«УТВЕРЖДАЮ»

И.о. декана факультета

математики и компьютерных наук

_____ А.Х. Сташ

«30» июня 2020 г.

Рабочая программа дисциплины (модуля)

Б1.В.17 Теоретико-числовые методы в криптографии

направление подготовки 01.03.02 Прикладная математика и информатика

направленность «Математическое моделирование и вычислительная математика»

РПД адаптирована для лиц с ограниченными возможностями здоровья и инвалидов

Майкоп, 2020

Факультет математики и компьютерных наук

Кафедра алгебры и геометрии

Составители (разработчики) программы: доцент кафедры алгебры и геометрии, кандидат физ.-матем. наук, доцент Х.М. Андрухаев _____,
ассистент кафедры алгебры и геометрии Т.А. Панеш _____

Рассмотрена и одобрена на заседании кафедры алгебры и геометрии от «26» июня 2020 г., протокол № 10

Заведующий кафедрой: кандидат экон. наук, доцент С.А. Бакижева _____

Согласовано:

Председатель УМК факультета: доцент кафедры прикладной математики, информационных технологий и информационной безопасности, кандидат пед. наук, доцент Ш.Т. Меретуков _____

Содержание

Пояснительная записка

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 01.03.02 Прикладная математика и информатика.

Дисциплина (модуль) «Теоретико-числовые методы в криптографии» относится к части, формируемой участниками образовательных отношений, блока дисциплин учебного плана.

Для освоения дисциплины (модуля) необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: не требуется.

Трудоемкость дисциплины: 2 з.е./ 72 ч.;

контактная работа: 34,25 ч.,

занятия лекционного типа – 16 ч.,

занятия семинарского типа (лабораторные работы) – 16 ч.,

контроль самостоятельной работы – 2 ч.,

иная контактная работа – 0,25 ч.,

контролируемая письменная работа – 0 ч.,

СР – 37,75 ч.,

контроль – 0 ч.

Ключевые слова: сравнение, сложность вычислений, теория чисел, криптография, криптосистема с открытым и скрытым ключами, криптосистема RSA, криптосистема Эль-Гамаля, криптосистема на основе проблемы «рюкзака», криптосистема на основе эллиптических кривых.

1. Цели и задачи дисциплины (модуля).

Целью дисциплины является формирование следующих компетенций.

Общепрофессиональной компетенции (ОПК):

Способен решать задачи профессиональной деятельности с использованием существующих информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-4).

Профессиональные компетенции (ПК):

Способен демонстрировать базовые знания математических и естественных наук, программирования и информационных технологий (ПК-1).

Задачами дисциплины являются формирование следующих знаний, умений и навыков:

Знания: основные понятия в криптографии (информация, кодирование, помеха устойчивости, шифрование, дешифрование), понятия сложность вычислений, однонаправленные функции, сравнения, классы вычетов, полные и приведенные системы вычетов, криптосистему RSA, криптосистему Эль-Гамаля, криптосистему на основе проблема «рюкзака», криптосистему на основе эллиптических кривых.

Умения: проводить оценки сложность вычислений, определять однонаправленные функции, доказывать основные утверждения модульной арифметики, шифровать криптосистемами RSA, Эль-Гамаля, на основе проблемы «рюкзака», на основе эллиптических кривых.

Навыки: определения порядка сложности вычислений, использования теорем Эйлера и Ферма, дискретного логарифмирования, шифрования криптосистемами RSA, Эль-Гамаля, на основе проблема рюкзака, на основе эллиптических кривых.

