональных знаний, формирования умений и навыков, приобретение опыта самостоятельной творческой деятельности. СРС помогает формировать культуру мышления студентов, расширять познавательную деятельность.

Виды самостоятельной работы по курсу:

а) по целям: подготовка к лекциям, к практическим занятиям, к контрольной работе,

к коллоквиуму; подготовка научного доклада и выполнение заданий.

б) по характеру работы: изучение литературы, конспекта лекций; поиск литературы в библиотеке; конспектирование рекомендуемой для самостоятельного изучения научной литературы; решение задач, тестов; работа с обучающими и контролирующими программами.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю) (при необходимости)

8.1. Перечень информационных технологий.

Использование презентаций при проведении лекционных занятий.

8.2 Перечень необходимого программного обеспечения

Программы для демонстрации и создания презентаций («Microsoft Power Point»).

8.3 Перечень необходимых информационных справочных систем

Электронная библиотечная система eLIBRARY.RU (<http://www.elibrary.ru/>)

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Лекционные занятия	Лекционная аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук, ...) и соответствующим программным обеспечением
2.	Лабораторные занятия	Специальное помещение, оснащенное доской, маркерами и мелом , Компьютерные классы
3.	Групповые (индивидуальные) консультации	Аудитория (кабинет)
4.	Текущий контроль, промежуточная аттестация	Аудитория, (кабинет)
5.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета.

6 семестр «ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ КРИПТОГРАФИИ»

Цели и задачи изучения дисциплины

1.1 Цель дисциплины

Целями освоения дисциплины «Дополнительные дисциплины для укрупненных групп специализаций и дисциплины специализаций» являются: подготовка в области применения современной вычислительной техники для решения практических задач математического и компьютерного моделирования, информатики; получение высшего профессионального (на уровне специалиста) образования, позволяющего выпускнику успешно работать в избранной сфере деятельности с применением современных компьютерных технологий.

1.2 Задачи дисциплины

Задачи освоения дисциплины «Теоретико-числовые методы криптографии»: получение базовых теоретических и исторических сведений о структуре и алгоритмах функционирования криптоалгоритмов. Применение этих знаний на практике, при рассмотрении перспектив развития математических и компьютерных наук, месте и роли защиты информации в структуре информатизации и математических методов построения защищенных информационных систем.

Изучение теоретических основ предмета: Числовые функции, основные теоремы о евклидовых кольцах, алгоритмы решения линейных и квадратных уравнений в конечных полях, кольцах вычетов, алгоритмы нахождения наибольших общих делителей, алгоритмов проверки простоты чисел;

системного подхода к организации защиты информации, передаваемой и обрабатываемой техническими средствами на основе применения криптографических методов; алгебраических и теоретико-числовых принципов синтеза и анализа шифров; математических методов, используемых в криптоанализе и криптографии.

1.3 Место дисциплины в структуре образовательной программы

Дисциплина Дополнительные дисциплины для укрупненных групп специализаций и дисциплины специализаций («Теоретико-числовые методы криптографии») относится к базовой части Блока 1 "Дисциплины (модули)" учебного плана и является одной из основных дисциплин в освоении математических знаний. Дисциплина «Теоретико-числовые методы криптографии» читается в 6 семестре.

Знания, полученные в этом курсе, могут быть использованы в ходе практик, в других компьютерных дисциплинах. Слушатели должны владеть знаниями в рамках программы курсов «Алгебра», «Математический анализ», «Технология программирования и работа на электронно-вычислительной машине (ЭВМ)».

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

Изучение данной дисциплины направлено на получение необходимого объема теоретических знаний, отвечающих требованиям ФГОС ВО и необходимых для дальнейшего успешного изучения всех дисциплин высшей математики, с формированием следующих общепрофессиональных и профессиональных компетенций: ОПК-1, ПК—5.

	Индекс	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны
--	--------	---------------------------------------	---

			знать	уметь	владеть
.	ОПК-1	готовность использовать фундаментальные знания в области ... алгебры, линейной алгебры, ...теории управления и оптимизации в будущей профессиональной деятельности.	об основных задачах и понятиях криптографии; об этапах развития криптографии; о видах информации, подлежащей шифрованию; о классификации шифров	использовать: типовые шифры замены и перестановки; частотные характеристики языков и их использование в криптоанализе; требования к шифрам и основные характеристики шифров; принципы построения современных шифрсистем	криптографической терминологией; навыками использования основных типов шифров и криптографических алгоритмов; методами криптоанализа простейших шифров
2.	ПК-5	способностью использовать методы математического и алгоритмического моделирования при решении теоретических и прикладных задач	о методах криптографического синтеза и анализа; о применениях криптографии в решении задач аутентификации, построения систем цифровой подписи; о методах криптозащиты компьютерных систем и сетей	Использовать типовые поточные и блочные шифры, системы шифрования с открытыми ключами, криптографические протоколы; постановки задач криптоанализа и подходы к их решению; основные математические методы, используемые в анализе типовых криптографических алгоритмов	навыками математического моделирования в криптографии; современной научно-технической литературой в области криптографической защиты

2 Структура и содержание дисциплины

2.1 Распределение трудоемкости дисциплины по видам работ

Общая трудоемкость дисциплины «Теоретико-числовые методы криптографии» составляет 3 зачетные единицы (108 часов, из них – 83,2 часа контактной работы (36 лекций, 36 часов лабораторных занятий, 11 часов КСР, 0,2 часов ИКР); 24,8 часа самостоятельной работы).

Вид учебной работы		Всего часов	Семестры 6-й
Аудиторные занятия (всего)		72	72
В том числе:			
Занятия лекционного типа		36	36
Занятия семинарского типа (семинары, практические занятия)		36	36
Иная контактная работа:			
Контроль самостоятельной работы (КСР)		11	11
в том числе Курсовая работа		7	7
Промежуточная аттестация (ИКР)		0,2	0,2
Самостоятельная работа, в том числе		24,8	24,8
Курсовая работа (подготовка и написание)		10	10
Проработка учебного (теоретического) материала		6	6
Выполнение домашних заданий (решение задач)		6	6
Подготовка к текущему контролю		2,8	2,8
Контроль:			
Подготовка к экзамену			
Общая трудоемкость	час.	108	108
	в том числе контакт-ная работа	83,2	83,2
	зач. ед	3	3

2.2 Структура дисциплины:

Разделы дисциплины, изучаемые в 6 семестре

№ раз-дела	Наименование разделов	Количество часов			
		Всего	Аудиторная работа		Самостоя-тельная ра-бота
			Л	ЛЗ	
1	2	3	4	5	6
1	Модели шифров.	26	10	10	6
2	Мультипликативные функ-ции.	22	8	8	6
3	Табличное и модульное гам-мирование.	26	10	10	6
4	Построение больших простых чисел.	23.8	8	8	6,8
	Итого:		36	36	24,8

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа

№ п/п	Наименование раздела	Содержание раздела	Форма текущего контроля
1	Модели шифров.	Блочные и поточные шифры. Понятие криптосистемы. Ручные и машинные шифры. Ключевая система шифра. Основные требования к шифрам	Проверка домашнего задания, реферативный доклад.
2	Мультипликативные функции.	Функция Эйлера и Мебиуса. Группы обратимых элементов в кольцах. Структура мультипликативной группы кольца вычетов. Обратимые элементы. Прimitивные элементы.	Проверка домашнего задания, реферативный доклад.
3	Табличное и модульное гаммирование.	Случайные и псевдослучайные гаммы. Регистры сдвига с обратной связью Криптограммы, полученные при повторном использовании ключа. Анализ криптограмм, полученных применением неравновероятной гаммы.	Проверка домашнего задания, реферативный доклад.
4	Построение больших простых чисел.	Алгоритмы проверки на простоту. Эллиптические кривые над конечными полями и алгоритмы вычисления на них. Электронная подпись.	зачет

2.3.2 Занятия семинарского типа не предусмотрены

2.3.3 Лабораторные занятия.

№ п/п	Наименование раздела	Содержание раздела	Форма текущего контроля
1	Модели шифров.	Блочные и поточные шифры. Понятие криптосистемы. Ручные и машинные шифры. Ключевая система шифра. Основные требования к шифрам	Проверка домашнего задания, реферативный доклад.
2	Мультипликативные функции.	Функция Эйлера и Мебиуса. Группы обратимых элементов в кольцах. Структура мультипликативной группы кольца вычетов. Обратимые элементы. Прimitивные элементы.	Проверка домашнего задания, реферативный доклад.
3	Табличное и модульное гаммирование.	Случайные и псевдослучайные гаммы. Регистры сдвига с обратной связью Криптограммы, полученные при повторном использовании ключа. Анализ криптограмм, полученных применением неравновероятной гаммы.	Проверка домашнего задания, реферативный доклад.
4	Построение больших простых чисел.	Алгоритмы проверки на простоту. Эллиптические кривые над конечными полями и алгоритмы вычисления на них. Электронная подпись.	Зачет, курсовая работа

2.3.4 Примерная тематика курсовых работ (проектов)

1. Освоение процессов зашифрования и расшифрования для простейших шифров.
2. Свойства простейших шифров.
3. Расчет мощности ключевой системы различных шифров.
4. Оценка расстояния единственности для простейших шифров.
5. Криптоанализ шифра Виженера.

