МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «СЕВЕРО-КАВКАЗСКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ»

«УТВЕРЖДАЮ»
Проректор по учебной работе _____ Г.Ю. Нагорная
«16» 01 2026 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Математические основы защиты информации

Уровень образовательной программы бакалавриат

Направление подготовки 01.03.02 Прикладная математика и информатика

Направленность(профиль) «Математические и информационные системы и технологии в астрономии»

Форма обучения: очная

Срок освоения ОП 4 года

Институт Цифровых технологий

Кафедра разработчик РПД Математика

Выпускающая кафедра Астрофизика

Начальник
учебно-методического управления _____ Семенова Л. У.

Директор института ЦТ _____ Кумратова А. М.

И. О. заведующего выпускающей кафедрой _____ Валявин Г. Г.

г. Черкесск, 2026 г

СОДЕРЖАНИЕ

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «**Математические основы защиты информации»** является ознакомление обучающихся с математическим основам информации, организационными, техническими, алгоритмическими и другими методами и средствами защиты компьютерной информации, с законодательством и стандартами в этой области, с современными криптосистемами.

Задачи дисциплины:

- освоение обучающимися основных положений теории информационной безопасности в компьютерных системах;
- освоение обучающимися математической основы защиты информации;
- освоение основных принципов и методов, применяемых при защите информации.
- изучение правовых основ защиты информации в компьютерной системе;
- изучение организационно-технических, программно-аппаратных методов и средств защиты информации;
- изучение стандартов, моделей и методов шифрования информации, методы идентификации пользователей, методы защиты программ от вирусов;
- изучение криптографических методов защиты информации в компьютерных системах
- оценивать защищенность компьютерных систем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

2.1. Дисциплина «Математические основы защиты информации» относится к обязательной части Блока 1. Дисциплины (модули), имеет тесную связь с другими дисциплинами.

2.2. Ниже приведены предшествующие и последующие дисциплины, направленные на формирование компетенций дисциплины в соответствии с матрицей компетенций ОП.

Предшествующие и последующие дисциплины, направленные на формирование компетенций

№ п/п	Предшествующие дисциплины	Последующие дисциплины
1	Теория вероятностей и математическая статистика	Учебная практика (Технологическая (проектно-технологическая) практика)
2	Исследование операций и теория игр	
3	Численные методы	

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты освоения образовательной программы (ОП) – компетенции обучающихся определяются требованиями стандарта по направлению подготовки 01.03.02 Прикладная математика и информатика и формируются в соответствии с матрицей компетенций ОП

№ п/п	Номер/ индекс компетенции	Наименование компетенции (или ее части)	В результате изучения дисциплины обучающиеся должны:
1	2	3	4
1.	ОПК-5	Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения	ОПК-5.1 Обладает базовыми знаниями в области алгоритмизации и программирования ОПК-5.2 Использует структурные особенности языков программирования и пакетов прикладных программ при реализации алгоритмов для решения прикладных задач ОПК-5.3 Разрабатывает компьютерные программы, пригодные для практического использования

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Объем дисциплины и виды работы

Вид учебной работы		Всего часов	Семестр 6 (часы)
1		2	
Аудиторная контактная работа (всего)		**54**	**54**
В том числе:			
Лекции (Л)		**18**	**18**
Практические занятия (ПЗ)		**36**	**36**
Лабораторные работы (ЛР)		-	-
Контактная внеаудиторная работа, в том числе		**1,5**	**1,5**
Индивидуальные и групповые консультации		1,5	1,5
Самостоятельная работа обучающегося (СРО) (всего)		**52**	**52**
Подготовка к практическим работам (ПР)		12	12
Работа с книжными и электронными источниками		20	20
Подготовка к промежуточному тестовому контролю		20	20
Промежуточная аттестация	Зачет с оценкой, в том числе	ЗаО	ЗаО
	Прием зачета с оценкой, час	**0,5**	**0,5**
	СРО, час.	-	-
ИТОГО: Общая трудоемкость	**часов**	**108**	**108**
	зач. ед.	**3**	**3**

