ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА (РОСАВИАЦИЯ)
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ ИМЕНИ ГЛАВНОГО МАРШАЛА АВИАЦИИ А.А. НОВИКОВА»

УТВЕРЖДАЮ

Ректор

_____ / Ю.Ю. Михальчевский

«23» марта 2023 года

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Основы криптографии

Направление подготовки
01.03.04 Прикладная математика

Направленность программы (профиль)
Математическое и программное обеспечение беспилотных авиационных систем

Квалификация выпускника
бакалавр

Форма обучения
очная

Санкт-Петербург
2023

1 Цели освоения дисциплины

Целями освоения дисциплины «Основы криптографии» являются:

- формирование комплекса теоретических знаний математических подходов к решению задач компьютерной безопасности;
- формирование навыков построения криптографических алгоритмов;
- приобретение умений и практических навыков использования математического аппарата для вывода свойств разрабатываемых методов;
- формирование умения самостоятельно повышать свои знания в области криптографии и защиты информации.

Задачами освоения дисциплины «Основы криптографии» являются:

– формирование у обучающихся знаний об основных результатах в области криптографических исследований;

– приобретение обучающимися умений анализировать методы криптографии при решении задач защиты информации;

– овладение обучающимися навыками решения основных криптографических задач.

Дисциплина обеспечивает подготовку выпускника к решению задач профессиональной деятельности научно-исследовательского типа.

2 Место дисциплины в структуре ОПОП ВО

Дисциплина «Основы криптографии» представляет собой дисциплину, относящуюся к блоку «Факультативы».

Дисциплина «Основы криптографии» базируется на результатах обучения, полученных при изучении дисциплин: «Алгоритмы и структуры данных», «Теория сложных вычислений и алгоритмов».

Дисциплина «Основы криптографии» является обеспечивающей для Производственной (научно-исследовательская работа) практики, Выполнения и защиты выпускной квалификационной работы.

Дисциплина «Основы криптографии» изучается в 7 семестре.

3 Компетенции обучающегося, формируемые в результате освоения дисциплины

Процесс освоения дисциплины «Основы криптографии» направлен на формирование следующих компетенций:

Код компетенции/ индикатора	Результат обучения: наименование компетенции, индикатора компетенции
ОПК-1	Способен применять знание фундаментальной математики и естественно-научных дисциплин при решении задач в области естественных наук и инженерной практике
$ИД^{1}_{ОПК1}$	Применяет знания фундаментальной математики при решении поставленных задач
$ИД^{2}_{ОПК1}$	Выбирает оптимальные методы фундаментальной математики при решении поставленных задач, в том числе в

Код компетенции/ индикатора	Результат обучения: наименование компетенции, индикатора компетенции
	профессиональной сфере.
ОПК-3	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности
$ИД^1_{ОПК3}$	Строит математические модели при решении научно-исследовательских задач.
$ИД^2_{ОПК3}$	Использует аналитические и научные пакеты прикладных программ для создания математических моделей.
ОПК-4	Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения
$ИД^1_{ОПК4}$	Владеет знаниями в области проектирования и разработки современных программных средств коммуникационных технологий.
$ИД^2_{ОПК4}$	Применяет имеющиеся навыки использования современных программных методов и средств коммуникационных технологий в профессиональной деятельности.

Планируемые результаты изучения дисциплины:

Знать:

- основные информационные источники, содержащие термины и понятия, относящиеся к криптографии;
- математические основы современной криптографии; показатели и проблемы стойкости криптосистем;

Уметь:

- самостоятельно анализировать модели обеспечения информационной безопасности; самостоятельно выбирать и анализировать информацию из информационных источников о языке программирования Java;
- осуществлять программную реализацию криптографических алгоритмов;

Владеть:

- навыками использования криптографических методов;
- методами оценки эффективности криптографических систем.

4 Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 академических часа.