6. Расчет характеристик метода перебора ключей.
7. Вычисление характеристик двоичных функций.
8. Анализ схемы DES при небольшом числе итераций.
9. Вычисление характеристик датчиков псевдослучайных чисел.

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Проработка учебного (теоретического) материала	Методические указания по организации самостоятельной работы, утвержденные кафедрой функционального анализа и алгебры протокол № 1 от 31.08.2017 г
2	Выполнение домашних заданий (решение задач)	Методические указания по организации самостоятельной работы, утвержденные кафедрой функционального анализа и алгебры протокол № 1 от 31.08.2017 г
3	Подготовка к текущему контролю	Методические указания по организации самостоятельной работы, утвержденные кафедрой функционального анализа и алгебры протокол № 1 от 31.08.2017 г

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа,

Для лиц с нарушениями слуха:

- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

- в печатной форме,
- в форме электронного документа,

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Таблица 4 – типовые задания для самоподготовки студентов

Перечень компетенций	Л	ЛЗ	Формы контроля
ОПК-1		+	Самостоятельная работа с доступом к источникам информации, отчет по реферату, зачет
ОПК-1 ПК-5	+		Обзор литературы, зачет
ОПК-1		+	Отчеты по практическим заданиям, реферативный доклад
ОПК-1	+	+	Дискуссия, зачет
ОПК-1	+		Реферативный доклад, зачет
ПК-5	+	+	Собеседование, зачет
ПК-5	+	+	Реферативный доклад, консультация
ОПК-1 ПК-5	+		Презентация, зачет

3. Образовательные технологии: активные и интерактивные формы, лекции, лабо-

ракторные занятия, контрольные работы, реферативные доклады (по некоторым темам в виде презентации). В течение семестра студенты решают задачи, указанные преподавателем, к каждому лабораторному занятию.

Использование компьютерных технологий

Применение на занятии компьютерных технологий позволяет студентам при рассмотрении определенных тем курса более глубоко освоить соответствующие понятия. В этой связи определенные лекционные и лабораторные занятия преподавателю целесообразно проводить в виде презентации. Также в виде презентации в соответствии с темой лабораторного занятия студенты могут излагать подготовленные ими некоторые свои реферативные доклады

К образовательным технологиям также относятся интерактивные методы обучения. Интерактивность подачи материала по дисциплине предполагает не только взаимодействия вида «преподаватель - студент» и «студент - преподаватель», но и «студент - студент». Все эти виды взаимодействия хорошо достигаются при изложении материала на занятиях в ходе дискуссий, а также на лабораторных занятиях в ходе изложения студентами реферативных докладов (возможно в виде презентации).

Се- местр	Вид занятия	Используемые интерактивные образовательные тех- нологии	Количе- ство ча- сов
6	Лаборатор- ные занятия	«Ручные и машинные шифры» (раздел 1) – <i>за- нятие в виде презентации.</i>	2
		«Анализ криптограмм» (раздел 3) - <i>занятие в виде презентации.</i>	2
		«Эллиптические кривые над конечными поля- ми» (раздел 4) – <i>занятие в виде презентации.</i>	2
		Тема Числа Кармайкла. Разложение чисел на простые числа.	2
		Дискуссия на тему: «. Метод локализации. Ал- горитм пополнения.» с докладами- презентациями	2
		Круглый стол на тему: «Алгоритмы факториза- ции целых чисел.» с докладами-презентациями	4
		Мозговой штурм» («мозговая атака»): Базисы Грёбнера.	2
		Компьютерная симуляция: Решение системы полиномиальных уравнений	2
Итого:			18

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций со студентом при помощи электронной информационно-образовательной среды ВУЗа.

В рамках реализации компетентностного подхода предусматриваются следующие основные виды активных и интерактивных форм проведения учебных занятий

- применение электронных образовательных ресурсов;
- компьютерные симуляции;

Дискуссия – это публичное обсуждение или свободный вербальный обмен знаниями, суждениями, идеями или мнениями по поводу какого-либо спорного вопроса, проблемы. Ее существенными чертами являются сочетание взаимодополняющего диалога и обсуждения-спора, столкновение различных точек зрения, позиций.

«Круглый стол» – одна из форм организации дискуссии, в которой на равных участвуют 15–25 человек; в ходе нее происходит обмен мнениями между всеми участниками.

Основное целевое назначение метода – обеспечение свободного, нерегламентированного обсуждения поставленных вопросов (тем) на основе постановки всех студентов в равное положение по отношению друг к другу. Как правило, перед участниками не стоит задача полностью решить проблему.

«Мозговой штурм» («мозговая атака») представляет собой разновидность групповой дискуссии, которая характеризуется отсутствием критики поисковых усилий, сбором всех вариантов решений, гипотез и предложений, рожденных в процессе осмысления какой-либо проблемы, их последующим анализом с точки зрения перспективы дальнейшего использования или реализации на практике. «Мозговой штурм» включает три этапа: подготовительный, этап генерирования идей, этап анализа и оценки идей. Продолжительность «мозгового штурма», как правило, не менее 1,5–2 часов.

Компьютерная симуляция – это максимально приближенная к реальности имитация различных процессов (физических, химических, экономических, социальных и проч.) и (или) деятельности с использованием программного обеспечения образовательного назначения

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Учебная деятельность проходит в соответствии с графиком учебного процесса. Процесс самостоятельной работы контролируется во время аудиторных занятий и индивидуальных консультаций.

Оценочными средствами дисциплины являются средства текущего контроля (контрольные работы, ответ у доски и проверка домашних заданий) и итоговая аттестация (зачет). Зачет выставляется по результатам работы в семестре с учетом выполнения домашних заданий и итоговой контрольной работы.

Контрольные работы и реферативные доклады оцениваются по пятибалльной системе. Зачет оценивается по системе: зачтено, не зачтено. На лабораторных занятиях контроль осуществляется при ответе у доски и при проверке домашних заданий.

Самостоятельная работа студента включает в себя повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным занятиям, к контрольным работам и к зачету. Такой вид СРС контролируется в ходе проверки домашних заданий, заданий контрольных работ и в ходе зачета. Предполагается самостоятельное изучение студентами теоретического материала по темам реферативных докладов, указанных ниже в пункте 6.4. Контроль осуществляется во время консультаций (вызывных или по желанию студента), а также на лабораторных занятиях.

Виды самостоятельной работы

Обязательными при изучении дисциплины «Теоретико-числовые методы криптографии» являются следующие виды самостоятельной работы:

- разбор и самостоятельное изучение теоретического материала по конспектам лекций и по учебным пособиям из списка источников литературы (п. 6.1);
- самостоятельное решение задач по темам лабораторных занятий (п. 6.2);
- подготовка к контрольным работам (п. 6.3);
- подготовка к реферативному докладу (п. 6.4);
- подготовка к зачету (п. 6.5).

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в печатной форме увеличенным шрифтом,
- в форме электронного документа.

Перечень

электронных документов, которые могут быть представлены
в печатной форме с увеличенным шрифтом

1. Рожков А.В. «Темы исследовательских работ и методические указания по их написанию», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 30 августа 2017 г.
2. Рожков А.В. «Комментарии к лекциям по криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 30 августа 2017 г.
3. Рожков А.В. «Решебник типовых задач по криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 30 августа 2017 г.
4. Рожков А.В. «Алгебраические методы криптографии. Методические указания», утвержденные кафедрой функционального анализа и алгебры, протокол № 1 от 30 августа 2017 г.
5. Рябко, Б.Я. Криптографические методы защиты информации [Электронный ресурс] : учебное пособие / Б.Я. Рябко, А.Н. Фионов. — Электрон. дан. — Москва : Горячая линия-Телеком, 2012. — 229 с. — Режим доступа: <https://e.lanbook.com/book/5193>
6. Бухштаб, А.А. Теория чисел [Электронный ресурс] : учебное пособие / А.А. Бухштаб. — Электрон. дан. — Санкт-Петербург : Лань, 2015. — 384 с. — Режим доступа: <https://e.lanbook.com/book/65053>
7. Торстейнсон, П. Криптография и безопасность в технологии. NET [Электронный ресурс] / П. Торстейнсон, Г.А. Ганеш ; под ред. С. М. Моляко ; пер. с англ. В. Д. Хорева. — Электрон. дан. — Москва : Издательство "Лаборатория знаний", 2015. — 428 с. — Режим доступа: <https://e.lanbook.com/book/70724>
8. Глухов, М.М. Введение в теоретико-числовые методы криптографии [Электронный ресурс] : учебное пособие / М.М. Глухов, И.А. Круглов, А.Б. Пичкур, А.В. Черемушкин. — Электрон. дан. — Санкт-Петербург : Лань, 2011. — 400 с. — Режим доступа: <https://e.lanbook.com/book/68466>

Критерии оценивания по промежуточной аттестации

Зачет выставляется по результатам работы студента в течение семестра. Отметка «зачтено» выставляется студентам, которые регулярно посещали занятия, выполняли домашние работы, написали контрольные работы на положительные оценки. Отметка «незачтено» выставляется студентам, которые пропустили более 60 % занятий и написали контрольные работы на неудовлетворительные оценки.