4.2. Содержание дисциплины

4.2.1. Разделы (темы) дисциплины, виды учебной деятельности и формы контроля

№ п/п	Наименование раздела (темы) дисциплины	Виды учебной деятельности, включая самостоятельную работу обучающихся (в часах)					Формы текущей и промежуточной аттестации
		Л	ЛР	ПЗ	СРО	всего	
1	2	3	4	5	6	7	8
Семестр 6							
1.	Раздел 1. Технология защиты информации. Информационная безопасность.	2		4	10	16	Текущий тестовый контроль, контрольные вопросы , задания для практических занятий
2.	Раздел 2. Математическая основа защиты информации	6		10	10	26	Текущий тестовый контроль, контрольные вопросы, задания для практических занятий
3.	Раздел 3. Элементы теории чисел.	6		10	20	36	Текущий тестовый контроль, контрольные вопросы, задания для практических занятий
4.	Раздел 4. Криптографические методы и средства обеспечения информационной безопасности	4		12	12	28	Текущий тестовый контроль, контрольные вопросы, задания для практических занятий
5	Контактная внеаудиторная работа					1,5	Индивидуальные и групповые консультации
	Промежуточная аттестация					**0,5**	Зачет с оценкой
Итого часов в 6 семестре:		**18**	**-**	**36**	**52**	**108**	
Всего:						**108**	

4.2.2. Лекционный курс

№ п/п	Наименование раздела дисциплины	Наименование темы лекции	Содержание лекции	Всего Часов (ОФО)
1	2	3	4	5
Семестр 6				
1.	Раздел 1. Технология защиты информации. Информационная безопасность.	1.1. Основные угрозы информации в компьютерных системах Понятие безопасности. Информационные ресурсы. Аппаратно-программные средства защиты информации.	Понятие безопасности. Информационные ресурсы. Взаимосвязь понятий информационной безопасности и защиты информации. Особенности защиты информации. Уязвимость информации. Понятие несанкционированного доступа к конфиденциальной информации. Дискреционная и мандатная политика безопасности. Правовые методы обеспечения информационной безопасности.	**2**
2.	Раздел 2. Математическая основа защиты информации	2.1 Теория чисел. Сложение по модулю. Теория чисел. Деление по модулю. Арифметика часов. Программирование алгоритма шифрования	Модулярная арифметика. Простые и составные числа. Числа близнецы. Задача факторизации. Основная теорема арифметики. Взаимно простые числа. Теорема Ферма-Эйлера. Наибольший общий делитель.	**2**
		2.2 Классификация технических средств защиты информации. Малая теорема Ферма	Физические средства защиты. Межсетевые экраны. Аутентификация пользователей на основе паролей и модели «рукопожатия». Аутентификация пользователей по биометрическим характеристикам	**2**
3.	Раздел 3. Элементы теории чисел.	3.1 Элементы теории чисел Функция Эйлера. Каноническое разложение чисел.	Взаимно простые числа. Сравнимость по модулю. Нахождение вычета некоторого числа по модулю. Кольцо вычетов. Арифметика часов. НОД. Алгоритм Эвклида. Инверсия по модулю.	**4**
		3.2 Основные понятия криптологии. Методы шифрования. Математические и инструментальные основы шифрования	Алгоритмы шифрования. Симметричные и асимметричные криптосистемы. Абсолютно стойкий шифр.	**2**
4.	Раздел 4. Криптографические методы и сред-	4.1 Защита программных средств от не санкционированного	Хеширование. Криптографическая система DES и ее модификация	**4**

	ства обеспечения информационной безопасности	использования	Алгоритм шифрования RSA	
		4.2 Вредоносные программы	Классификация вредоносных программы. Загрузочные и файловые вирусы. Методы обнаружения и удаления вирусов. Программные закладки и методы защиты от них.	**2**
ИТОГО часов в семестре:				**18**
Всего:				**18**