Наименование	Всего часов	Семестр
		7
Общая трудоемкость дисциплины	72	72
Контактная работа:	28,3	28,3
лекции	14	14
практические занятия	14	14
семинары	-	-
лабораторные работы	-	-
курсовой проект (работа)	-	-
Самостоятельная работа студента	35	35
Промежуточная аттестация	9	9

контактная работа	0.3	0.3
самостоятельная работа по подготовке к зачету	8.7	8.7

5 Содержание дисциплины

5.1 Соотнесения тем (разделов) дисциплины и формируемых компетенций

Темы (разделы) дисциплины	Количество часов	Компетенции			Образовательные технологии	Оценочные средства
		ОПК-1	ОПК-3	ОПК-4		
Тема 1. Обеспечение информационной безопасности деятельности общества. Модели обеспечения информационной безопасности	18	+	+		ВК, Л, ПЗ, СРС	Д
Тема 2. Симметричные и ассиметричные криптографические системы	20	+		+	Л, ПЗ, СРС	П
Тема 3. Электронные цифровые подписи.	25	+	+		Л, ПЗ, СРС	П
Всего по дисциплине	63					
Промежуточная аттестация	9					
Итого по дисциплине	72					

Л – лекция, ПЗ – практическое занятие, СРС – самостоятельная работа студента, ВК – входной контроль, П – проект, Д – доклад.

5.2. Темы (разделы) дисциплины и виды занятий

Наименование темы (раздела) дисциплины	Л	ПЗ	С	ЛР	СРС	КР	Всего часов
Тема 1. Обеспечение информационной безопасности деятельности общества. Модели обеспечения информационной безопасности	4	4	-	-	10	-	18
Тема 2. Симметричные и ассиметричные криптографические системы	4	4	-	-	12	-	20
Тема 3. Электронные цифровые подписи	6	6	-	-	13	-	25

Наименование темы (раздела) дисциплины	Л	ПЗ	С	ЛР	СРС	КР	Всего часов
и криптографические ключи.							
Всего по дисциплине	14	14	-	-	35	-	63
Промежуточная аттестация							9
Итого по дисциплине							72

Сокращения: Л − лекция, ПЗ – практическое занятие, С – семинары,
ЛР – лабораторная работа, СРС − самостоятельная работа студента, КР – курсовая работа.

5.3 Содержание дисциплины

Тема 1. Обеспечение информационной безопасности деятельности общества. Модели обеспечения информационной безопасности

Информационная безопасность деятельности общества и ее основные положения. Организационные, физико-технические, информационные и программно-математические угрозы. Эволюция подходов к обеспечению информационной безопасности. Стратегии, модели и системы предотвращения несанкционированного доступа в информационные системы. Критерии и классы оценки защищенности объектов и деятельности.

Тема 2. Симметричные и ассиметричные криптографические системы

Основные классы симметричных криптосистем. Блочные шифры. Алгоритмы блочного шифрования. Режимы применения блочных шифров. Потоковые шифры. Ассиметричные шифры. Односторонние функции и функции ловушки. Ассиметричные системы шифрования

Тема 3. Электронные цифровые подписи и криптографические ключи

Постановка задачи. Алгоритмы электронной цифровой подписи. Функции хэширования. Обычная система управления ключами. Управление ключами, основанное на системах с открытым ключом. Протокол обмена секретным ключом. Использование сертификатов. Протоколы аутентификации. Анонимное распределение ключей.

5.4 Практические занятия

Номер темы дисциплины	Тематика практических занятий (семинаров)	Трудоемкость (часы)
1	Практическое занятие №1. Классификация видов угроз информационной безопасности. Эволюция подходов к обеспечению информационной безопасности	2
	Практическое занятие №2. Комплексное информационное обеспечение безопасности государства.	2
	Практическое занятие №3. Анализ алгоритмов DES, алгоритм Rijndael, RC6.	2

2	Практическое занятие №4. Программная реализация алгоритмов шифрования.	2
3	Практическое занятие №5. Стандарты электронной цифровой подписи. Анализ алгоритмов цифровой подписи, основанных на ассиметричных криптосистемах.	2
	Практическое занятие №6. Программная реализация алгоритма хэширования.	2
	Практическое занятие № 7-8. Управление ключами, основанное на системах с открытым ключом. Использование сертификатов.	2
Итого по дисциплине:		14

5.5 Лабораторный практикум

Лабораторный практикум учебным планом не предусмотрен.

5.6 Самостоятельная работа

Номер темы дисциплины	Виды самостоятельной работы	Трудоемкость (часы)
1	1. Поиск, анализ информации и проработка учебного материала [1, 2, 3]. 2. Подготовка к докладу.	10
2	1. Поиск, анализ информации и проработка учебного материала [1,4,5-14]. 2. Подготовка к проекту.	12
3	1. Поиск, анализ информации и проработка учебного материала [1,4,5-14]. 2. Подготовка к проекту.	13
Итого по дисциплине		35

5.7 Курсовые работы (проекты)

Курсовые работы (проекты) учебным планом не предусмотрены.