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

5.1 Основная литература:

1. Рябко Б.Я, Фионов А.Н. Криптографические методы защиты информации [Электронный ресурс]. — М.: Горячая линия-Телеком, 2012. — URL:

<https://e.lanbook.com/reader/book/5193/#1>

2. Глухов М.М., Круглов И.А., Пичкур А.Б., Черемушкин А.В. Введение в теоретико-числовые методы криптографии. [Электронный ресурс]. - СПб.: Лань, 2011. - URL: <https://e.lanbook.com/reader/book/68466/#1>

5.2 Дополнительная литература:

1. Бухштаб А.А. Теория чисел, 4-е изд. [Электронный ресурс]. - СПб.: Лань, 2015. - URL: <https://e.lanbook.com/reader/book/65053/#1>
2. Торстейнсон П., Ганеш Г.А. Криптография и безопасность в технологии .NET. 3-е изд. [Электронный ресурс]. – М.: Лаборатория знаний, 2015. – URL: <https://e.lanbook.com/reader/book/70724/#1>

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», в том числе современные профессиональные базы данных и информационные справочные системы, необходимые для освоения дисциплины (модуля).

1. Пакет компьютерной алгебры Sage 8.3. Официальный сайт <http://sagemath.org/>
2. Пакет компьютерной алгебры Gap4r9p3. Официальный сайт <http://www.gap-system.org/>
3. Пакет компьютерной алгебры PARI/GP 2.11 Официальный сайт <http://pari.math.u-bordeaux.fr/>
4. Справочно-правовая система «Консультант Плюс» (<http://www.consultant.ru>)
5. База данных Научной электронной библиотеки eLIBRARY.RU <https://elibrary.ru/>

Методические указания для обучающихся по освоению дисциплины (модуля)

Для подготовки к ответам на теоретические вопросы в ходе контрольных работ и на зачете студентам достаточно использовать материал лекций. Весь этот теоретический материал содержится в учебных пособиях из списка основной литературы 1 – 2. Для изучения теоретического материала, необходимого для подготовки реферативного доклада, кроме основных источников литературы возможно использование дополнительных источников и Интернет-ресурса. В случае затруднений, возникающих у студентов в процессе самостоятельного изучения теории, преподаватель разъясняет сложные моменты на консультациях.

Список теоретических вопросов (для самостоятельных работ и зачета)

1. Защита персональных данных.
2. История криптографии; классические шифры, шифры гаммирования.
3. Принципы построения криптографических алгоритмов.
4. Различие между программными и аппаратными реализациями шифров.
5. Функция Эйлера и Мебиуса.
6. Группы обратимых элементов в кольцах.
7. Структура мультипликативной группы кольца вычетов.
8. Обратимые элементы.
9. Примитивные элементы.
10. Особенности использования вычислительной техники в криптографии вопросы организации сетей засекреченной связи.
11. Криптографические хеш-функции.
12. Электронная подпись.
13. Криптографические протоколы.
14. Предмет и задачи программно-аппаратной защиты информации.
15. Идентификация субъекта, понятие протокола идентификации.
16. Пароли и ключи, организация хранения ключей.

7,2 Методические указания к самостоятельной подготовке студентов для вы-

полнения практических заданий лабораторных занятий

Для выполнения домашнего практического задания необходимо разобрать материал по соответствующей теме лабораторного занятия. При этом используются указания, данные преподавателем в ходе занятия, а также теоретико-практический материал, имеющийся в источниках из списка основной литературы. Если студент не смог понять приведенный в указанных источниках разбор типовых примеров в той степени, чтобы самостоятельно использовать предложенный алгоритм для решения задания, то он может получить консультацию преподавателя.

Список типовых практических заданий (для лабораторных занятий и зачета)

1. Применения и разработки шифровальных средств.
2. Применения электронной подписи.
3. Криптографические методы обеспечения информационной безопасности.
4. Алгоритмы проверки на простоту.
5. Эллиптические кривые над конечными полями.
6. Алгоритмы вычисления в конечных полях.
7. Электронная подпись по схеме Эль Гамала.
8. Электронная подпись на основе RSA.
9. Случайные и псевдослучайные гаммы.
10. Регистры сдвига с обратной связью.
11. Схема Файстеля.
12. Подсчет количества точек на эллиптической кривой.
13. Операция сложения на эллиптической кривой.
14. Схема алгоритма RSA.
15. Криптограммы, полученные при повторном использовании ключа.
16. Анализ криптограмм, полученных применением неравновероятной гаммы.
17. Стандарт РФ. ГОСТ 28147 – 89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
18. Стандарт РФ. ГОСТ Р 34.11–2012. Информационная технология. Криптографическая защита информации. Функция хэширования.
19. Стандарт РФ. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой.

7.3. Методические указания к самостоятельной подготовке студентов к выполнению контрольных работ

В течение семестра проводятся три контрольных работы, каждая из которых длится 45 минут и состоит из трех практических и одного теоретического задания. Тематика трех контрольных работ соответствует тематике трех содержательных разделов дисциплины: Каждое задание оценивается по пятибалльной шкале, высокая оценка ставится при получении не менее 16 баллов, нижний порог успешности составляет 7 баллов. Для подготовки к контрольной работе необходимо выполнять задания в ходе лабораторных занятий, а также домашние задания. В процессе самоподготовки студенту желательно ознакомиться с разбором опорных по рассматриваемым темам задач, имеющихся в пособиях из списка литературы. Выше в пункте 6.2 приведен список заданий, который включает в себя все типы практических заданий контрольных работ.

Примерные контрольные (самостоятельные) работы

1. Нахождение примитивного элемента конечного поля.
2. Построение таблицы логарифма Якоби конечного поля.
3. Решение систем линейных уравнений над конечным полем.
4. Алгоритм быстрого возведения в степень.
5. Нахождение обратных элементов в конечном поле.

6. Расширения конечных полей.
7. Алгоритм шифрования AES: структура поля $GF(2^8)$, нахождение обратных элементов.
8. Алгоритм шифрования AES: фактор кольцо $GF(2^8)[x]/\text{ид}((x+1)^4)$, преобразование столбцов.
9. Алгоритм шифрования AES: Линейное преобразование, собственные значения

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

матрицы

10. Алгоритм RSA – выбор секретных параметров p, q, d , вычисление открытого ключа n, e .
11. Рюкзачная система шифрования. Быстрорастущий вектор. Скрытие быстрорастущего вектора после преобразования умножения по модулю.
12. Решение систем линейных уравнений по разным модулям.
13. Решение систем линейных уравнений в кольце целых чисел.
14. Линейный регистр сдвига с обратной связью

$$S_{n+k} = a_{k-1}S_{n+k-1} + a_{k-2}S_{n+k-2} + \dots + a_1S_{n+1} + a_0S_n + a, n = 0, 1, 2, \dots$$

15. Характеристический многочлен регистра сдвига $x^k = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \dots + a_1x + a_0$

16. Нахождение явного вида значений регистра сдвига

$S_n = \beta_1\alpha_1^n + \beta_2\alpha_2^n + \dots + \beta_k\alpha_k^n, n = 0, 1, 2, \dots$, где $\alpha_1, \alpha_2, \dots, \alpha_k$ - корни характеристического многочлена, коэффициенты $\beta_1, \beta_2, \dots, \beta_k \in P$ являются решениями системы

$$\begin{cases} \beta_1\alpha_1^0 + \beta_2\alpha_2^0 + \dots + \beta_k\alpha_k^0 = S_0 \\ \beta_1\alpha_1^1 + \beta_2\alpha_2^1 + \dots + \beta_k\alpha_k^1 = S_1 \\ \dots \\ \beta_1\alpha_1^{k-1} + \beta_2\alpha_2^{k-1} + \dots + \beta_k\alpha_k^{k-1} = S_{k-1} \end{cases}.$$

17. Матрица линейного регистра сдвига

$$A = \begin{pmatrix} 0 & 0 & \dots & 0 & 0 & a_0 \\ 1 & 0 & \dots & 0 & 0 & a_1 \\ 0 & 1 & \dots & 0 & 0 & a_2 \\ 0 & 0 & \dots & 0 & 0 & a_3 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & a_{k-3} \\ 0 & 0 & \dots & 1 & 0 & a_{k-2} \\ 0 & 0 & \dots & 0 & 1 & a_{k-1} \end{pmatrix}$$

ее собственные значения и жорданова форма.

18. Квадратичный закон взаимности. Вычисление квадратичных вычетов и невычетов.
19. Извлечение квадратных корней по простому модулю $p \equiv 3(\text{mod } 4) \Rightarrow p = 4k + 3$.
20. Извлечение квадратных корней по простому модулю $p \equiv 1(\text{mod } 4) \Rightarrow p = 4k + 1$.

7.4. Методические рекомендации к самостоятельной подготовке студентов к реферативному докладу

Каждый студент должен подготовить в течение семестра реферативный доклад по одной из тем, предназначенной для самостоятельного изучения. Для подготовки доклада желательно кроме основных источников литературы использовать дополнительные источники, а также Интернет-ресурс. Доклад может быть представлен студентом на лабораторном занятии, возможно, в виде презентации, если тема занятия соответствует теме доклада. Также студент может представить отчет о подготовке реферативного доклада в письменной форме в конце семестра. Оформление письменного отчета должно удовлетворять требованиям: а) текст набирается 14 шрифтом на бумаге формата А 4; б) на титульном листе кроме темы также указывается факультет, направление (бакалавриат), курс, группа, ФИО студента; в) содержание материала по объему составляет 4-5 страниц; г) список литературы содержит не менее двух источников (возможно, из списка литературы в пункте 7).