4.2.3. Практические занятия

№ п/п	**Наименование раздела дисциплины**	**Наименование практического занятия**	**Содержание практического занятия**	**Всего часов (ОФО)**
1	2	3	4	5
Семестр 6				
1.	Раздел 1. Технология защиты информации. Информационная безопасность.	1.1 Понятие безопасности. Информационные ресурсы. Аппаратно-программные средства защиты информации	Особенности защиты информации. Уязвимость информации. Понятие несанкционированного доступа к конфиденциальной информации. Дискреционная и мандатная политика безопасности. Правовые методы обеспечения информационной безопасности.	**8**
2	Раздел 2. Математическая основа защиты информации	2.1 Электронная цифровая подпись. Вычисление ЭЦП.	Теория чисел. Разложение чисел на простые множители Деление по модулю. Арифметика часов. Программирование алгоритма шифрования	**8**
3	Раздел 3. Элементы теории чисел.	3.1 Симметричное шифрование	Шифрование методом блочной перестановки. Шифр Гронсфельда. Программная реализация	**8**
		3.2 Асимметричное шифрование	Шифрование перестановочным шифром. Одноалфавитное шифрование. Цифровая подпись.	**6**
4	Раздел 4. Криптографические методы и средства обеспечения информационной безопасности	4.1 Методика использования антивирусных программ	Использование двух ключей: открытый и закрытый. Шифр RSA. Программная реализация	**6**
ИТОГО часов в 6 семестре:				**36**
Всего:				**36**

4.3. Самостоятельная работа обучающегося

№ п/п	Наименование раздела (темы) дисциплины	№ п/п	Виды СРО	Всего Часов (ОФО)
1	3	4	5	6
Семестр 6				
1.	Раздел 1. Технология защиты информации. Информационная безопасность.	1.1	Работа с основной и дополнительной литературой. Чтение конспекта лекций. Подготовка к лабораторному практикуму.	10
2.	Раздел 2. Математическая основа защиты информации	2.1	Проработка лекций, работа с учебниками. Подготовка к практическим занятиям.	10
		2.2	Изучение конспекта лекций. Выполнения индивидуальных заданий по практикуму.	
3.	Раздел 3. Элементы теории чисел.	3.1	Работа с лекционным материалом, поиск и обзор литературы и электронных источников информации по теме теории чисел	20
		3.2	Изучение конспекта лекций для выполнения практической работы	
4.	Раздел 4. Криптографические методы и средства обеспечения информационной безопасности	4.1	Изучение конспекта лекций для выполнения практической работы.	12
		4.2	Изучение конспекта лекций. Выполнения практических задач.	
ИТОГО часов в 6 семестре:				**52**
Всего:				**52**

5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

5.1. Методические указания для подготовки обучающихся к лекционным занятиям

Обучающийся, готовясь к лекционному занятию, включает выполнение всех видов заданий размещенных в каждой лекции, т.е. задания выполняются еще до лекционного занятия по соответствующей теме. В ходе лекционных занятий, обучающийся должен вести конспектирование лекционного материала, обращать внимание на термины и определения, а также формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Обучающийся должен оставить в рабочих конспектах поля, на которых делает пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. Обучающийся также должен задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций. Дорабатывать свой конспект лекции, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной учебной программой. Обучающийся должен уметь проводить текущей лекции с предшествующей лекцией.

5.2. Методические указания для подготовки обучающихся к лабораторным занятиям (не предусмотрено)

5.3. Методические указания для подготовки обучающихся к практическим занятиям

В ходе подготовки к практическим занятиям, обучающийся должен:

- изучить основную и дополнительную литературу, ознакомиться с новыми публикациями в периодических и электронных изданиях по теме практического занятия учебной программы;
- подготовиться к устному опросу, для этого подготовить ответы по всем учебным вопросам, выносимым на практическое занятие;
- подготовиться к выполнению текущего практического занятия, изучая соответствующую тему лекции;
- после прохождения каждого раздела, обучающийся, для целей закрепления пройденного материала проходит тесты;
- осуществляет самоконтроль качества подготовки к практическому занятию, осуществляя проверку своих знаний, отвечая на вопросы для самопроверки по соответствующей теме.
- обучающийся, при подготовке к практическому занятию может консультироваться с преподавателем через электронную почту и получать от него наводящие разъяснения.

