Приложение к ОПОП
«Математические методы в информационных технологиях»

СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

МИНОБРНАУКИ РОССИИ

федеральное государственное автономное образовательное учреждение высшего образования
**«Санкт-Петербургский государственный электротехнический университет
«ЛЭТИ» им. В.И.Ульянова (Ленина)»
(СПбГЭТУ «ЛЭТИ»)**

РАБОЧАЯ ПРОГРАММА

дисциплины

«КРИПТОГРАФИЯ И ЗАЩИТА ИНФОРМАЦИИ»

для подготовки бакалавров

по направлению

01.03.02 «Прикладная математика и информатика»

по профилю

«Математические методы в информационных технологиях»

Санкт-Петербург

2023

ЛИСТ СОГЛАСОВАНИЯ

Разработчики:

старший преподаватель Абросимов И.К.

заведующий кафедрой, д.пед.н., доцент Поздняков С.Н.

Рабочая программа рассмотрена и одобрена на заседании кафедры АМ 12.01.2023, протокол № 3

Рабочая программа рассмотрена и одобрена учебно-методической комиссией ФКТИ, 16.02.2023, протокол № 2

Согласовано в ИС ИОТ

Начальник ОМОЛА Загороднюк О.В.

1 СТРУКТУРА ДИСЦИПЛИНЫ

Обеспечивающий факультет	ФКТИ
Обеспечивающая кафедра	АМ
Общая трудоемкость (ЗЕТ)	4
Курс	4
Семестр	7
Виды занятий	
Лекции (академ. часов)	17
Лабораторные занятия (академ. часов)	17
Практические занятия (академ. часов)	17
Иная контактная работа (академ. часов)	1
Все контактные часы (академ. часов)	52
Самостоятельная работа, включая часы на контроль (академ. часов)	92
Всего (академ. часов)	144
Вид промежуточной аттестации	
Экзамен (курс)	4

2 АННОТАЦИЯ ДИСЦИПЛИНЫ

«КРИПТОГРАФИЯ И ЗАЩИТА ИНФОРМАЦИИ»

Дисциплина служит для приобретения знаний, умений и навыков в области математических методов защиты информации. В рамках дисциплины изучаются основные понятия и методы теории чисел с их приложениями в современной криптографии. Это алгоритмы операций в конечных алгебраических структурах, алгоритмы вычисления порядков элементов конечных алгебраических структур и генерации элементов заданного порядка, подходы к решению вычислительно трудных задач, используемых в качестве основы криптосистем. Также рассматриваются методы оценки сложности детерминистических и вероятностных алгоритмов, используемых в криптографии. В результате изучения данной дисциплины студенты смогут выполнять анализ производительности и стойкости криптосистем.

SUBJECT SUMMARY

«CRYPTOGRAPHY AND INFORMATION PROTECTION»

The discipline serves to acquire knowledge, skills and abilities on mathematical methods of information security. In this discipline the basic concepts and methods of number theory with their applications in modern cryptography are studied. These are algorithms of operations in finite algebraic structures, algorithms for calculating the orders of elements of finite algebraic structures and generating elements of a given order, approaches to solving computationally difficult problems used as the basis of cryptosystems. Methods for estimating the complexity of deterministic and probabilistic algorithms used in cryptography are also considered. As a result of studying this discipline, students will be able to analyze the performance and security of cryptosystems.

3 ОБЩИЕ ПОЛОЖЕНИЯ

3.1 Цели и задачи дисциплины

1. Дисциплина нацелена на изучение методов и алгоритмов теории чисел, имеющих приложение к решению криптографических задач и приобретение практических навыков их применения в профессиональной деятельности. Теоретический базис дисциплины основывается на знаниях из линейной и абстрактной алгебр, дискретной математики, математической логики и теории алгоритмов.