Таблица 1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций

Компетенция (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Результаты обучения**
ОПК-4 Способен решать задачи профессиональной деятельности с использованием существующих информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	ОПК-4.1 Знает изучаемый язык программирования, сетевые технологии, применение веб-технологий.	Знает: понятия информации, кодирования, помехи устойчивости, шифрования, дешифрования.
	ОПК-4.2 Умеет вести устную и письменную коммуникации на изучаемом языке.	Знает: понятия сложность вычислений, однонаправленные функции. Умеет: проводить оценки сложность вычислений, определять однонаправленные функции. Владеет: навыками определения порядка сложности вычислений.
	ОПК-4.3 Имеет практический опыт использования методики педагогической деятельности.	Знает: сравнения, классы вычетов, полные и приведенные системы вычетов. Умеет: доказывать основные утверждения модульной арифметики. Владеет: навыками использования теорем Эйлера и Ферма, дискретного логарифмирования.
ПК-1 Способен демонстрировать базовые знания математических и естественных наук, программирования и информационных технологий	ПК-1.1 Обладает базовыми знаниями, полученными в области математических и (или) естественных наук, программирования и информационных технологий	Знает: криптосистему RSA, криптосистему Эль-Гамаля, криптосистему на основе проблема «рюкзака», криптосистему на основе эллиптических кривых.
	ПК-1.2 Умеет находить, формулировать и решать стандартные задачи в собственной научно-исследовательской деятельности в области программирования и информационных технологий	Умеет: шифровать криптосистемами RSA, Эль-Гамаля, на основе проблемы «рюкзака», на основе эллиптических кривых.

	ПК-1.3 Имеет практический опыт научно-исследовательской деятельности в области программирования и информационных технологий	Владеет: навыками шифрования криптосистемами RSA, Эль-Гамаля, на основе проблема рюкзака, на основе эллиптических кривых.

2. Объем дисциплины (модуля) по видам учебной работы.

Таблица 2. Объем дисциплины (модуля) общая трудоемкость: 2 з.е. / 72 ч.

Форма обучения: очная

Виды учебной работы	Всего часов	Распределение по семестрам в часах			
		VIII			
Общая трудоемкость дисциплины	72	72			
Контактная работа:	34,25	34,25			
занятия лекционного типа	16	16			
занятия семинарского типа (лабораторные работы)	16	16			
контроль самостоятельной работы	2	2			
иная контактная работа	0,25	0,25			
контролируемая письменная работа					
контроль					
Самостоятельная работа (СР)	37,75	37,75			
Курсовая работа (проект)	-	-			
Вид промежуточного контроля (зачет, экзамен, диф. зачет)	зачет	зачет			

3. Содержание дисциплины (модуля).

Таблица 3. Распределение часов по темам и видам учебной работы

Форма обучения: очная

Семестр 8

Номер раздела	Наименование разделов и тем дисциплины (модуля)	Объем в часах					
		Всего	Л	Лаб	С	КСР	СР и иная работа

1.	Основные понятия криптографии.	8	2	2			4
2.	Сложность вычислений. Однонаправленные функции в теории чисел.	8	2	2			4
3.	Начало модульной арифметики.	8	2	2			4
4.	Теорема Ферма и Эйлера. RSA.	10	2	2			6
5.	Дискретное логарифмирование в конечном поле.	10	2	2			6
6.	Шифрсистема Эль-Гамаля.	12	2	2		2	4
7.	Проблема «рюкзака».	8	2	2			4
8.	Шифросистема на основе теории эллиптических кривых.	10	2	2			6
Итого:		72	16	16	0	2	38

4. Самостоятельная работа обучающихся.

Цели самостоятельной работы – освоить те разделы дисциплины, которые не были затронуты в процессе аудиторных занятий, но предусмотрены рабочей программой, а также расширить границы получаемых знаний, умений и навыков (владений) в процессе дополнительного изучения отдельных тем, решении практических задач, исследования отдельных вопросов дисциплины с помощью учебно-методической литературы; подготовиться к занятиям семинарского типа.

Виды самостоятельной работы:

- выполнение домашних заданий;
- изучение отдельных тем, вопросов, их конспектирование;
- подготовка докладов по отдельным вопросам тем;
- подготовка презентаций по отдельным вопросам тем;
- выполнение домашних контрольных заданий;
- подготовка к занятиям семинарского типа;
- подготовка к написанию математических диктантов;
- подготовка к написанию стандартных задач;
- подготовка к написанию контрольной работе.