5.4. Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обучающихся включает в себя выполнение различного рода заданий, которые ориентированы на более глубокое усвоение материала изучаемой дисциплины. По каждой теме дисциплины обучающимся 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. Обучающимся следует:

- руководствоваться графиком самостоятельной работы, определенным на кафедре;
- выполнять все плановые задания, выдаваемые преподавателем для самостоятельного выполнения, и разбирать неясные вопросы на лабораторных и практических занятиях, а также получить информацию на консультациях.

5.5 Методические рекомендации прохождения тестирования

Подготовку к итоговому тестированию необходимо осуществлять поэтапно.

На первом этапе необходимо повторить основные положения всех тем, детально разбирая наиболее сложные моменты. Непонятные вопросы необходимо выписывать, чтобы по ним можно было проконсультироваться с преподавателем перед прохождением итогового тестирования. Подготовку по темам каждой дидактической единицы целесообразно производить отдельно. На этом этапе необходимо использовать материалы лекционного курса, материалы семинарских занятий, тестовые задания для текущего контроля знаний, а также презентации лекционного курса.

На втором этапе подготовки предлагается без повторения теоретического материала дать ответы тестовые задания для рубежного контроля знаний. Если ответы на какие-то вопросы вызвали затруднение, необходимо еще раз повторить соответствующий теоретический материал.

Наконец, третий этап подготовки необходимо осуществить непосредственно накануне теста. На данном этапе необходимо аккуратно просмотреть весь лекционный курс.

В случае, если результаты выполнения тестового задания оказались неудовлетворительными, необходимо зафиксировать темы, на вопросы по которым были даны неверные ответы, и еще раз углубленно повторить соответствующие темы в соответствии с указанными выше тремя этапами подготовки к тестированию

5.6 Работа с литературными источниками и интернет ресурсами

В процессе подготовки к практическим занятиям, обучающимся необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы.

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме.

Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем по каждой теме семинарского или практического занятия, что позволяет обучающимся проявить свою индивидуальность в рамках выступления на данных занятиях, выявить широкий спектр мнений по изучаемой проблеме.

5.7. Промежуточная аттестация

По итогам семестра проводится зачет с оценкой. При подготовке к сдаче зачета с оценкой рекомендуется пользоваться материалами лекции и практических занятий, и материалами, изученными в ходе текущей самостоятельной работы. Зачет с оценкой проводится в устной или письменной форме. К зачету с оценкой допускаются обучающиеся, которые выполнили индивидуальные задания к практическим занятиям.

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

№ п/п	Виды учебной работы	Образовательные технологии	Всего часов
1	2	3	4
Семестр 6			
1	Арифметика часов. НОД. Алгоритм Эвклида. Инверсия по модулю.	Лекция–информация. Метод мозгового штурма	2
2	Взаимно простые числа. Теорема Ферма-Эйлера.	Лекция – информация. Презентация Метод мозгового штурма	2
4	Теория чисел. Сложение по модулю. Теория чисел. Деление по модулю. Арифметика часов. Программирование алгоритма шифрования	Лекция – информация. Презентация Метод мозгового штурма	2
5	Деление по модулю. Арифметика часов.	Лекция – информация. Презентация Метод мозгового штурма	2
6	Электронная цифровая подпись. Вычисление ЭЦП.	Лекция – информация. Презентация	2
7	Понятие безопасности. Информационные ресурсы. Аппаратно-программные средства защиты информации	Лекция – информация. Презентация	2
Итого часов в 6 семестре:			**12**
Всего:			**12**