2. Задачи дисциплины:
-изучение основных понятий и методов теории чисел с их приложениями в современной криптографии;
-приобретение умений применения алгоритмов операций в конечных кольцах и группе точек эллиптической кривой, алгоритмов вычисления порядков и генерации элементов заданного порядка;
-освоение подходов к решению задач факторизации и дискретного логарифмирования, алгоритмов генерации простых чисел;
-рассмотрение методов оценки сложности алгоритмов, являющихся составными частями современных криптосистем или используемых для криптоанализа.
Дисциплина участвует в формировании общепрофессиональных компетенций, предусмотренные федеральным государственным образовательным стандартом высшего профессионального образования.

3. Дисциплина обеспечивает получение знаний об основных алгоритмах, используемых в составе современных криптографических систем и способах оценки производительности и стойкости таких алгоритмов.

4. Дисциплина вырабатывает умения, необходимые для работы с современными криптосистемами, в частности, выработку значений параметров, необходимых для корректной работы криптографических систем и оценку производи-

тельности криптосистем.

5. Результатом освоения дисциплины является приобретение практических навыков применения и анализа алгоритмов, основанных на теоретико-числовых принципах, используемых в современных криптосистемах.

3.2 Место дисциплины в структуре ОПОП

Дисциплина изучается на основе ранее освоенных дисциплин учебного плана:

1. «Алгебра и геометрия»

2. «Дискретная математика и теоретическая информатика»

3. «Алгебраические структуры»

4. «Комбинаторика и теория графов»

5. «Построение и анализ алгоритмов»

6. «Теория вероятностей и математическая статистика»

7. «Математическая логика и теория алгоритмов»

и обеспечивает изучение последующих дисциплин:

1. «Производственная практика (научно-исследовательская работа)»

2. «Производственная практика (преддипломная практика)»

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

В результате освоения образовательной программы обучающийся должен достичь следующие результаты обучения по дисциплине:

Код компетенции/ индикатора компетенции	**Наименование компетенции/индикатора компетенции**
ОПК-4	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности
ОПК-4.1	*Знает принципы, методы и средства решения стандартных задач профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности*
ОПК-4.2	*Умеет решать стандартные задачи профессиональной деятельности с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности*
ПК-0	Способен разрабатывать информационные модели и применять их для решения задач профессиональной деятельности
ПК-0.2	*Создает и модифицирует информационные модели для решения задач профессиональной деятельности*

4 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Содержание разделов дисциплины

4.1.1 Наименование тем и часы на все виды нагрузки

№ п/п	Наименование темы дисциплины	Лек, ач	Пр, ач	Лаб, ач	ИКР, ач	СР, ач
1	Введение	1	0	0	0	0
2	Простейшие теоретико-числовые алгоритмы и их анализ	2	3	5	0	16
3	Мультипликативная группа вычетов по модулю	3	4	0	0.25	14
4	Факторизация и дискретное логарифмирование	3	4	4	0.25	14
5	Группа точек эллиптической кривой	1	1	0	0	8
6	Двухключевые криптосистемы	2	2	0	0.25	14
7	Симметричные криптосистемы	2	1	4	0.25	14
8	Хеш-функции	2	2	4	0	12
9	Заключение	1	0	0	0	0
	Итого, ач	17	17	17	1	92
	Из них ач на контроль	0	0	0	0	35
	Общая трудоемкость освоения, ач/зе	144/4				

4.1.2 Содержание

№ п/п	Наименование темы дисциплины	Содержание
1	Введение	Основные понятия криптографии: криптография как наука, отличие от стеганографии, определения открытого текста, шифротекста, шифра и ключа, классификация шифров, понятие генератора односторонних функций с секретом.
2	Простейшие теоретико-числовые алгоритмы и их анализ	Оценка сложности алгоритмов в худшем и в среднем случаях. Число и его битовая длина как входные данные. Кольцо остатков от деления на натуральное число и алгоритмы операций в нем.
3	Мультипликативная группа вычетов по модулю	Показатели по модулю и их свойства. Алгоритмы вычисления показателя числа и нахождения числа, отвечающего заданному показателю по модулю. Первообразные корни. Квадратичные сравнения и их решение.