Таблица 4. Содержание самостоятельной работы обучающихся

№, п/п	Вид самостоятельной работы	Разделы рабочей программы	Форма отчетности

1	Внеаудиторная: - изучение теоретического материала по конспектам лекций; конспектирование вопросов, оговоренных на лекции, по учебной литературе; - выполнение домашних заданий и подготовка к практическим занятиям; - подготовка к написаниям математических диктантов, стандартных задач, контрольных работ.	1-8 1-8 1-8	конспект, реферат; письменная работа; письменная работа.

4.1. Типы семестровых заданий:

1. Подготовка отдельных докладов по темам занятий.
2. Поиск учебных видеофильмов, роликов для дальнейшей демонстрации на занятии.
3. Подготовка мультимедийной презентации.

5. Учебно-методическое обеспечение дисциплины (модуля).

Таблица 5.1. Основная литература

№	Наименование, библиографическое описание
1.	Бухштаб, А. А. Теория чисел: учебное пособие / А. А. Бухштаб. — 5-е изд., стер. — Санкт-Петербург: Лань, 2020. — 384 с. — ISBN 978-5-8114-5836-3. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/147139.— Режим доступа: для авториз. пользователей.
2.	Введение в теоретико-числовые методы криптографии: учебное пособие / М. М. Глухов, И. А. Круглов, А. Б. Пичкур, А. В. Черемушкин. — Санкт-Петербург: Лань, 2021. — 400 с. — ISBN 978-5-8114-1116-0. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/167921. — Режим доступа: для авториз. пользователей.
3.	Виноградов, И. М. Основы теории чисел: учебное пособие / И. М. Виноградов. — 14-е изд., стер. — Санкт-Петербург: Лань, 2020. — 176 с. — ISBN 978-5-8114-5329-0. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/13928. — Режим доступа: для авториз. пользователей.
4.	Михелович, Ш.Х. Теория чисел: учебное пособие / Ш.Х. Михелович; отв. ред. И.Б. Погребысский; Академия наук СССР, Институт истории естествознания и техники. – Москва: Высшая школа, 1962. – 260 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=437366. – ISBN 978-5-4475-7997-5. – Текст : электронный.
5.	Котов, Ю.А. Криптографические методы защиты информации: стандартные шифры. Шифры с открытым ключом: [16+] / Ю.А. Котов; Новосибирский государственный технический университет. – Новосибирск: Новосибирский

	государственный технический университет, 2017. – 67 с.: ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=574782. – Библиогр. с 46. – ISBN 978-5-7782-3411-6. – Текст : электронный.
6.	Сизый, С.В. Лекции по теории чисел: учебное пособие / С.В. Сизый. – 2-е изд., испр. – Москва: Физматлит, 2008. – 191 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=68386. – ISBN 978-5-9221-0741-9. – Текст : электронный.

Таблица 5.2. Дополнительная литература

№	Наименование, библиографическое описание
1.	Василенко, О.Н. Теоретико-числовые алгоритмы в криптографии (2-е издание, дополненное) / О.Н. Василенко. – 2-е изд., доп. – Москва: МЦНМО, 2006. – 336 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=61814. – ISBN 5-94057-103-4. – Текст : электронный.
2.	Мартынов, Л. М. Алгебра и теория чисел для криптографии: учебное пособие / Л. М. Мартынов. — Санкт-Петербург: Лань, 2020. — 456 с. — ISBN 978-5-8114-4424-3. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/140740. — Режим доступа: для авториз. пользователей.
3.	Минеев, М.П. Лекции по арифметическим вопросам криптографии. – М.: Изд-во «Попечительский совет Механико-математического факультета МГУ им. М.В.Ломоносова», 2010. – 186 с.
4.	Черемушкин, А.В. Лекции по арифметическим алгоритмам в криптографии. – М.: МЦНМО, 2002. – 104 с.

Таблица 5.3. Ресурсы информационно-телекоммуникационной сети «Интернет»

№ п/п	Название (адрес) ресурса
1.	Информационная система «Единое окно доступа к образовательным ресурсам» http://window.edu.ru/
2.	Базы данных ИНИОН РАН http://inion.ru/resources/bazy-dannykh-inion-ran/
3.	Университетская информационная система Россия uisrussia.msu.ru

Таблица 5.4. Периодические издания

№ п/п	Наименование
1.	Журнал «Математические вопросы в криптографии» http://www.mathnet.ru/mvk издается академией криптографии Российской Федерации математического института им. В. А. Стеклова Российской академии наук в виде четырех выпуска в год.
2.	Журнал «Математический сборник» http://www.mathnet.ru/msb основан в 1866 году, издается Математическим институтом им. В. А. Стеклова Российской академии наук.