6 Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:

1. Фомичёв, В. М. **Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты** : учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников ; под ред. В. М. Фомичёва. — М. : Издательство Юрайт, 2017. — 209 с. — (Серия : Бакалавр. Академический курс). — ISBN 978-5-534-01740-3. — Режим доступа : www.biblio-online.ru/book/A01C7E90-A5B7-4B50-B348-31CB49CA5B3D .

2. Нестеров, С.А. **Основы информационной безопасности** [Электронный ресурс] : учебное пособие / С.А. Нестеров. — Электрон. дан. — Санкт-Петербург : Лань, 2018. — 324 с. — Режим доступа: https://e.lanbook.com/book/103908 . — Загл. с экрана.

3. Фомичёв, В. М. **Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты: учебник для академического бакалавриата** / В. М. Фомичёв, Д. А. Мельников; под ред. В. М. Фомичёва. — М.: Издательство Юрайт, 2018. — 245 с. — (Серия: Бакалавр. Академический курс). — ISBN 978-5-9916-7090-6. — Режим доступа : www.biblio-online.ru/book/AF99BBDE-AF3A-43A9-A90F-B99806553C25

б) дополнительная литература:

4. Васильева, И. Н. **Криптографические методы защиты информации** : учебник и практикум для академического бакалавриата / И. Н. Васильева. — М. : Издательство Юрайт, 2017. — 349 с. — (Серия : Бакалавр. Академический курс). — ISBN 978-5-534-02883-6. — Режим доступа : www.biblio-online.ru/book/38C7E67F-676F-4A9E-8E92-FD548EA095BA .

5. **Введение в теоретико-числовые методы криптографии** [Электронный ресурс] : учебное пособие / М.М. Глухов [и др.]. — Электрон. дан. — Санкт-Петербург: Лань, 2011. — 400 с. — Режим доступа: https://e.lanbook.com/book/68466 . — Загл. с экрана .

в) перечень ресурсов информационно-телекоммуникационной сети «Интернет»:

6 **. Математическая криптография** [Электронный ресурс]. – Режим доступа: http://cryptography.ru/ . – Загл. с экрана. (дата обращения: 29.09.2023).

7 **. Интернет-проект «Задачи»** [Электронный ресурс]. – Режим доступа: https://stepik.org/course/217/syllabus .– Загл. с экрана. (дата обращения: 29.09.2023).

8 **. Параллель: Базовая электронная энциклопедия по параллельным вычислениям**. [Электронный ресурс]. – Режим доступа: http://www.problems.ru/ .– Загл. с экрана. (дата обращения: 29.09.2023).

г) программное обеспечение (лицензионное), базы данных, информационно-справочные и поисковые системы:

9 **Единое окно доступа к образовательным ресурсам** [Электронный ресурс]. – Режим доступа:http://window.edu.ru, свободный (дата обращения: 29.09.2023).

10 **Электронная библиотека научных публикаций «eLIBRARY.RU»** [Электронный ресурс] — Режим доступа: http://elibrary.ru/, свободный (дата обращения: 29.09.2023).

11 **Электронно-библиотечная система издательства «Лань»** [Электронный ресурс] — Режим доступа: http://e.lanbook.com/, свободный (дата обращения: 29.09.2023).

12 **Cygwin** [Электронный ресурс] — Режим доступа: https://www.cygwin.com/ - свободный (дата обращения: 29.09.2023).

13 **Сайт библиотеки GNU MP** [Электронный ресурс] — Режим доступа: http://gmplib.org – свободный (дата обращения: 29.09.2023).

14 **Сайт библиотеки GNU Crypto** [Электронный ресурс] — Режим доступа: http://www.gnu.org/s/gnu-crypto - свободный (дата обращения: 29.09.2023).

7 Материально-техническое обеспечение дисциплины

Компьютерные классы кафедры № 8 с доступом в Интернет, переносной проектор.

Информационно-справочные и материальные ресурсы библиотеки СПбГУ ГА.

Лицензионное программное обеспечение: Microsoft Office, Cygwin.