№ п/п	Наименование темы дисциплины	Содержание
4	Факторизация и дискретное логарифмирование	Алгоритм дискретного логарифмирования Гельфонда-Шенкса. Применение гладких чисел для решения задач факторизации и дискретного логарифмирования: алгоритм факторизации Диксона и алгоритм дискретного логарифмирования Адлемана. Применение парадокса дней рождения для решения задач факторизации и дискретного логарифмирования: модификация Флойда ро-методов Полларда для факторизации и дискретного логарифмирования. P-1 -метод факторизации Полларда. Алгоритм дискретного логарифмирования Полига-Хеллмана.
5	Группа точек эллиптической кривой	Группа точек эллиптической кривой, бесконечно удаленная точка. Геометрический и алгебраический способы сложения точек эллиптической кривой в форме Вейерштрасса. Алгоритмы сложения различных точек и удвоения точки эллиптической кривой, особые случаи сложения точек. Алгоритм вычисления произведения целого числа на точку эллиптической кривой.
6	Двухключевые криптосистемы	Криптосистемы RSA и Эль-Гамаля, выбор их параметров. Атаки на двухключевые криптосхемы. Схемы электронной подписи.
7	Симметричные криптосистемы	Блочные шифры, их структура. Режимы работы блочных шифров. Шифр AES. Атаки на блочные шифры.
8	Хеш-функции	Криптографические хеш-функции, их свойства. Поиск коллизий.
9	Заключение	Подведение итогов курса

4.2 Перечень лабораторных работ

Наименование лабораторной работы	Количество ауд. часов
1. Экспериментальное оценивание сложности вероятностного алгоритма	5
2. Исследование алгоритмов факторизации и дискретного логарифмирования	4
3. Методы криптоанализа	4
4. Исследование свойств хеш-функций	4
Итого	17

4.3 Перечень практических занятий

Наименование практических занятий	Количество ауд. часов
1. Анализ сложности алгоритмов	3
2. Алгоритмы операций в конечных кольцах	3

Наименование практических занятий	Количество ауд. часов
3. Алгоритмы вычисления порядка и нахождения элементов заданного порядка	2
4. Алгоритмы факторизации и дискретного логарифмирования	4
5. Особенности работы с криптосистемами	5
Итого	17

4.4 Курсовое проектирование

Курсовая работа (проект) не предусмотрены.

4.5 Реферат

Реферат не предусмотрен.

4.6 Индивидуальное домашнее задание

Целью выполнения ИДЗ является освоение базовых теоретико-числовых алгоритмов, применяемые в криптографии.

В качестве индивидуального домашнего задания (ИДЗ) студентам предлагаются варианты задач на теоретико-числовые алгоритмы, применяемые в криптографии.

Пример варианта ИДЗ:

1. Найти показатель числа 5 по модулю 184;
2. Найти наименьшее число a, соответствующая степень которого относится к показателю 6 по модулю 31;
3. Найти алгоритмом Тоннели-Шенкса наименьшее натуральное число, квадрат которого сравним с 3 по модулю 23;
4. Факторизовать алгоритмом Диксона число $m = 4819$, если известно, что 139 и 233 являются 5 - гладкими числами по модулю m.
5. Утроить точку (12, 4) эллиптической кривой $y^2 = x^3 + 11x + 2 \pmod{13}$.

Отчетом по выполнению ИДЗ является документ, не содержащий рукописных записей (т.е. оформленный с использованием только компьютера) и выклады-

ваемый в соответствующий раздел курса дисциплины ”Криптография и защита информации” в системе дистанционного обучения (Moodle).

Отчет по ИДЗ должен содержать:

1. Титульный лист, оформленный в соответствии с требованиями СПбГЭТУ;
2. Вариант задач, выданный студенту в качестве ИДЗ
3. Таблицу с ответами на каждую из решенных студентом задач;
4. Полное решение каждой из решенных студентом задач варианта - формулировка задачи, формализация (при необходимости), полное решение, оформленное в соответствии с требованиями СПбГЭТУ.

4.7 Доклад

Доклад не предусмотрен.

4.8 Кейс

Кейс не предусмотрен.