3.	Журнал «Вестник Московского университета. Серия 1. Математика. Механика» http://vestnik.math.msu.su/ был основан в 1946 году, издается Московским государственным университетом им. М.В. Ломоносова.
4.	Журнал «Исследование по алгебре, теории чисел, функциональному анализу и смежным вопросам» https://www.sgu.ru/research/nauchnye-izdaniya-sgu/prodolzhayushchiesya-izdaniya/issledovanie-po-algebre-teorii-chisel-funkcionalnomu был основан 2003 году, издается Саратовским национальным исследовательским государственным университетом имени Н.Г.Чернышевского.

Таблица 5.5. Современные профессиональные базы данных и информационные справочные системы

№ п/п	Наименование
1.	Общероссийский математический портал http://www.mathnet.ru/
2.	ООО «Научная электронная библиотека» (НЭБ) www.elibrary.ru
3.	Проект Евклид https://www.projecteuclid.org/
4.	ФГБУ «Российская государственная библиотека» http://dvs.rsl.ru
5.	ЭБС «Лань» www.e.lanbook.com
6.	ЭБС «Университетская библиотека онлайн» www.biblioclub.ru
7.	ЭБС «Юрайт» www.biblio-online.ru
8.	ЭБС АГУ на платформе аппаратно-программного комплекса ООО КДУ http://adygnet.bibliotech.ru
9.	Science Direct https://www.sciencedirect.com/

6. Образовательные технологии

Таблица 6. Образовательные технологии

№ п/п	**Наименование раздела**	**Виды учебных занятий**	**Образовательные технологии**
1	**2**	**3**	**4**
1.	Основные понятия криптографии.	Лекционные занятие 1. Лабораторная работа 1.	Развернутая беседа с обсуждением доклада. Консультирование и проверка домашних. Математический диктант.
2.	Сложность вычислений. Однонаправленные функции в теории чисел.	Лекционные занятие 2. Лабораторная работа 2.	Развернутая беседа с обсуждением доклада. Консультирование и проверка домашних. Математический диктант. Стандартные задачи.
3.	Начало модульной арифметики.	Лекционные занятие 3. Лабораторная работа 3.	Развернутая беседа с обсуждением доклада. Консультирование и проверка домашних.

			Математический диктант. Стандартные задачи.
4.	Теорема Ферма и Эйлера. RSA.	Лекционные занятие 4. Лабораторная работа 4.	Развернутая беседа с обсуждением доклада. Консультирование и проверка домашних. Математический диктант. Стандартные задачи.
5.	Дискретное логарифмирование в конечном поле.	Лекционные занятие 5. Лабораторная работа 5.	Развернутая беседа с обсуждением доклада. Консультирование и проверка домашних. Математический диктант. Стандартные задачи.
6.	Шифрсистема Эль-Гамаля.	Лекционные занятие 6. Лабораторная работа 6.	Развернутая беседа с обсуждением доклада. Консультирование и проверка домашних. Математический диктант. Стандартные задачи.
7.	Проблема «рюкзака».	Лекционные занятие 7. Лабораторная работа 7.	Развернутая беседа с обсуждением доклада. Консультирование и проверка домашних. Математический диктант. Стандартные задачи.
8.	Шифросистема на основе теории эллиптических кривых.	Лекционные занятие 8. Лабораторная работа 8.	Развернутая беседа с обсуждением доклада. Консультирование и проверка домашних. Математический диктант. Стандартные задачи.

7. Методические рекомендации по дисциплине (модулю).

Методические рекомендации преподавателю

Изучив содержание учебной дисциплины, целесообразно разработать матрицу наиболее предпочтительных методов обучения и форм самостоятельной работы студентов, адекватных видам семинарских занятий.