Примерные темы реферативных докладов

1. Алгебраическое и вероятностное определение шифр системы.
2. Криптосистемы с открытым ключом.
3. Понятие сертификата.
4. Криптосистема RSA. Выбор параметров.
5. Шифр AES
6. ГОСТ -89
7. Криптографические хэш-функции. Стандарты ГОСТ Р 34.11-2012 и SHA.
8. Схема Эль-Гамала
9. Вычисления на эллиптической кривой.
10. Цифровая подпись. Схемы цифровой подписи.
11. Стандарты ГОСТ Р 34.
12. Стандарт DSS.
13. Анализ программного криптопродукта.

7.4. Методические указания к самостоятельной подготовке студентов к зачету

Согласно учебному плану дисциплины «Теоретико-числовые методы криптографии» итоговой формой контроля является зачет. Для допуска к зачету студент должен научиться на лабораторных занятиях решать практические задания по темам разделов 1-3 (табл. 4.1), выполнять домашние задания, а также успешно выполнить три контрольные работы. Типы практических заданий на зачет соответствуют заданиям из пункта 6.2. Также на зачете студентам предлагаются и теоретические задания, состоящие в письменном ответе на один из вопросов, приведенных в пункте 6.1. Количество практических и теоретических заданий зависит от активности и результативности работы студента в течение семестра. Если при условии хорошей посещаемости и активной работы на занятиях студент по трем контрольным работам и реферативному докладу заслужил высокие оценки, то он автоматически получает допуск к экзамену.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

8.1. Перечень информационных технологий.

не предусмотрены

8.2 Перечень необходимого программного обеспечения

а) перечень лицензионного программного обеспечения:

№	Производитель	Наименование
---	---------------	--------------

1	Microsoft	Microsoft Windows 8, 10
2	Microsoft	Microsoft Office Professional Plus
4	WolframResearch	Mathematica
5	MapleSoft	Maple 18
6	Mathworks	MATLAB Wavelet Toolbox

в) Перечень свободно распространяемого программного обеспечения

№	Перечень свободно распространяемого программного обеспечения
1.	Пакет компьютерной алгебры Sage 8.3. Официальный сайт http://sagemath.org/
2.	Пакет компьютерной алгебры Gap4r9p3. Официальный сайт http://www.gap-system.org/
3.	Пакет компьютерной алгебры PARI/GT 2.11. Официальный сайт http://pari.math.u-bordeaux.fr/
4.	Библиотека для работы с большими целыми числами GMP 6.1.2. Официальный сайт https://gmplib.org/
5.	Язык программирования Python. Официальный сайт https://www.python.org/
6.	Язык программирования Julia. Официальный сайт http://julialang.org/
7.	Язык программирования Cython. Официальный сайт http://cython.org/
8.	Компилятор PyPy, оптимизирующий код Python и Cython. Официальный сайт http://pypy.org/
9.	Python в облаке, интегрированная среда разработки Anaconda. Официальный сайт https://store.continuum.io/cshop/anaconda/
10.	Математические пакеты Python, проект SciPy. Официальный сайт http://www.scipy.org/
11.	Клиентская ОС Debian 9.5. Официальный сайт https://www.debian.org/index.ru.html
12.	Издательская система LaTeX/MiKTeX 2.9. Официальный сайт http://www.miktex.org/
13.	Утилиты Руссиновича https://technet.microsoft.com/ru-ru/library/bb545021.aspx
14.	Анализ защищенности сети Kali Linux 2018.3. https://www.kali.org/
15.	Анализ защищенности сети Snort 3.0. Официальный сайт https://www.snort.org/
16.	Офисная система Apache OpenOffice 4.1.5. Официальный сайт https://www.openoffice.org/ru/

8.3 Перечень необходимых информационных справочных систем

не предусмотрены

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
6.	Лекционные занятия	Лекционная аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук, ...) и соответствующим программным обеспечением (ПО)

7.	Лабораторные занятия	Специальное помещение, оснащенное доской, маркерами и мелом Компьютерные классы
8.	Групповые (индивидуальные) консультации	Аудитория (кабинет)
9.	Текущий контроль, промежуточная аттестация	Аудитория, (кабинет)
10.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета

7 семестр «МЕТОД БАЗИСНЫХ ПОТЕНЦИАЛОВ»

Объем трудоемкости: 4 зачетные единицы (144 часа, из них – 76,5 часа контактной работы (36 лекций, 36 часов лабораторных занятий, 4 часа КСР, 0,5 часов ИКР); 40,8 часа самостоятельной работы, 26,7 ч. контроль)

1 Цели и задачи изучения дисциплины (модуля).

1.1 Цель освоения дисциплины.

Целями освоения дисциплины «Дополнительные дисциплины для укрупненных групп специализаций и дисциплины специализаций» являются: подготовка в области применения современной вычислительной техники для решения практических задач математического и компьютерного моделирования, информатики; получение высшего профессионального (на уровне специалиста) образования, позволяющего выпускнику успешно работать в избранной сфере деятельности с применением современных компьютерных технологий.

1.2 Задачи дисциплины.

Задачи дисциплины: ознакомить студентов с возможностями современных компьютерных технологий для решения прикладных задач, операционными системами, современными информационными технологиями, научить применять современные информационные технологии на практике.

Получаемые знания необходимы для понимания и освоения всех курсов компьютерных наук.

1.3 Место дисциплины (модуля) в структуре образовательной программы.

Дисциплина «Дополнительные дисциплины для укрупненных групп специализаций и дисциплины специализаций» относится к вариативной части Блока 1 "Дисциплины (модули)" учебного плана.

Знания и умения, приобретенные студентами в результате изучения дисциплины, будут использоваться при изучении общих и специальных курсов, при выполнении курсовых работ, связанных с применением компьютерных технологий.

1.4 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы.

Изучение данной учебной дисциплины направлено на формирование у обучающихся компетенций

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	владеть
1.	ОПК-1	готовностью использовать фундаментальные знания в области математического анализа, комплексного и функционального анализа, алгебры, линейной алгебры, аналитической геометрии, дифференциальной геометрии и топологии, дифференциальных уравнений и уравнений в частных производных, дискретной математики, теории вероятностей, математической статистики и случайных процессов, численных методов, теоретической механики, механики сплошной среды, теории управления и оптимизации в будущей профессиональной деятельности	Вычислительные методы математической физики и математические модели основны физических, экономических, прочих процессов и явлений	решать стандартные задачи профессиональной деятельности на основе математической и программистской культуры	способностью решать стандартные задачи профессиональной деятельности
2	ПК-5	способностью использовать методы математического и алгоритмического моделирования при решении теоретических и прикладных задач	методы математического и алгоритмического моделирования	использовать методы математического и алгоритмического моделирования при решении теоретических и прикладных задач	навыками математического и алгоритмического моделирования при решении теоретических и прикладных задач

2. Структура и содержание дисциплины.

2.1 Распределение трудоёмкости дисциплины по видам работ.

Общая трудоёмкость дисциплины составляет 4зач.ед. (144 часа), их распределение по видам работ представлено в таблице

Вид учебной работы	Всего ча-	Семестры (часы)
--------------------	-----------	-----------------

	сов	7-й
Контактная работа, в том числе:		
Аудиторные занятия (всего)	72	72
Занятия лекционного типа	36	36
Занятия семинарского типа (семинары, практические занятия)		
Лабораторные занятия	36	36
Иная контактная работа:		
Контроль самостоятельной работы (КСР)	4	4
Промежуточная аттестация (ИКР)	0,5	0,5
Самостоятельная работа, в том числе:		
Проработка учебного (теоретического) материала	40,8	40,8
Подготовка к текущему контролю	26,7	26,7
Общая трудоемкость	час.	144
	в том числе контактная работа	76,5
	зач. ед	4

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
Разделы дисциплины, изучаемые в 7 семестре

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Вне-аудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
7-й семестр						
1	Проектирование вектора на конечномерное подпространство	26	8		8	10
2	Гармонические функции	30	10		10	10
3	Метод базисных потенциалов	26	8		8	10
4	Обратные задачи потенциала	30,8	10		10	10,8
	<i>Итого по дисциплине:</i>		36		36	40,8

Примечание: Л – лекции, ПЗ – практические занятия / семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа студента

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа.

№	Наименование раздела	Содержание раздела	Форма текущего контроля
---	----------------------	--------------------	-------------------------

1	2	3	4
7-й семестр			
1	Проектирование вектора на конечномерное подпространство	Евклидово и гильбертово пространства. Матрица Грама. Неврожденность определителя. Пространство L_2	
2	Гармонические функции	Принцип максимума для гармонических функций. Аналитичность гармонических функций. Задача Дирихле. Интегральное представление гармонических функций	
3	Метод базисных потенциалов	Структура метода. Основные определения. Линейная независимость базисных потенциалов. Полнота системы базисных потенциалов.	
4	Обратные задачи потенциала	Обратная задача объемного потенциала. Теорема Новикова. Приложения.	