4.9 Организация и учебно-методическое обеспечение самостоятельной работы

Изучение дисциплины сопровождается самостоятельной работой студентов с рекомендованными преподавателем литературными источниками и информационными ресурсами сети Интернет.

Планирование времени для изучения дисциплины осуществляется на весь период обучения, предусматривая при этом регулярное повторение пройденного материала. Обучающимся, в рамках вне аудиторной самостоятельной работы, необходимо регулярно дополнять сведениями из литературных источников материал, законспектированный на лекциях. При этом на основе изучения рекомендованной литературы целесообразно составить конспект основных положений, терминов и определений, необходимых для освоения разделов учебной

дисциплины.

Особое место уделяется консультированию, как одной из форм обучения и контроля самостоятельной работы. Консультирование предполагает особым образом организованное взаимодействие между преподавателем и студентами, при этом предполагается, что консультант либо знает готовое решение, которое он может предписать консультируемому, либо он владеет способами деятельности, которые указывают путь решения проблемы.

Самостоятельное изучение студентами теоретических основ дисциплины обеспечено необходимыми учебно-методическими материалами (учебники, учебные пособия, конспект лекций и т.п.), выполненными в печатном или электронном виде.

По каждой теме содержания рабочей программы могут быть предусмотрены индивидуальные домашние задания.

Изучение студентами дисциплины сопровождается проведением регулярных консультаций преподавателей, обеспечивающих практические занятия по дисциплине, за счет бюджета времени, отводимого на консультации (внеаудиторные занятия, относящиеся к разделу «Самостоятельные часы для изучения дисциплины»).

При необходимости допускается замена аудиторных занятий на занятия с применением дистанционных образовательных технологий. Изучающие дисциплину студенты получают доступ к курсу посредством использования системы дистанционного обучения. Каждую неделю будет доступна новая тема курса в виде презентации по соответствующей теме и заданиями для проверки освоенности материала, имеющие ограниченный срок выполнения (от недели до двух недель). Весь учебный курс рассчитан на один семестр (17 недель).

Текущая СРС	**Примерная трудоемкость, ач**
Работа с лекционным материалом, с учебной литературой	16

Текущая СРС	Примерная трудоемкость, ач
Опережающая самостоятельная работа (изучение нового материала до его изложения на занятиях)	8
Самостоятельное изучение разделов дисциплины	9
Выполнение домашних заданий, домашних контрольных работ	8
Подготовка к лабораторным работам, к практическим и семинарским занятиям	8
Подготовка к контрольным работам, коллоквиумам	8
Выполнение расчетно-графических работ	0
Выполнение курсового проекта или курсовой работы	0
Поиск, изучение и презентация информации по заданной проблеме, анализ научных публикаций по заданной теме	0
Работа над междисциплинарным проектом	0
Анализ данных по заданной теме, выполнение расчетов, составление схем и моделей, на основе собранных данных	0
Подготовка к зачету, дифференцированному зачету, экзамену	35
ИТОГО СРС	92