Необходимо предусмотреть развитие форм самостоятельной работы, выводя студентов к завершению изучения учебной дисциплины на её высший уровень. По учебному плану предусмотрено проведение разного типа занятий.

Вузовское занятие – главное звено дидактического цикла обучения. Его цель – формирование у студентов ориентировочной основы для последующего усвоения

материала методом самостоятельной работы. Содержание занятий должно отвечать следующим дидактическим требованиям:

- изложение материала от простого к сложному;
- логичность, четкость и ясность в изложении материала;
- возможность проблемного изложения, дискуссии, диалога с целью активизации деятельности студентов;
- опора смысловой части занятий на подлинные факты, события, явления, статистические данные;
- тесная связь теоретических положений и выводов с практикой и будущей профессиональной деятельностью студентов.

Преподаватель, читающий курсы в вузе, должен знать существующие в педагогической науке и используемые на практике варианты занятий, их дидактические и воспитывающие возможности, а также их методическое место в структуре процесса обучения.

В начале каждого практического занятия преподаватель организует повторение изученного по контрольным вопросам к данному практическому занятию, вспоминает со студентами понятийный аппарат. При возникновении затруднений у студентов при решении задач преподаватель подробно разбирает каждый шаг решения с обязательным вовлечением студентов группы в процесс обсуждения алгоритма решения задачи.

В условиях преобладающего теоретического обучения обязательным условием для формирования умений и навыков является усвоение теоретического материала, поэтому вопросы контроля должны проверять тот теоретический материал, содержание которого представлено в конспекте занятий и указанной литературе.

По уровню сложности предусматриваются самые различные вопросы, предполагающие воспроизведение и закрепление теоретического материала, проверку его осмысления, вопросы на обобщение, анализ и синтез и др. Обязательно предусматриваются контрольные вопросы на проверку усвоения определений ключевых понятий, знание фактов, теорий, концепций, то есть всего того, что определяет основное содержание темы.

Вопросы и задания для контроля должны позволить студентам самостоятельно определить уровень усвоения учебного материала по теме на практическом занятии.

Семинар проводится по узловым и наиболее сложным вопросам (темам, разделам) учебной программы. Он может быть построен как на материале одной лекции, так и на содержании обзорной лекции, а также по определённой теме без чтения предварительной лекции. Главная и определяющая особенность любого семинара – наличие элементов дискуссии, проблемности, диалога между преподавателем и студентами и самими студентами.

При подготовке классического семинара желательно придерживаться следующего алгоритма:

а) разработка учебно-методического материала:

- формулировка темы, соответствующей программе;
- определение дидактических, воспитывающих и формирующих целей занятия;
- выбор методов, приемов и средств обучения для проведения семинара;
- подбор литературы для преподавателя и студентов;

- при необходимости проведение консультаций для студентов;

б) подготовка студентов и преподавателя:

- составление плана семинара из 3-4 вопросов;
- предоставление студентам 4-5 дней для подготовки к семинару;
- предоставление рекомендаций о последовательности изучения литературы (учебники, учебные пособия, законы и постановления, руководства и положения, конспекты лекций, статьи, справочники, информационные сборники и бюллетени, статистические данные и др.);
- создание набора наглядных пособий.

Подводя итоги семинара, можно использовать следующие критерии (показатели) оценки ответов:

- полнота и конкретность ответа;
- последовательность и логика изложения;
- связь теоретических положений с практикой;
- обоснованность и доказательность излагаемых положений;
- наличие качественных и количественных показателей;
- наличие иллюстраций к ответам в виде исторических фактов, примеров и пр.;
- уровень культуры речи;
- использование наглядных пособий и т.п.

В конце семинара рекомендуется дать оценку всего семинарского занятия, обратив особое внимание на следующие аспекты:

- качество подготовки;
- степень усвоения знаний;
- активность;
- положительные стороны в работе студентов;
- ценные и конструктивные предложения;
- недостатки в работе студентов;
- задачи и пути устранения недостатков.

При проведении аттестации студентов важно всегда помнить, что систематичность, объективность, аргументированность – главные принципы, на которых основаны контроль и оценка знаний студентов. Знание критериев оценки знаний обязательно для преподавателя и студента.