2.3.2 Занятия семинарского типа.

Занятия семинарского типа не предусмотрены

2.3.3 Лабораторные занятия.

№	Наименование лабораторных работ	Форма текущего контроля
1	3	4
7-й семестр		
1	Проектирование на конечномерную гиперплоскость	ЛР
2	Численное решение СЛАУ	ЛР
3	Вычисление интегралов	ЛР
4	Численное решение внутренней задачи Дирихле для уравнения Лапласа методом базисных потенциалов	ЛР
5	Вторая и третья внутренние краевые задачи для уравнения Лапласа. Решение методом базисных потенциалов.	ЛР
6	Конечно-разностные методы решения краевых задач для уравнения Лапласа	ЛР
7	Применение модифицированные системы базисных функций.	ЛР
8	Обратная задача объемного потенциала.	ЛР
9	Выделение гармонической составляющей.	ЛР

Защита лабораторной работы (ЛР), выполнение курсового проекта (КП), курсовой работы (КР), расчетно-графического задания (РГЗ), написание реферата (Р), эссе (Э), коллоквиум (К), тестирование (Т) и т.д.

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Проработка учеб-	Литература из основного и дополнительного списков

	ного (теоретического) материала	
2	Подготовка к текущему контролю	Образцы программ по темам лабораторных занятий в электронном виде

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в форме электронного документа,

Для лиц с нарушениями слуха:

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в форме электронного документа,

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3. Образовательные технологии.

Лекции, лабораторные занятия, контрольные работы, зачет.

Разбор практических задач и примеров, моделирование ситуаций, приводящих к тем или иным ошибкам в программе, выработка навыков выявления и исправления ошибок в процессе написания программы. Построение тестовых примеров для выявления ошибок в программе и сравнения эффективности различных алгоритмов.

Используемые интерактивные образовательные технологии:

Се- мест р	Вид занятия	Используемые интерактивные образовательные технологии	Кол-во часов
7	Лабораторные занятия	Дискуссия на тему: «Интегральные операторы теории потенциала. Фундаментальное решение уравнения Лапласа. Потенциалы простого и двойного слоя, объемный потенциал»	6
		Дискуссия на тему: «Потенциал Робена. Интегральные операторы. Представление функций потенциалами. Лемма Новикова»	6
		Дискуссия на тему: «Внутренняя и внешняя задача Дирихле для уравнения Лапласа и Пуассона. Внутренняя задача и внешняя задача Неймана для уравнения Лапласа и уравнения Пуассона»	6
Итого:			18

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Фонд оценочных средств дисциплины состоит из средств текущего контроля выполнения заданий лабораторных работ, средств для итоговой аттестации (зачета, экзамена).

Задания для самостоятельной работы

Теоретические вопросы:

- 1) Изложите метод математического моделирования физических процессов.
- 2) Изложите постановку краевых задач математической физики.
- 3) Докажите существование и единственность решения краевых задач математической физики.
- 4) Поясните понятия корректности и некорректности.
- 5) Изложите постановку обратных задач математической физики
- 6) Расскажите про интегральные операторы теории потенциала.
- 7) Изложите фундаментальное решение уравнения Лапласа.
- 8) Изложите потенциал Робена.
- 9) Изложите представление функций потенциалами.
- 10) Изложите лемму Новикова.
- 11) Объясните полноту сдвигов фундаментального решения уравнения Лапласа в подпространстве гармонических функций.
- 12) Изложите системы потенциалов, полные на границе области.
- 13) Докажите полноту модифицированных систем полученных из фундаментального решения.
- 14) Приведите классификацию дифференциальных уравнений в частных производных.
- 15) Выведите уравнение теплопроводности.
- 16) Дайте понятие эллиптического уравнения.
- 17) Изложите алгоритм задачи Робена.
- 18) Изложите алгоритм внутренней и внешней задачи Дирихле для уравнения Лапласа и Пуассона.
- 19) Изложите алгоритм внутренней задачи и внешней задачи Неймана для уравнения Лапласа и уравнения Пуассона.
- 20) Изложите алгоритм задачи граничного управления температурой.
- 21) Выведите волновое уравнение.

Лабораторные задания:

- 1) Математическое моделирование физических процессов.
- 2) Математическая физика. Постановка краевых задач. Существование и единственность решения.
- 3) Корректность и некорректность. Обратные задачи.
- 4) Классификация дифференциальных уравнений в частных производных.
- 5) Уравнение теплопроводности, волновое уравнение, стационарные процессы и эллиптические уравнения.
- 6) Интегральные операторы теории потенциала.
- 7) Фундаментальное решение уравнения Лапласа.
- 8) Потенциалы простого и двойного слоя, объемный потенциал.
- 9) Потенциал Робена. Интегральные операторы.
- 10) Представление функций потенциалами. Лемма Новикова.
- 11) Полнота сдвигов фундаментального решения уравнения Лапласа в подпространстве гармонических функций.
- 12) Системы потенциалов, полные на границе области. Полнота модифицированных систем полученных из фундаментального решения
- 13) Алгоритм задачи Робена.
- 14) Внутренняя и внешняя задача Дирихле для уравнения Лапласа и Пуассона.
- 15) Внутренняя задача и внешняя задача Неймана для уравнения Лапласа и уравнения Пуассона.
- 16) Граничное управление температурой. Бигармоническое уравнение

Экзаменационные материалы для промежуточной аттестации (экзамен, 7 семестр)

- 1) Математическое моделирование физических процессов.

- 2) Математическая физика.
- 3) Постановка краевых задач.
- 4) Существование и единственность решения.
- 5) Корректность и некорректность.
- 6) Обратные задачи.
- 7) Классификация дифференциальных уравнений в частных производных.
- 8) Уравнение теплопроводности.
- 9) Волновое уравнение.
- 10) Стационарные процессы.
- 11) Эллиптические уравнения.
- 12) Интегральные операторы теории потенциала.
- 13) Фундаментальное решение уравнения Лапласа.
- 14) Потенциалы простого и двойного слоя.
- 15) Объемный потенциал.
- 16) Потенциал Робена.
- 17) Интегральные операторы.
- 18) Представление функций потенциалами.
- 19) Лемма Новикова.
- 20) Полнота сдвигов фундаментального решения уравнения Лапласа в подпространстве гармонических функций.
- 21) Системы потенциалов, полные на границе области.
- 22) Полнота модифицированных систем полученных из фундаментального решения.
- 23) Алгоритм задачи Робена.
- 24) Внутренняя и внешняя задача Дирихле для уравнения Лапласа и Пуассона.
- 25) Внутренняя задача и внешняя задача Неймана для уравнения Лапласа и уравнения Пуассона.
- 26) Граничное управление температурой.
- 27) Бигармоническое уравнение.

Виды самостоятельной работы

Обязательными при изучении дисциплины являются следующие виды самостоятельной работы:

- разбор и самостоятельное изучение теоретического материала по конспектам лекций и по учебным пособиям из списка источников литературы;
- подготовка к зачету.
- подготовка к экзамену
- подготовка курсовой работы

4.1. Методические указания к самостоятельному изучению студентами теоретического материала

Весь теоретический материал, необходимый для сдачи зачета, содержится в учебных пособиях из списка основной литературы. В случае затруднений, возникающих у студентов в процессе самостоятельного изучения теории, преподаватель разъясняет сложные моменты на консультациях.

4.2. Методические указания к самостоятельной подготовке студентов к выполнению заданий по темам практических занятий

Для выполнения практического задания необходимо разобрать материал по соответствующей теме практического занятия. При этом используются указания, данные преподавателем в ходе занятия, а также теоретический материал из списка основной литературы. Если студент не смог понять приведенный в указанных задачниках материал, то он может получить консультацию преподавателя.

4.3. Методические указания к самостоятельной подготовке студентов к выполнению лабораторных работ

Лабораторные работы выполняются, как правило, в компьютерном классе. Отдельные работы могут выполняться в аудитории при наличии у студентов портативных компьютеров.

На лабораторных занятиях изучаются вопросы практического использования возможностей компьютера для решения поставленной задачи. Студент должен правильно выбрать необходимые средства для решения задачи, решить задачу, проверить правильность полученного решения. По отдельным темам студентам поручается выступить с докладами на занятиях.

Вопросы к экзамену

1. Пространства со скалярным произведением. Гильбертово пространство.
2. Проекция вектора на конечномерное подпространство.
3. Доказательство невырожденности матрицы Грама.
4. Решение систем линейных уравнений. Метод Гаусса.
5. Численное интегрирование. Методы прямоугольников, трапеций, Симпсона.
6. Гармонические функции. Принцип максимума гармонических функций.
7. Фундаментальное решение уравнения Лапласа.
8. Интегральное представление функций
9. Бесконечная дифференцируемость гармонической функции
10. Оценка производных гармонической функции
11. Аналитичность гармонической функции
12. Системы базисных потенциалов. Линейная независимость.
13. Пространство L_2
14. Точки Лебега.
15. Потенциал простого слоя. Непрерывность.
16. Потенциал простого слоя. Разрыв нормальной производной.
17. Полнота системы базисных функций в L_2
18. Соболевские пространства W_2^1 .
18. Задача Дирихле для уравнения Лапласа. Классическая и обобщенная постановки.
19. Задача Неймана для уравнения Лапласа. Классическая и обобщенная постановки.
20. Задача Робена для уравнения Лапласа. Классическая и обобщенные постановки.
21. Решение задачи Дирихле для уравнения Лапласа методом базисных потенциалов.
22. Решение задачи Неймана для уравнения Лапласа методом базисных потенциалов.
23. Решение задачи Робена для уравнения Лапласа методом базисных потенциалов.
24. Префиксное кодирование. Двоичные деревья.
25. Оптимальное префиксное кодирование. Код Хаффмана.
26. Арифметическое кодирование. Нюансы реализации.
27. Сжатие изображений. JPEG.
28. Двойное косинус преобразование.
29. Квантование.
30. Сингулярное разложение.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля).