5 Учебно-методическое обеспечение дисциплины

5.1 Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

№ п/п	Название, библиографическое описание	К-во экз. в библ.
Основная литература		
1	Поздняков, Сергей Николаевич. Дискретная математика [Текст] : учеб. для вузов по направлениям подгот. ”Информатика и вычисл. техника”, ”Информационные системы”, ”Информационная безопасность” / С.Н. Поздняков, С.В. Рыбин, 2008. -448 с.	493
2	Дернова, Евгения Сергеевна. Элементы теоретических основ криптографии [Текст] : учеб. пособие / Е.С. Дернова, Н.А. Молдовян, П.А. Молдовяну, 2009. -91 с.	77
3	Казакевич, Виктория Григорьевна. Теория чисел и алгоритмы кодирования [Текст] : учеб.-метод. пособие / В. Г. Казакевич, Е. А. Толкачева, 2019. -31 с.	100
4	Бухштаб А. А. Теория чисел [Электронный ресурс] : учебное пособие для вузов / А. А. Бухштаб, 2020. -384 с.	неогр.
5	Ларин, Сергей Васильевич. Алгебра и теория чисел. Группы, кольца и поля [Электронный ресурс] : Учебное пособие для вузов / Ларин С. В., 2021. -160 с	неогр.
6	Молдовян Н. А. Криптография: от примитивов к синтезу алгоритмов [Электронный ресурс] / Н. А. Молдовян, А. А. Молдовян, М. А. Еремеев, 2004. -448 с.	неогр.
Дополнительная литература		
1	Молдовян, Александр Андреевич. Криптография [Текст] : учебное пособие / А.А.Молдовян, Н.А.Молдовян, Б.Я.Советов, 2001. -218 с.	19
2	Молдовян, Николай Андреевич. Теоретический минимум и алгоритмы цифровой подписи [Текст] : учеб. пособие по направлению ”Прикладные математика и физика” / Н.А. Молдовян, 2010. -289 с.	26
3	Молдовян Н. А. Введение в криптосистемы с открытым ключом / Н. А. Молдовян, А. А. Молдовян, 2005. -286 с. -Текст : электронный.	неогр.

5.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», используемых при освоении дисциплины

№ п/п	Электронный адрес
1	Молдовян Н.А. Введение в криптосистемы с открытым ключомhttps://ibooks.ru/reading.php?short=1&productid=356859

5.3 Адрес сайта курса

Адрес сайта курса: https://vec.etu.ru/moodle/course/view.php?id=13153

6 Критерии оценивания и оценочные материалы

6.1 Критерии оценивания

Для дисциплины «Криптография и защита информации» предусмотрены следующие формы промежуточной аттестации: экзамен.

Экзамен

Оценка	Описание
Неудовлетворительно	Выставляется студенту, продемонстрировавшему существенные пробелы в знаниях основного учебного материала, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий
Удовлетворительно	Выставляется студенту, продемонстрировавшему знание основного учебного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по профессии, справляющемуся с выполнением заданий, предусмотренных программой, обладающему необходимыми знаниями, но допустившему неточности в ответах на аттестационном испытании и при выполнении учебных заданий
Хорошо	Выставляется студенту, продемонстрировавшему полное знание учебного материала, успешно выполнившему предусмотренные программой задачи, освоившему основную рекомендованную литературу, показавшему систематический характер знаний по дисциплине и способному к их самостоятельному пополнению и обновлению в ходе дальнейшей учебы и профессиональной деятельности
Отлично	Выставляется студенту, продемонстрировавшему всестороннее систематическое знание учебного материала, умение свободно выполнять практические задания, освоившему основную литературу и ознакомившемуся с дополнительной литературой, рекомендованной рабочей программой дисциплины, усвоившему взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявившему творческие способности в понимании, изложении и использовании учебного материала

Особенности допуска

Для допуска к экзамену студенту требуется выполнить две контрольных работы на отличную от ”неудовлетворительно” оценку, успешно защитить все лабораторные работы и сдать ИДЗ на отличную от ”неудовлетворительно” оценку.

Экзамен проходит по билетам. Для первого вопроса требуется сформулировать все определения и доказать все теоремы (если они есть), прямо связанные с темой вопроса. Для второго вопроса требуется сформулировать определение вычисляемой величины, те теоремы, непосредственно на основе которых работают алгоритмы, описание алгоритмов (словесное или при помощи формул) и доказать корректность и асимптотическую сложность алгоритмов.

В ходе экзамена с каждым студентом проводится собеседование как по вопросам билета, так и, при необходимости, по темам курса в целом. В процессе экзамена студенту могут быть предложены дополнительные задачи.