8 Образовательные и информационные технологии

Дисциплина «Основы криптографии» предполагает использование следующих образовательных технологий: входной контроль, практические занятия и самостоятельная работа студента.

Входной контроль проводится преподавателем в начале изучения дисциплины с целью коррекции процесса усвоения студентами дидактических единиц. Он осуществляется по вопросам из дисциплин, на которых базируется дисциплина «Основы криптографии» (п. 2).

Лекция составляет основу теоретического обучения в рамках дисциплины и направлена на систематизированное изложение накопленных и актуальных научных знаний. На лекции концентрируется внимание обучающихся на наиболее сложных и узловых вопросах, стимулируется их активная познавательная деятельность.

Практическое занятие по дисциплине «Основы криптографии» содействует выработке у обучающихся умений и навыков применения знаний, полученных в ходе самостоятельной работы. Практические занятия как образовательная технология помогает студентам систематизировать, закрепить и углубить знания.

Самостоятельная работа студента проявляется в систематизации, планировании, контроле и регулировании его учебно-профессиональной деятельности, а также собственные познавательно-мыслительные действия без непосредственной помощь и руководства со стороны преподавателя. Основной целью самостоятельной работы студента является формирование навыка самостоятельного приобретения им знаний по некоторым несложным вопросам теоретического курса, закрепление и углубление полученных знаний, умений и навыков во время практических занятий. Самостоятельная работа подразумевает выполнение студентом поиска, анализа информации, проработку на этой основе учебного материала, подготовку к докладу, а также подготовку проекта.

В рамках изучения дисциплины «Основы криптографии» предполагается использовать в качестве информационных технологий среду MS Office, Cygwin.

9 Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины

Фонд оценочных средств дисциплины «Основы криптографии» представляет собой комплекс методических и контрольных измерительных материалов, предназначенных для определения качества результатов обучения и уровня сформированности компетенций обучающихся в ходе освоения данной дисциплины. В свою очередь, задачами использования фонда оценочных средств являются осуществление как текущего контроля успеваемости студентов, так и промежуточной аттестации в форме зачета.

Фонд оценочных средств дисциплины «Основы криптографии» для текущего контроля включает: проект и доклад.

Доклад представляет собой публичное выступление по представлению

полученных результатов анализа определенной учебно-исследовательской темы.

Типовые темы докладов представлены в п. 9.4.

Проект предназначен для проверки умений и навыков самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве. Проект является конечным программным продуктом.

Промежуточная аттестация по итогам освоения дисциплины проводится в виде зачета в 7 семестре. Этот вид промежуточной аттестации позволяет оценить уровень освоения студентом компетенций за весь период изучения дисциплины. Зачет предполагает устные ответы на 2 теоретических вопроса из перечня вопросов, вынесенных на промежуточную аттестацию, а также решение задачи.

9.1 Балльно-рейтинговая оценка текущего контроля успеваемости и знаний студентов по дисциплине

Не применяется.

9.2 Методические рекомендации по проведению процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Доклад:

«зачтено»: грамотное и непротиворечивое изложение сути вопроса при использовании современных источников. Обучающийся способен сделать обоснованные выводы, а также уверенно отвечать на заданные в ходе обсуждения вопросы;

«не зачтено»: неудовлетворительное качество изложения материала и неспособность обучающегося сделать обоснованные выводы или рекомендации.

Проект:

«зачтено»: работа зачитывается в том случае, если задание выполнено полностью, в соответствии с поставленными требованиями и сделаны необходимые выводы;

«не зачтено»: работа не зачитывается в том случае, если обучающийся не выполнил задания, или результат выполнения задания не соответствует поставленным требованиям.

По итогам освоения дисциплины «Основы криптографии» проводится аттестация обучающихся в форме зачета и предполагает решение задач на компьютере по билетам на практические вопросы из перечня.

Зачет является заключительным этапом изучения дисциплины «Основы криптографии» и имеет целью проверить и оценить учебную работу студентов, уровень полученных ими знаний, умение применять их к решению практических задач, овладение практическими навыками в объеме требований образовательной программы на промежуточном этапе формирования компетенции ПК-2.

Во время подготовки к зачету студенты могут пользоваться материальным обеспечением, перечень которого утверждается заведующим кафедры.