5.1 Основная литература:

1. Розендорн, Э.Р. Уравнения с частными производными : учебник / Э.Р. Розендорн, Е.С. Соболева, Г.М. Фатеева ; ред. Э.Р. Розендорна. - 2-е изд., стер. - Москва : Физматлит, 2017. - 334 с. : ил. - Библиогр.: с. 324-325. - ISBN 978-5-9221-1756-2 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=485339>.

2. Ильин, А.М. Уравнения математической физики : учебное пособие / А.М. Ильин. - Москва : Физматлит, 2009. - 192 с. - ISBN 978-5-9221-1036-5 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=69318>

5.2 Дополнительная литература:

1, Полянин, А. Д. Нелинейные уравнения математической физики и механики. / А. Д. Полянин, В. Ф. Зайцев, А. И. Журов. — 2-е изд., испр. и доп. — М. : Издательство Юрайт, 2018. — 256 с. — (Серия : Бакалавр. Академический курс). — ISBN 978-5-534-02317-6. — Режим доступа : www.biblio-online.ru/book/BA8375FD-BC61-4F27-98E2-27AF3AFDF2E4.

2. Карчевский, М.М. Уравнения математической физики. Дополнительные главы [Электронный ресурс] : учебное пособие / М.М. Карчевский, М.Ф. Павлова. — Электрон. дан. — Санкт-Петербург : Лань, 2016. — 276 с. — Режим доступа: <https://e.lanbook.com/book/72983>

Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровья имеются издания в электронном виде в электронно-библиотечных системах.

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», в том числе современные профессиональные базы данных и информационные справочные системы, необходимые для освоения дисциплины (модуля).

1. База данных Научной электронной библиотеки eLIBRARY.RU <https://elibrary.ru/>

2. База данных Всероссийского института научной и технической информации (ВИНИТИ) РАН <http://www2.viniti.ru/>

7. Методические указания для обучающихся по освоению дисциплины (модуля).

По курсу предусмотрено проведение лекционных занятий, на которых дается основной теоретический материал, рассматриваются основные приёмы решения задач и решаются примеры практических задач.

На лабораторных занятиях студенты, решая семестровые задания, приобретают практические навыки применения компьютерных технологий, написания и отладки программ, программной реализации алгоритмов.

Важнейшим этапом курса является самостоятельная работа по дисциплине, во время которой студенты осуществляют проработку необходимого материала, используя литературу из основного и дополнительного списков, готовятся к текущему контролю, изучая примеры задач, рассмотренных на лекциях и на практических занятиях, и образцы программ по темам лабораторных занятий (выдаются студентам в электронном виде).

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю).

8.1 Перечень информационных технологий.

Освоение курса предполагает теоретическое изучение компьютерных технологий и проведение практических занятий с использованием компьютера.

8.2 Перечень необходимого лицензионного программного обеспечения.

MicrosoftOffice

MathCad

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащённость
1.	Лекционные занятия	Лекционная аудитория, оснащённая презентационной техникой (проектор, экран, компьютер/ноутбук, ...) и соответствующим программным обеспечением (ПО)
2.	Лабораторные занятия	Специальное помещение, оснащённое доской, маркерами и мелом , Компьютерные классы
3.	Групповые (индивидуальные) консультации	Аудитория (кабинет)
4.	Текущий контроль, промежуточная аттестация	Аудитория, (кабинет)
5.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащённый компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета.

8 семестр «ОБРАБОТКА ДАННЫХ, ИЗОБРАЖЕНИЙ И ЗВУКА»

Объем трудоемкости: 4 зачетные единицы (144 часа, из них – 76,5 часа контактной работы (36 лекций, 36 часов лабораторных занятий, 11 часа КСР, 0,3 часов ИКР); 34 часа самостоятельной работы, 26,7 ч. контроль)

1.1 Цель освоения дисциплины.

Целями освоения дисциплины «Дополнительные дисциплины для укрупненных групп специализаций и дисциплины специализаций» являются: подготовка в области применения современной вычислительной техники для решения практических задач математического и компьютерного моделирования, информатики; получение высшего профессионального (на уровне специалиста) образования, позволяющего выпускнику успешно работать в избранной сфере деятельности с применением современных компьютерных технологий.

1.2 Задачи дисциплины.

Задачи дисциплины: ознакомить студентов с возможностями современных компьютерных технологий для решения прикладных задач, операционными системами, современными информационными технологиями, научить применять современные информационные технологии на практике.

Получаемые знания необходимы для понимания и освоения всех курсов компьютерных наук.

1.3 Место дисциплины (модуля) в структуре образовательной программы.

Дисциплина «Дополнительные дисциплины для укрупненных групп специализаций и дисциплины специализаций» относится к вариативной части Блока 1 "Дисциплины (модули)" учебного плана.

Знания и умения, приобретенные студентами в результате изучения дисциплины, будут использоваться при изучении общих и специальных курсов, при выполнении курсовых работ, связанных с применением компьютерных технологий.

1.4 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы.

Изучение данной учебной дисциплины направлено на формирование у обучающихся компетенций

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	владеть
1.	ОПК-1	готовностью использовать фундаментальные знания в области математического анализа, комплексного и функционального анализа, алгебры, линейной алгебры, аналитической геометрии, дифференциальной геометрии и топологии, дифференциальных уравнений и уравнений в частных производных, дис-	Вычислительные методы математической физики и математические модели основны физических, экономических, прочих процессов и явлений	решать стандартные задачи профессиональной деятельности на основе математической и программистской культуры	способностью решать стандартные задачи профессиональной деятельности

№ п.п.	Индекс компетенции	Содержание компетенции (или её части)	В результате изучения учебной дисциплины обучающиеся должны		
			знать	уметь	владеть
		кретной математики, теории вероятностей, математической статистики и случайных процессов, численных методов, теоретической механики, механики сплошной среды, теории управления и оптимизации в будущей профессиональной деятельности			
2	ПК-5	способностью использовать методы математического и алгоритмического моделирования при решении теоретических и прикладных задач	методы математического и алгоритмического моделирования	использовать методы математического и алгоритмического моделирования при решении теоретических и прикладных задач	навыками математического и алгоритмического моделирования при решении теоретических и прикладных задач

2. Структура и содержание дисциплины.

2.1 Распределение трудоёмкости дисциплины по видам работ.

Общая трудоёмкость дисциплины составляет 4 зач.ед. (144сов), их распределение по видам работ представлено в таблице

Вид учебной работы	Всего часов	Семестры (часы)
		8-й
Контактная работа, в том числе:		
Аудиторные занятия (всего)	74	74
Занятия лекционного типа	36	36
Занятия семинарского типа (семинары, практические занятия)		
Лабораторные занятия	36	36
Иная контактная работа:		
Контроль самостоятельной работы (КСР)	11	11
в том числе Курсовая работа	7	7
Промежуточная аттестация (ИКР)	0,3	0,3
Самостоятельная работа, в том числе:		

Курсовая работа (подготовка и написание)	14	14
Проработка учебного (теоретического) материала	20	20
Подготовка к текущему контролю	26,7	26,7
Общая трудоемкость	144	144
	76,3	76,3
	4	4

2.2 Структура дисциплины:

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы дисциплины, изучаемые в 8 семестре

№	Наименование разделов	Количество часов				
		Всего	Аудиторная работа			Вне-аудиторная работа
			Л	ПЗ	ЛР	СРС
1	2	3	4	5	6	7
8-й семестр						
1	Методы сжатия без потерь	27	8		10	9
2	Сжатие изображений	27	10		8	9
3	Обработка изображений	27	8		10	9
4	Вейвлетные методы сжатия изображений	25	10		8	7
	<i>Итого по дисциплине:</i>		36		36	34

Примечание: Л – лекции, ПЗ – практические занятия / семинары, ЛР – лабораторные занятия, СРС – самостоятельная работа студента

2.3 Содержание разделов дисциплины:

2.3.1 Занятия лекционного типа.

№	Наименование раздела	Содержание раздела	Форма текущего контроля
1	2	3	4
8-й семестр			
1	Методы сжатия без потерь	Коды переменной длины. Кодирование Хаффмана. Адаптивные коды Хаффмана. Арифметическое кодирование.	
2	Сжатие изображений	Словарные методы LZ77, LZSS, LZW. Сжатие изображений JPEG. DCT. Преобразование изображений.	
3	Обработка изображений	Классические модели: радиоактивный распад, размножение бактерий, «хищник-жертва», война двух армий. Применение ЭВМ в процессе моделирования.	
4	Вейвлетные методы сжатия изображений	Преобразование Хаара. Преобразование DWT. Вейвлеты Добеши. SPIHT.	