6.2 Оценочные материалы для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине

Вопросы к экзамену

№ п/п	Описание
1	Основные понятия криптографии
2	Оценка сложности детерминистических алгоритмов
3	Оценка сложности вероятностных алгоритмов
4	Порядок элемента мультипликативной группы
5	Нахождение элемента заданного порядка
6	Извлечение квадратного корня по модулю
7	Ро -метод Полларда, модификация Флойда
8	Р-1 -метод Полларда
9	Алгоритм Гельфонда-Шенкса
10	Алгоритм Полига-Хеллмана
11	Применение гладких чисел для факторизации
12	Применение гладких чисел для дискретного логарифмирования
13	Группа точек эллиптической кривой
14	Алгоритмы шифрования RSA и Эль-Гамаля

15	Схемы цифровой подписи
16	Методы криптоанализа двухключевых шифров
17	Устройство блочных шифров
18	Алгоритм шифрования AES
19	Методы криптоанализа симметричных шифров
20	Криптографические хеш-функции

Форма билета

Министерство науки и высшего образования Российской Федерации

ФГАОУ ВО «Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В.И. Ульянова (Ленина)»

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

Дисциплина **Криптография и защита информации** ФКТИ

1. Порядок элемента мультипликативной группы.
2. Метод сложения-удвоения для умножения точки эллиптической кривой на число.
3. Найти наименьшее натуральное x, если квадрат x сравним с 31 по модулю 37.

УТВЕРЖДАЮ

Заведующий кафедрой С. Н. Поздняков

Образцы задач (заданий) для контрольных (проверочных) работ

Контрольная работа № 1. Базовые вычислительные алгоритмы

1. Дать определение понятия: порядок числа по модулю
2. Докажите, что сложность алгоритма быстрого возведения в степень по модулю пропорциональна кубу этого модуля
3. Вычислить порядок числа 125 по модулю 9261

4. Найти наименьшее натуральное x, если квадрат x сравним с 126 по модулю 143
5. Факторизовать алгоритмом Диксона число $m = 4331$, если известно, что 198 является 5 - гладким числом по модулю m.

Контрольная работа № 2. Особенности вычислений в криптосистемах

1. Дать определение понятия: криптографическая хеш-функция
2. Докажите, что для нахождения секретных параметров криптосистемы RSA необходимо знать значение функции Эйлера от RSA-модуля
3. На эллиптической кривой, заданной в форме Вейерштрасса, параметры которой a = 3, b = 16, p = 19 задана точка с координатами (2, 7). Утройте эту точку
4. Найти обратный к байту ’B7’, используя неприводимый многочлен процедуры SubBytes() шифра AES
5. Не используя алгоритмы факторизации, разложить на множители RSA-модуль, равный 221, если известно, что открытая экспонента равна 11, а секретная экспонента равна 35

Весь комплект контрольно-измерительных материалов для проверки сформированности компетенции (индикатора компетенции) размещен в закрытой части по адресу, указанному в п. 5.3

6.3 График текущего контроля успеваемости

Неделя	Темы занятий	Вид контроля
1	Простейшие теоретико-числовые алгоритмы и их анализ Мультипликативная группа вычетов по модулю	
2		
3		
4		Отчет по лаб. работе
5	Факторизация и дискретное логарифмирование Группа точек эллиптической кривой	
6		
7		Отчет по лаб. работе
8	Простейшие теоретико-числовые алгоритмы и их анализ Мультипликативная группа вычетов по модулю Факторизация и дискретное логарифмирование	Контрольная работа
9	Двухключевые криптосистемы Симметричные криптосистемы	
10		
11		Отчет по лаб. работе
12	Мультипликативная группа вычетов по модулю Факторизация и дискретное логарифмирование Группа точек эллиптической кривой	
13		ИДЗ / ИДРГЗ / ИДРЗ
14	Хеш-функции	
15		Отчет по лаб. работе
16	Группа точек эллиптической кривой Двухключевые криптосистемы Симметричные криптосистемы Хеш-функции	Контрольная работа

6.4 Методика текущего контроля

на лекционных занятиях

Текущий контроль включает контроль посещаемости и написание **двух контрольных работ**.

Студент считается получившим зачет по лекционным занятиям при одновременном выполнении следующих условий:

1. Посещено не менее 60% лекций;
2. Все контрольные точки написаны на оценку не ниже ”удовлетворительно”.