Методические указания студентам по дисциплине

Профессиональная подготовка в современных вузах строится по принципу «от теории к практике», что создает базу для формирования умений и владений (навыков) на основе усвоения теоретического материала. Именно поэтому следует особое внимание уделять качеству усвоения теоретического материала.

Изучение дисциплины предусматривает практические занятия, а также самостоятельную работу. Изучение курса завершается промежуточной аттестацией. Успешное изучение курса требует посещения занятий, активной работы на практических

занятиях, выполнения всех учебных заданий, ознакомления с основной и дополнительной литературой.

Практическое занятие – форма организации обучения, которая направлена на формирование практических умений и навыков и является связующим звеном между самостоятельным теоретическим освоением студентами учебной дисциплины и применением ее положений на практике. Практическое занятие позволяет развить у студентов профессиональную культуру и профессиональную коммуникацию. Преподаватель в этом случае является координатором обсуждений предложенных практических заданий, подготовка которых является обязательной. Поэтому тема, практические задания и основные источники обсуждения предлагаются студентам заранее. Цели обсуждения и выполнения заданий направлены на формирование знаний, умений и навыков профессиональной полемики и формирование компетенций. На этапе подготовки доминирует самостоятельная работа студентов по решению проблем и заданий, а в процессе занятия идет активное обсуждение, дискуссии и выступления студентов, где они под руководством преподавателя делают обобщающие выводы и заключения.

Зная тему практического занятия, необходимо готовиться к нему заблаговременно: читать рекомендованную и дополнительную литературу, конспект лекций, методические указания к практическим занятиям, структурировать материал, составлять словарь терминов, отвечать на контрольные вопросы, решать ситуационные задачи и т.п. На практическом занятии вы можете получить консультацию преподавателя по любому учебному вопросу изучаемой темы.

Под самостоятельной работой студентов понимают учебную деятельность студентов, которая организована преподавателями, но осуществляется студентом без непосредственного участия преподавателя в учебной деятельности студента. Все виды самостоятельной работы студентов по дисциплине представлены в фонде оценочных средств. Четкая организация самостоятельной работы студентов делает ее эффективной. Это обеспечивается предоставлением студентам: учебных и учебно-методических пособий; тематических планов лекций, практических занятий, образцов контрольных работ, тестов, кейсов и др.; перечня знаний и умений, которыми они должны овладеть при изучении дисциплины; информации о процедуре сдачи зачета и экзамена и др. Ответы представляются в письменной форме (печатной, непосредственно преподавателю, или электронной).

Самостоятельная работа студента является основным средством овладения учебным материалом во время, свободное от обязательных учебных занятий. Она включает в себя выполнение различного рода заданий, которые ориентированы на более глубокое усвоение материала изучаемой дисциплины. По каждой теме учебной дисциплины студентам предлагается перечень заданий для самостоятельной работы.

К выполнению заданий для самостоятельной работы предъявляются следующие требования: задания должны исполняться самостоятельно и представляться в установленный срок, а также соответствовать установленным требованиям по оформлению. Студентам следует: руководствоваться графиком самостоятельной работы, выполнять все плановые задания, выдаваемые преподавателем для самостоятельного выполнения, и разбирать на семинарах и консультациях неясные вопросы; при подготовке

к экзамену параллельно прорабатывать соответствующие теоретические и практические разделы дисциплины, фиксируя неясные моменты для их обсуждения на консультации с преподавателем.

Самостоятельная работа студентов является обязательным компонентом образовательного процесса, так как она обеспечивает закрепление получаемых на лекционных занятиях знаний путем приобретения навыков осмысления и расширения их содержания, навыков решения актуальных проблем формирования общекультурных и профессиональных компетенций, научно-исследовательской деятельности, подготовки к семинарам, лабораторным работам, сдаче зачетов и экзаменов.

Подготовка к промежуточной аттестации ведется на основе полученного лекционного материала и рекомендованной литературы, осмысления работы на практических занятиях и самостоятельной работы.