2.3.2 Занятия семинарского типа.

Занятия семинарского типа не предусмотрены

№	Наименование лабораторных работ	Форма текущего контроля
1	3	4
8-й семестр		
1	Построение оптимального префиксного кода	ЛР
2	Арифметическое кодирование	ЛР
3	Словарные методы LZ77, LZSS, LZW	ЛР
4	Сжатие изображений JPEG	ЛР
5	SVD в сжатии изображений	ЛР
6	Размытие и контрастирование изображений	ЛР
7	Наложение изображений	ЛР
8	Вычисление вейвлет-преобразований	ЛР
9	Сжатие изображений. SPIHT	ЛР

Защита лабораторной работы (ЛР), выполнение курсового проекта (КП), курсовой работы (КР), расчетно-графического задания (РГЗ), написание реферата (Р), эссе (Э), коллоквиум (К), тестирование (Т) и т.д.

2.3.4 Примерная тематика курсовых работ (проектов)

- 1 Кодирование и декодирование Хаффмана
- 2 Адаптивные коды Хаффмана: несжатые коды, модификация дерева, переполнение счетчика, кодовое переполнение, вариант алгоритма
- 3 Факсимильное сжатие. Одномерное и двумерное кодирование
- 4 Арифметическое кодирование: детали реализации метода, потеря значащих цифр
- 5 Коды Гаррея
- 6 Ортогональные и матричные преобразования изображений
- 7 Дискретные синус- и косинус-преобразования изображений
- 8 Кодирование и квантование JPEG
- 9 Коды Голомба для JPEG-LS
- 10 Основные принципы сжатия видео
- 11 Кодирование частотной области звука
- 12 Психоакустические модели

2.4 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

№	Вид СРС	Перечень учебно-методического обеспечения дисциплины по выполнению самостоятельной работы
1	2	3
1	Проработка учебного (теоретического) материала	Литература из основного и дополнительного списков
2	Подготовка к текущему контролю	Образцы программ по темам лабораторных занятий в электронном виде

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- Для лиц с нарушениями зрения:
- в форме электронного документа,
- Для лиц с нарушениями слуха:

– в форме электронного документа.
 Для лиц с нарушениями опорно-двигательного аппарата:
 – в форме электронного документа,
 Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

3. Образовательные технологии.

Лекции, лабораторные занятия, контрольные работы, зачет.

Разбор практических задач и примеров, моделирование ситуаций, приводящих к тем или иным ошибкам в программе, выработка навыков выявления и исправления ошибок в процессе написания программы. Построение тестовых примеров для выявления ошибок в программе и сравнения эффективности различных алгоритмов.

Используемые интерактивные образовательные технологии:

Се- мест р	Вид занятия	Используемые интерактивные образовательные технологии	Кол-во часов
8	Лекционные занятия	Проблемная лекция: «Поворот изображения. Масштабирование. Проблема повторного квантования»	6
		Проблемная лекция: «Задача обращения аппаратной функции. Рефокусировка. Томография. Задача шумоподавления»	6
		Проблемная лекция: «Объектная сегментация изображений. Цветовая сегментация»	6
8	Лабораторные занятия	Дискуссия на тему: «Дифференцирование изображения. Псевдоградиент Ди Зензо. Свёртки. Быстрые свёртки с полиномами»	6
		Дискуссия на тему: «Винеровская фильтрация»	6
		Дискуссия на тему: «Сжатие изображений. Сжатие без потерь: RLE (PCX, TIFF), Хаффмана (TIFF), LZW (TIFF, GIF, PNG), арифметическое кодирование»	6
Итого:			36

Для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

4. Оценочные средства для текущего контроля успеваемости и промежуточной аттестации

Фонд оценочных средств дисциплины состоит из средств текущего контроля выполнения заданий лабораторных работ, средств для итоговой аттестации (экзамена).

Текущий контроль (Индивидуальное задание №1)

1. Выбрать из библиотеки сканов один из предназначенных для проведения работы образцов: образец с периодической структурой или любой другой по выбору преподавателя.

2. Построить Фурье-спектр изображения. Провести обработку полученного изображения. Выполнить фильтрацию изображения. Измерить и сравнить параметры шероховатости изображений до и после фильтрации. Измерить величины преобладающих пространственных частот спектра, сравнить соответствующие этим частотам периоды повторения элементов изображения с интервалами, полученными при измерениях на изображе-

нии. Определить углы между направлениями на изображении двумя способами и сравнить результаты.

В результате обработки Фурье-спектра можно сделать вывод о наличии периодичности структуры, её ориентации относительно осей исходного изображения, а также о величине преобладающих частот в периодичности структуры на анализируемом изображении.

3. Построить вейвлет-спектр изображения. Провести обработку полученного изображения.

4. Пройти собеседование по выполненной работе.

Примеры вопросов к собеседованию.

1. Какие типы искажений характерны для СЗМ изображений и по каким причинам они возникают?

2. Каковы основные методы фильтрации СЗМ изображений?

3. Назовите некоторые методы определения количественных характеристик изображений.

4. Для каких изображений следует воспользоваться частотным представлением?

5. Какую информацию об изображении можно получить по его Фурье-образу?

Текущий контроль (Индивидуальное задание №2)

Отделение объектов от фона и разрезание на сегменты

Дана пиксельная фотография. Необходимо отделить фон от изображений каждого зерна и разрезать изображение на сегменты, содержащие единичные зёрна, например:

Задание по работе

1. Необходимо отделить фон от изображений каждого зерна средствами Wolfram Mathematica, MatLab или OpenCV и т.п., операторами сегментации и выделения связных компонент.

2. Бинаризованное изображение «фон-объект» разрезать на сегменты, содержащие единичные зёрна:

3. Пройти собеседование по выполненной работе.

(Индивидуальное задание №3)

Распознавание цифр номера автомобиля

В данном задании необходимо разработать функцию(модуль), выделяющую и распознающую цифровой код автомобиля. Цифровой код - это три основные цифры номера, без кода региона. В функции должен быть реализован метод выделения областей цифр на изображении знака, и два метода распознавания цифр. Первый метод должен использовать классификатор, основанный на геометрических признаках сегментов цифр. Второй метод должен основываться на сопоставлении с шаблоном.

Индивидуальное задание №4 Распознавание дорожных знаков

Целью задания является знакомство с одним из популярных подходов к распознаванию объектов, основанном на использовании классификатора SVM и дескриптора HOG. Реализовать метод классификации знаков дорожного движения по схеме linear SVM + HOG. Алгоритм должен быть реализован в виде функции со следующей сигнатурой: `class = recognize_sign(img, model, mode)`, где

1. `img` - цветное изображение знака

2. `model` - модель классификатора. Будет подгружена один раз с помощью вызова функции `load(model_path, 'model')`. Для базового варианта файл модели должен называться `model_base.mat`, для бонусного - `model_bonus.mat`

3. `mode` - число `uint`, показывающее какую часть задания запускать. 0 - базовая часть задания, 1 - бонусная часть задания

4. class - строка, обозначающая распознанный класс дорожного знака

Материалы к собеседованию.

1. ФИО: <Фамилия Имя Отчество> Группа: <номер группы>
2. Задание: <номер задания> / <название задания>
3. Система: <система программирования> ОС: <операционная система>
4. Затраченное время: укажите, сколько потратили времени на выполнение задания, на что ушло больше всего и т.д.
5. Комментарии: <комментарии по реализации / пожелания / впечатления и т.д.>
6. Ответы на вопросы:
 - Краткое описание особенностей вашего алгоритма
 - Какой размер изображений был использован в распознавании?
 - С какими трудностями вы столкнулись при выполнении задания?
 - Какой точности вам удалось достичь на скользящем контроле на выданных вам данных?

ВОПРОСЫ К ЭКЗАМЕНУ

1. Каким образом осуществляется дискретизация сигнала?
2. Как выбирается величина шага дискретизации?
3. Каким образом осуществляется квантование изображения?
4. В чем заключается алгоритм двумерной свертки?
5. В каких функциях присутствует алгоритм двумерной свертки?
6. В чем отличие алгоритма медианной фильтрации от алгоритма фильтрации с помощью операции усреднения с порогом?
7. Какие типы шумов формирует функция по зашумлению изображений `imnoise`?
8. Для каких целей можно использовать функцию `freqz2`?
9. Каким образом можно сформировать маску линейного фильтра по желаемой АЧХ?
10. Какая функция позволяет сформировать двумерный фильтр из одномерного?
11. Что обуславливает искажения изображения при его формировании?
12. Какие функции использовались для моделирования «размытия» изображения и его восстановления в задании лабораторной работы?
13. Какие принципы лежат в основе построения фильтров Винера, гомоморфного фильтра?
14. Какие логические операции над бинарными изображениями вы знаете?
15. Какие морфологические операции обработки изображения относятся к базовым?
16. Какие операции являются комбинированием эрозии и дилатации?
17. Какие функции пакета ИРТ выполняют операции эрозии и дилатации, замыкания, размыкания?
18. В чем заключается сегментация изображения?
19. Какие признаки используются для сегментации?
20. В чем заключается метод выращивания областей, использующийся для сегментации изображения?
21. В чем заключается метод разделения, использующийся для сегментации изображения?
22. Что является входными параметрами функции сегментации методом разделения?
23. В чем заключается преобразование яркостного среза?
24. Какие параметры возвращает функция `imrpxel`?
25. Какие функции используются для выполнения двумерного прямого и обратного преобразования Фурье в системе MatLab?
26. Зачем используется двумерная дискретизация? Приведите примеры функции дискретизации. Чем назначение структурообразующего элемента в морфологических операциях?
27. Для чего используются морфологические операции?