Контроль самостоятельности выполнения работ студентами предполагает визуальное наблюдение за ними в процессе написания контрольной работы и ин-

дивидуальное собеседование со студентом в том случае, если возникают сомнения в том, что задачи были решены этим студентом самостоятельно.

Критерии оценивания контрольных работ

Контрольные работы оцениваются следующим образом.

Задача 1 оценивается в 1 балл, задача 2 - в 3 балла, задачи 3-5 - в 2 балла каждая.

Шкала перевода в четырехбалльную шкалу оценки следующая:

0-4 балла за решение задач контрольной работы - «неудовлетворительно»,

5-6 баллов - «удовлетворительно»,

7-8 баллов - «хорошо»,

9-10 баллов - «отлично».

В случае написания контрольной на оценку «неудовлетворительно» студент имеет возможность выполнить работу над ошибками, которая состоит в полном решении задач 3, 4 и 5 контрольной работы и защите решений на собеседовании с преподавателем. Если студент не написал контрольные работы, то он может сделать это во время зачетной недели. В случае успешного выполнения работы над ошибками, студент считается получившим оценку «удовлетворительно» за исправляемую контрольную работу.

Если допуск не получен по причине недостаточной посещаемости, то для его получения на зачетной неделе проводится собеседование, по итогам которого принимается решение о допуске студента на экзамен. Собеседование включает в себя вопросы по темам пропущенных лекций (не менее двух), количество которых определяется тем, насколько полными и правильными даются на них ответы.

на практических (семинарских) занятиях

Текущий контроль включает контроль посещаемости, оценивание активности работы студента на практических занятиях и оценивание выполнения индивидуального домашнего задания (ИДЗ).

Студент считается получившим зачет по практическим занятиям при одновременном выполнении следующих условий:

1. Посещено не менее 60% практических занятий;
2. За активность работы получена, как минимум, одна оценка «отлично», либо две оценки не ниже «хорошо», либо три оценки не ниже «удовлетворительно»;
3. ИДЗ выполнено на оценку не ниже «удовлетворительно».

Активность оценивается путем учета количества и полноты решения задач у доски. Полнота решения оценивается по четырехбалльной шкале.

Если студент посетил менее 60% практических занятий, или не проявил достаточную активность на них, то для допуска студенту выдается одна или несколько задач, которые студент решает и защищает, и по итогам защиты принимается решение о допуске студента на экзамен. Количество задач определяется тем, насколько полными и правильными были их решения, но не может быть менее одной и более трех. Оценивание решений ведется по четырехбалльной шкале, аналогично задачам, решаемым на практических занятиях в семестре. Задачи даются по темам пропущенных студентом практических занятий. Для получения зачета за семестр в этом случае студент должен одну оценку «отлично», либо две оценки не ниже «хорошо».

Критерии оценивания ИДЗ

ИДЗ оцениваются следующим образом. Каждая задача оценивается в 3 балла каждая, согласно следующим критериям:

1. Верный выбора алгоритма решения и полнота решения задачи;
2. Получение верного ответа к задаче;
3. Правильность оформления решения задачи.

Таким образом, при выполнении первого критерия за задачу ставится 1 балл, за одновременное выполнение критериев 1 и 2, либо 1 и 3 - 2 балла и за выполнение всех трех критериев - 3 балла. В случае невыполнения первого критерия независимо от выполнения остальных критериев за решение задачи ставится 0 баллов.

Шкала перевода в четырехбалльную шкалу оценки следующая:

0-4 балла за решение задач контрольной работы - «неудовлетворительно»,

5-6 баллов - «удовлетворительно»,

7-8 баллов - «хорошо»,

9-10 баллов - «отлично».

В случае сдачи ИДЗ на оценку ниже «удовлетворительно», студенту потребуется выполнить работу над ошибками и защитить свой отчет по ИДЗ на собеседовании с преподавателем. В случае успешного выполнения работы над ошибками, студент считается получившим оценку «удовлетворительно» за исправляемое ИДЗ.

на лабораторных занятиях

Текущий контроль включает **выполнение и защиту четырех лабораторных работ**.