На подготовку к ответу студенту предоставляется до 60 минут. По готовности к ответу или по вызову экзаменатора студент предъявляет решенные на зачете задачи. После ответа студента экзаменатор имеет право задать ему дополнительные

вопросы в объеме учебной программы.

В итоге проведенного зачета студенту выставляется зачет/незачет. Экзаменатор несет личную ответственность за правильность выставленного зачета и оформления зачетной ведомости и зачетной книжки.

9.3 Темы курсовых работ (проектов) по дисциплине

Написание курсовых работ (проектов) учебным планом не предусмотрено.

9.4 Контрольные задания для проведения входного контроля остаточных знаний по обеспечивающим дисциплинам

1. Формальное определение алгоритма.
2. Пример вычислительной проблемы.
3. Формальное описание алгоритма. Отличия от кода языка высокого уровня.
4. Роль асимптотической нотации в определении производительности алгоритмов и структур данных.
5. Амортизационный анализ – назначение и примеры использования.

9.5 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Компетенции	Показатели оценивания (индикаторы достижения) компетенций	Критерии оценивания
I этап		
ОПК-1 ОПК-3 ОПК-4	$ИД^1_{ОПК1}$ $ИД^1_{ОПК3}$ $ИД^1_{ОПК4}$	Знает: самостоятельно находит информационные источники, относящиеся к криптографическому анализу; - называет основные классы криптосистем, простейшие шифры и их свойства; Умеет:

		- воспроизводить модели обеспечения информационной безопасности - составляет криптографические алгоритмы с использованием псевдокода и (или) блок-схем; Владеет: - перечисляет основные криптографические задачи и методы их решения; - перечисляет типы основных способов криптоанализа шифров, способы построения хеш-функций и основные требования к ним, основные типы электронной подписи и криптографических протоколов;
II этап		
ОПК-1 ОПК-3 ОПК-4	$ИД^{2}_{ОПК1}$ $ИД^{2}_{ОПК3}$ $ИД^{2}_{ОПК4}$	Знает: -выделяет из имеющейся избыточной информации необходимую для решения поставленной задачи; - строит математические модели шифров, классифицирует показатели стойкости криптосистем; Умеет: - анализирует стратегии обеспечения информационной безопасости, оценивает защищенность процессов переработки информации; - определяет криптографический алгоритм и составляет его с использованием заданного языка программирования; Владеет: - объясняет и применяет методы решения основных криптографических задач; - анализирует эффективность хеш-функций, классифицирует основные типы электронной подписи, оценивает их эффективность.

Ответ студента на зачете оценивается одной из следующих оценок: *«зачтено»* и *«незачтено»*, которые выставляются по следующим критериям.

Оценки *«зачтено»* заслуживает студент, обнаруживший всестороннее, систематическое и глубокое знание учебного и нормативного материала, умеющий свободно выполнять задания, предусмотренные программой, усвоивший основную литературу, а также знакомый с дополнительной литературой, рекомендованной преподавателем. Также оценка *«зачтено»* выставляется студентам, обнаружившим полное знание учебного материала, успешно выполняющим предусмотренные в программе задания, демонстрирующим систематический характер знаний по дисциплине и способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности.

Наконец, оценкой *«зачтено»* оцениваются ответы студентов, показавших знание основного учебного материала в объеме, необходимом для дальнейшей учебы и в предстоящей работе по профессии, справляющихся с выполнением заданий, предусмотренных программой, но допустившим погрешности в ответе на экзамене и при выполнении контрольных заданий, не носящие принципиального характера, когда установлено, что студент обладает необходимыми знаниями для последующего устранения указанных погрешностей под руководством преподавателя.

Оценка *«незачтено»* выставляется студентам, обнаружившим пробелы в знаниях основного учебного материала, допускающим принципиальные ошибки в выполнении предусмотренных программой заданий. Такой оценки заслуживают ответы студентов, носящие несистематизированный, отрывочный, поверхностный характер, когда студент не понимает существа излагаемых им вопросов, что свидетельствует о том, что студент не может дальше продолжать обучение или приступать к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине.

9.6 Типовые контрольные задания для проведения текущего контроля и промежуточной аттестации по итогам освоения дисциплины

Типовое задание для проекта.

Выполнить программную реализацию современного алгоритма блочного шифрования DES, используя язык программирования C++.