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля).

5.1 Основная литература:

1.. Современные компьютерные технологии : учебное пособие / Р.Г. Хисматов, Р.Г. Сафин, Д.В. Тунцев, Н.Ф. Тимербаев ; Министерство образования и науки России, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Казанский национальный исследовательский технологический университет». - Казань : Издательство КНИТУ, 2014. - 83 с. : схем. - Библиогр. в кн. - ISBN 978-5-7882-1559-4 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=428016>

2. Сжатие цифровых изображений [Электронный ресурс] : учебное пособие / О.О. Евсютин [и др.]. — Электрон. дан. — Москва : Горячая линия-Телеком, 2013. — 124 с. — Режим доступа: <https://e.lanbook.com/book/55671>

3. Кирнос, В.Н. Информатика II. Основы алгоритмизации и программирования на языке C++ : учебно-методическое пособие / В.Н. Кирнос ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - Томск : Эль Контент, 2013. - 160 с. : ил.,табл., схем. - ISBN 978-5-4332-0068-5 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=208651>

5.2 Дополнительная литература:

1. Окулов, С.М. Динамическое программирование / С.М. Окулов, О.А. Пестов. – М. : Издательство "Лаборатория знаний", 2015. – 299 с. – ISBN 978-5-9963-2572-6. – [Электронный ресурс]. – URL: <http://e.lanbook.com/book/66114>

2. Огнева, М. В. Программирование на языке c++: практический курс : учебное пособие для бакалавриата и специалитета / М. В. Огнева, Е. В. Кудрина. — М. : Издательство Юрайт, 2018. — 335 с. — (Серия : Бакалавр и специалист). — ISBN 978-5-534-05123-0. — URL: <https://biblio-online.ru/book/7670D7EC-AC37-4675-8EAE-DD671BC6D0E4/programmirovanie-na-yazyke-s-prakticheskiy-kurs>

3. Кирнос, В.Н. Информатика II. Основы алгоритмизации и программирования на языке C++ : учебно-методическое пособие / В.Н. Кирнос ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - Томск : Эль Контент, 2013. - 160 с. : ил.,табл., схем. - ISBN 978-5-4332-0068-5 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=20865>

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», в том числе современные профессиональные базы данных и информационные справочные системы, необходимые для освоения дисциплины (модуля).

3. База данных Научной электронной библиотеки eLIBRARY.RU <https://elibrary.ru/>

4. База данных Всероссийского института научной и технической информации (ВИНИТИ) РАН <http://www2.viniti.ru/>

7. Методические указания для обучающихся по освоению дисциплины (модуля).

По курсу предусмотрено проведение лекционных занятий, на которых дается основной теоретический материал, рассматриваются основные приёмы решения задач и решаются примеры практических задач.

На лабораторных занятиях студенты, решая семестровые задания, приобретают практические навыки применения компьютерных технологий, написания и отладки программ, программной реализации алгоритмов.

Важнейшим этапом курса является самостоятельная работа по дисциплине, во время которой студенты осуществляют проработку необходимого материала, используя

литературу из основного и дополнительного списков, готовятся к текущему контролю, изучая примеры задач, рассмотренных на лекциях и на практических занятиях, и образцы программ по темам лабораторных занятий (выдаются студентам в электронном виде).

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю).

8.1 Перечень информационных технологий.

Освоение курса предполагает теоретическое изучение компьютерных технологий и проведение практических занятий с использованием компьютера.

7.2 Перечень необходимого лицензионного программного обеспечения.

Microsoft Office

MathCad

8. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)

№	Вид работ	Материально-техническое обеспечение дисциплины (модуля) и оснащенность
1.	Лекционные занятия	Лекционная аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук, ...) и соответствующим программным обеспечением (ПО)
2.	Лабораторные занятия	Специальное помещение, оснащенное доской, маркерами и мелом , Компьютерные классы
3.	Групповые (индивидуальные) консультации	Аудитория (кабинет)
4.	Курсовое проектирование	Кабинет для выполнения курсовых работ
5.	Текущий контроль, промежуточная аттестация	Аудитория, (кабинет)
6.	Самостоятельная работа	Кабинет для самостоятельной работы, оснащенный компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета.

Рецензия

на рабочую программу дисциплины «Дополнительные дисциплины для укрупненных групп специализаций и дисциплины специализаций», предназначенную для студентов специальности

01.05.01 Фундаментальные математика и механика

Изучение различных разделов и приложений методов математического моделирования является неотъемлемой частью подготовки квалифицированного математика. «Дополнительные дисциплины для укрупненных групп специализаций и дисциплины специализаций» объединяют в себе несколько дисциплин, описывающих использование математических методов в различных прикладных разделах. Поэтому создание рабочей программы по данному курсу является актуальным.

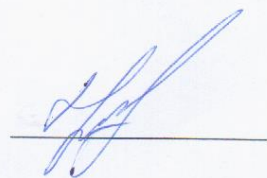
Представленная на рецензию программа описывает требования к уровню усвоения дисциплины, объем учебных часов и их распределение по формам занятий, требования к обязательному минимуму содержания программы, перечень литературы и пособий, формы контроля. Содержание теоретического материала дисциплины полно отражает необходимые знания для формирования компетенций по дисциплине. Материалы для самостоятельной учебной работы студентов содержат основные теоретические положения, необходимые для усвоения указанных тем. Список рекомендуемой литературы содержит основные современные источники отечественных авторов. Критерии оценок по дисциплине отражают необходимые компетенции, которые должны быть сформированы у студентов.

Разработанная рабочая программа дисциплины «Дополнительные дисциплины для укрупненных групп специализаций и дисциплины специализаций» соответствует требованиям ФГОС ВО и способствует качественному овладению обучающимися необходимыми компетенциями.

Считаю, что данная программа соответствует современному уровню подготовки специалистов по специальности 01.05.01 «Фундаментальные математика и механика» и может быть рекомендована для обеспечения основной образовательной программы по дисциплине «Дополнительные дисциплины для укрупненных групп специализаций и дисциплины специализаций» для студентов специальности 01.05.01 «Фундаментальные математика и механика».

Рецензент

Доктор технических наук, профессор
кафедры прикладной математики
ФГБОУ ВО «Кубанский государственный
технологический университет»



Наумова Н.А.



Рецензия

на рабочую программу дисциплины «Дополнительные дисциплины для укрупненных групп специализаций и дисциплины специализаций», предназначенную для студентов специальности
01.05.01 Фундаментальные математика и механика

Изучение различных аспектов приложения математики в естественных науках является важным для подготовки квалифицированного специалиста в области математики. Поэтому создание рабочей программы по данному курсу является актуальным.

Рабочая программа дисциплины «Дополнительные дисциплины для укрупненных групп специализаций и дисциплины специализаций» включает в себя все необходимые структурные части. Учебная программа предусматривает формирование у обучающихся математического аппарата, включающего в себя математические знания, умения и навыки необходимые для дальнейшей профессиональной деятельности. Все основные разделы программы нашли свое отражение в перечне представленных в программе необходимых знаний, умений и компетенций. Распределение времени, отводимого на изучение различных разделов курса, включая самостоятельную работу, соответствует их трудоемкости.

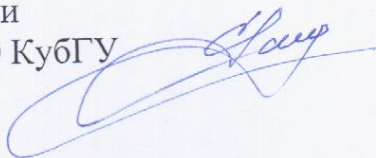
Программа отвечает современным требованиям к обучению и отражает современные тенденции в обучении и воспитании личности. Содержание рабочей программы охватывает весь материал, необходимый для обучения студентов высших учебных заведений по специальности «Фундаментальные математика и механика».

Содержание разделов, их разделение по видам занятий, и трудоемкость в часах отвечают требовательности и целесообразности. Структура и содержание курса взаимно дополняют друг друга. Также в программе приведены примеры заданий для контрольных работ, билеты для экзаменов, перечень основной и дополнительной литературы, доступной для обучающихся.

В целом, рабочая программа дисциплины «Дополнительные дисциплины для укрупненных групп специализаций и дисциплины специализаций» составлена в соответствии с требованиями ФГОС ВО и отвечает современным требованиям к качественному образовательному процессу. Данная рабочая программа может быть использована для обеспечения основной образовательной программы по специальности подготовки 01.05.01 «Фундаментальные математика и механика» по дисциплине «Дополнительные дисциплины для укрупненных групп специализаций и дисциплины специализаций».

Рецензент:

кандидат физико-математических наук, доцент, зав. кафедрой
вычислительной математики
и информатики ФГБОУ ВО КубГУ



Гайденко С.В.