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:

- занятия оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;

- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;

- письменные задания оформляются увеличенным шрифтом;

- зачёт проводится в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих:

- занятия оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;

- письменные задания выполняются на компьютере в письменной форме;

- зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата:

- занятия оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

- письменные задания выполняются на компьютере со специализированным программным обеспечением;

- зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:

- в печатной форме увеличенным шрифтом;
- в форме электронного документа;
- в форме аудиофайла.

- для глухих и слабослышащих:

- в печатной форме;
- в форме электронного документа.

- для обучающихся с нарушениями опорно-двигательного аппарата:

- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения.

9. Материально-техническое обеспечение дисциплины (модуля)

Лекционные занятия проводятся в аудиториях лекционного типа, предоставляемых деканатом факультета в соответствии с расписанием, оснащённых презентационной техникой (проектор, экран, компьютер/ноутбук) и соответствующим программным обеспечением (LibreOffice, Microsoft Office 2010 Russian Academic OPEN, Microsoft Office Professional Plus 2010 Russian Academic OPEN).

Лабораторные занятия проводятся в аудиториях семинарского типа, предоставляемых деканатом факультета в соответствии с расписанием, оснащённых презентационной техникой (проектор, экран, компьютер/ноутбук) и соответствующим

программным обеспечением (LibreOffice, Microsoft Office 2010 Russian Academic OPEN, Microsoft Office Professional Plus 2010 Russian Academic OPEN).

Групповые (индивидуальные) консультации проводятся в аудитории, оснащённой персональными компьютерами с установленным програмным обеспечением (Lazarus, Eclipse, NetBeans, Visual Studio, PyCharm, IntelliJ Idea).

Текущий контроль, промежуточная аттестация проводятся в аудитории, оснащённой персональными компьютерами с установленным программным обеспечением (Lazarus, Eclipse, NetBeans, Visual Studio, PyCharm, IntelliJ Idea).

Самостоятельная работа проводится в кабинете для самостоятельной работы, оснащённой компьютерной техникой с возможностью подключения к сети «Интернет», программой экранного увеличения и обеспеченный доступом в электронную информационно-образовательную среду университета.

Программное обеспечение, рекомендованное для использования в АГУ:

Операционные системы, такие как:

Ubuntu (https://ubuntu.com/download), Microsoft Windows 2000 Server CAL Russian, Microsoft Win Starter 7 Russian Academic OPEN.

Браузеры последней версии, такие как:

Google Chrome (https://www.google.com/chrome),
Mozilla Firefox(https://www.mozilla.org/ru/firefox/new/)

Визуальные среды программирования, такие как:

Lazarus (https://www.lazarus-ide.org/index.php?page=downloads),
Eclipse (https://www.eclipse.org/downloads/),
NetBeans (https://netbeans.apache.org/download/index.html),
Visual Studio (https://visualstudio.microsoft.com),
PyCharm (https://www.jetbrains.com/ru-ru/pycharm/download/),
IntelliJ Idea (https://www.jetbrains.com/ru-ru/idea/download).

Пакеты офисных приложений, такие как:

LibreOffice (https://www.libreoffice.org/download/download),
Microsoft Office 2010 Russian Academic OPEN,
Microsoft Office Professional Plus 2010 Russian Academic OPEN.

Текстовые редакторы, такие как:

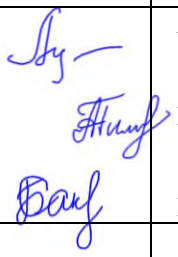
Notepad++ (https://notepad-plus-plus.org/downloads),
Latex (https://www.latex-project.org/get/).

Графический 3D пакет Blender (https://www.blender.org/download).

Растовый графический редактор GIMP (https://www.gimp.org/downloads).

Векторный графический редактор Inkscape (https://inkscape.org/release/inkscape-1.0.2).

10. Лист регистрации изменений

Номер изменения	Номера листов			Основание для внесения изменения	Подпись	Расшифровка подписи	Дата	Дата введения изменения
	заменен ных	новых	аннулиров анных					
1.	10, 16, 17			Приведени е в соответств ие ФГОС		Андрухаев ХМ Панеш ТА Бакижева СА	16.03.21	16.03.21