Типовые темы докладов:

1. Основные составляющие национальных интересов Российской Федерации в информационной сфере.
2. Информация, основные свойства и характеристики безопасности ее применения.
3. Комплексное обеспечение информационной безопасности государства.
4. Области и объекты по обеспечению информационной безопасности и защите информационной деятельности.

5. Технологии обеспечения безопасности обработки информации.
6. Обеспечение информационной безопасности в нормальных и чрезвычайных ситуациях.

Перечень типовых вопросов к зачету для проведения промежуточной аттестации по дисциплине

1. Определение информационной безопасности.
2. Что такое доступность информации?
3. Какие возможные степени секретности Вы знаете?
4. Перечислите основные типы угроз информационной безопасности. Приведите примеры к каждому типу.
5. Какие основные эволюционные подходы к обеспечению информационной безопасности деятельности общества Вы знаете?
6. Сформулируйте основные проблемы информационной безопасности.
7. Каковы основные группы моделей безопасности?
8. Какие модели разграничения доступа Вы знаете?
9. Какие существуют критерии оценки защищенности объектов?
10. Алгоритм блочного шифрования DES и его модификации.
11. Алгоритм блочного шифрования AES. Алгоритм Rijndael.
12. Алгоритм блочного шифрования RC6.
13. Алгоритм блочного шифрования Safer.
14. Потоковое шифрование. Метод RC4.
15. Потоковое шифрование. Метод SEAL.
16. Потоковое шифрование. Метод WAKE.
17. Ассиметричная криптосистема шифрования Эль-Гамаля.
18. Криптосистема, основанная на проблеме Диффи-Хеллмана.
19. Алгоритмы цифровой электронной подписи.
20. Стандарты цифровой электронной подписи.
21. Функции хэширования. Достоинства и недостатки различных видов хэширования.

Типовая задача для промежуточной аттестации:

Описать (привести блок-схему или псевдокод) алгоритм симметричного шифрования. Режим выполнения алгоритма – простая замена.

10 Методические рекомендации для обучающихся по освоению дисциплины

Методика преподавания дисциплины «Основы криптографии» характеризуется совокупностью методов, приемов и средств обучения, обеспечивающих реализацию содержания и учебно-воспитательных целей дисциплины, которая может быть представлена как некоторая методическая система, включающая методы, приемы и средства обучения. Такой подход позволяет более качественно подойти к вопросу освоения дисциплины обучающимися.

Основными видами учебных занятий по дисциплине являются практические занятия. Объем и виды учебных занятий определены представленной рабочей программой дисциплины.

Практические занятия по дисциплине имеют целью:
- углубление, расширение и конкретизацию знаний, до уровня, на котором возможно их практическое использование;
- отработку навыков и умений в пользовании соответствующем математическим аппаратом.

Основу практических занятий составляет работа каждого обучаемого индивидуальная и (или) коллективная, по приобретению умений и навыков использования закономерностей, принципов, методов, форм и средств, составляющих содержание дисциплины в профессиональной деятельности и в подготовке к изучению дисциплин, формирующих компетенции выпускника.

По результатам контроля знаний и умений преподаватель должен провести анализ хода и итогов практических занятий, отметить успехи студентов в решении учебной задачи, а также недостатки и ошибки, разобрать их причины и дать методические указания к их устранению. Таким образом, практические занятия являются важной формой обучения, в ходе которых знания студентов превращаются в профессиональные необходимые умения, навыки.

Зачет являются заключительными оценочным средством, по итогам которого выявляется общий уровень овладения обучающимися предусмотренных компетенций по тематическим вопросам всего курса.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 01.03.04 «Прикладная математика».

Программа рассмотрена и утверждена на заседании кафедры №8 Прикладной математики и информатики

«18» сентября 2023 года, протокол № 2.

Разработчик:

к.т.н. Земсков Ю.В.

(*ученая степень, ученое звание, фамилия и инициалы разработчика*)

И.о.заведующего кафедрой № 8 Прикладной математики и информатики

к.т.н. Земсков Ю.В.

(*ученая степень, ученое звание, фамилия и инициалы заведующего кафедрой*)

Программа согласована:

Руководитель ОПОП

д.т.н., доцент Костин Г.А.

(*ученая степень, ученое звание, фамилия и инициалы руководителя ОПОП*)

Программа рассмотрена и согласована на заседании Учебно-методического совета Университета «22» 11 2023 года, протокол № 3.