Лабораторные работы выполняются в бригадах от одного до трех студентов. Смена состава бригады допускается перед началом выполнения очередной лабораторной работы и не допускается в процессе выполнения работы.

Все студенты одной бригады считается получившими зачет по лабораторным занятиям при выполнении всех лабораторных работ и защиты отчетов по каждой из лабораторных работ на оценку «зачет». Решение об успешности защиты каждого из членов бригад принимается индивидуально относительно

каждого участника бригады.

Работы оцениваются по своевременной сдачи и полноте отчета по лабораторной работе, а также индивидуального собеседования (защиты) по выполненной лабораторной работе. Результатом оценивания каждой лабораторной работы является оценка «зачет» или «незачет».

Лабораторная работа считается сданной своевременно в случае, когда неделя, на которой сдается работа соответствует графику сдачи лабораторных работ. В случае одновременной сдачи на одном лабораторном занятии двух отчетов по лабораторным работам, один из которых сдается в срок, а второй - с опозданием, приоритет имеют те, кто сдают работу в срок.

Отчет по лабораторной работе выполняется бригадой студентов и должен содержать:

1. Цель работы;
2. Теоретические сведения, необходимые для выполнения работы;
3. Задание на лабораторную работу;
4. Решение поставленной в работе задачи;
5. Вывод;
6. Список используемой литературы.

Отчет считается полным, если в нем имеются все вышеперечисленные разделы и их содержание соответствует требованиям, выдвигаемым к данной лабораторной работе. Неполные отчеты могут быть отправлены на доработку.

На защите выполненной лабораторной работы каждый участник бригады получает вопрос по теоретической части соответствующего раздела учебного курса, или по процедуре проведения экспериментальных исследований, или по последующей обработке результатов, после чего ему предоставляется время для подготовки ответа. При обсуждении ответа преподаватель может задать несколько уточняющих вопросов. В случае если студент демонстрирует достаточное знание вопроса, работа считается защищенной.

При защите лабораторной работы каждый участник бригады должен показать: владение базовой терминологией, требуемой для выполнения работы, понимание методики исследования и знание особенностей её применения, понимание и умение объяснять особенности применяемых методов, возможные области их применения и т.д., умение давать качественную и количественную оценку полученных экспериментальных результатов и прогнозировать реакции исследуемого объекта на различные воздействия, а также навыки и умения, приобретенные при выполнении лабораторной работы.

самостоятельной работы студентов

Контроль самостоятельной работы студентов осуществляется на лекционных, лабораторных и практических занятиях студентов по методикам, описанным выше.

7 Описание информационных технологий и материально-технической базы

Тип занятий	Тип помещения	Требования к помещению	Требования к программному обеспечению
Лекция	Лекционная аудитория	Количество посадочных мест – в соответствии с контингентом, рабочее место преподавателя, меловая или маркерная доска, компьютер или ноутбук, подключенные к проектору для показа презентаций	1) Windows XP и выше; 2) Microsoft Office 2007 и выше
Лабораторные работы	Лаборатория	Количество посадочных мест – в соответствии с контингентом, компьютерный класс; , рабочее место преподавателя.	1) Windows XP и выше; 2) Microsoft Office 2007 и выше 3) Среда разработки на языке программирования C++
Практические занятия	Аудитория	Количество посадочных мест – в соответствии с контингентом, рабочее место преподавателя, меловая или маркерная доска	
Самостоятельная работа	Помещение для самостоятельной работа	Оснащено компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.	1) Windows XP и выше; 2) Microsoft Office 2007 и выше

8 Адаптация рабочей программы для лиц с ОВЗ

Адаптированная программа разрабатывается при наличии заявления со стороны обучающегося (родителей, законных представителей) и медицинских показаний (рекомендациями психолого-медико-педагогической комиссии). Для инвалидов адаптированная образовательная программа разрабатывается в соответствии с индивидуальной программой реабилитации.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Дата	Изменение	Дата и номер протокола заседания УМК	Автор	Начальник ОМОЛА