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

1. Алешников С.И. Математические методы защиты информации. Часть 5. Методы алгебраических кривых : учебное пособие / Алешников С.И., Алексеенко Е.С.. — Калининград : Балтийский федеральный университет им. Иммануила Канта, 2010. — 158 c. — ISBN 978-5-9971-0073-5. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/23796.html . — Режим доступа: для авторизир. пользователей
2. Метелица Н.Т. Вычислительные сети и защита информации : учебное пособие / Метелица Н.Т.. — Краснодар : Южный институт менеджмента, 2013. — 48 c. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/25962.html . — Режим доступа: для авторизир. пользователей
3. Краковский Ю.М. Защита информации : учебное пособие / Краковский Ю.М.. — Ростов-на-Дону : Феникс, 2016. — 349 c. — ISBN 978-5-222-26911-4. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/59350.html. — Режим доступа: для авторизир. пользователей: https://www.iprbookshop.ru/59350.html

Дополнительная литература

1. Алешников С.И. Математические методы защиты информации. Часть 3. Вычислительный практикум по числовым полям и криптографии в квадратичных полях : практическое пособие / Алешников С.И., Козьминых Е.В.. — Калининград : Балтийский федеральный университет им. Иммануила Канта, 2006. — 97 c. — ISBN 5-88874-689-4. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/23851.html . — Режим доступа: для авторизир. пользователей
2. Никифоров С.Н. Защита информации. Защита от внешних вторжений : учебное пособие / Никифоров С.Н.. — Санкт-Петербург : Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017. — 84 c. — ISBN 978-5-9227-0757-2. — Текст электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/74381.html — Режим доступа: для авторизир. пользователей

7.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

http://elibrary.ru - Научная электронная библиотека.

7.3. Информационные технологии, лицензионное программное обеспечение

Лицензионное программное обеспечение	Реквизиты лицензий/ договоров
Антивирус Dr.Web Desktop Security Suite	Лицензионный договор № 621 Срок действия: с 25.09.2025 до 24.09.2026
Консультант Плюс	Договор № 7 от 15.01.2026 г.
Цифровой образовательный ресурс IPR SMART	Лицензионный договор № 12873/25П от 02.07.2025 г. Срок действия: с 01.07.2025 г. до 30.06.2026 г.
Бесплатное ПО	
LibreOffice, OpenOffice, Sumatra PDF, 7-Zip, Adobe Acrobat Reader	

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

8.1. Требования к аудиториям (помещениям, местам) для проведения занятий

1.Учебная аудитория для проведения занятий лекционного типа
Ауд.243
Специализированная мебель:
Кафедра настольная - 1шт., доска меловая - 1шт., стулья – 65 шт., парты - 34шт.
Технические средства обучения, служащие для предоставления учебной информации большой аудитории:
Экран на штативе – 1 шт.
Проектор – 1 шт.
Ноутбук – 1 шт

2.Учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнение курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации
Ауд.251
Специализированная мебель:
Стол преподавательский - 1шт., компьютерные столы - 10шт., парты -7шт., стулья - 24шт., доска меловая - 1шт.
Лабораторное оборудование, технические средства обучения, служащие для предоставления учебной информации большой аудитории:
Персональный компьютер – 10 шт.
Экран настенный рулонный – 1 шт.

3.Лаборатория компьютерной графики
Ауд.251
Специализированная мебель:
Стол преподавательский - 1шт., компьютерные столы - 10шт., парты -7шт., стулья - 24шт., доска меловая - 1шт.
Лабораторное оборудование, технические средства обучения, служащие для предоставления учебной информации большой аудитории:
Персональный компьютер – 10 шт.
Экран настенный рулонный – 1 шт.

8.2. Требования к оборудованию рабочих мест преподавателя и обучающихся

Рабочее место преподавателя, оснащенное компьютером с доступом в Интернет.

Рабочие места обучающихся, оснащенные компьютерами с доступом в Интернет, предназначенные для работы в электронной образовательной среде, и т.п.

8.3. Требования к специализированному оборудованию нет

9. ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Для обеспечения образования инвалидов и обучающихся с ограниченными возможностями здоровья разрабатывается (в случае необходимости) адаптированная образовательная программа, индивидуальный учебный план с учетом особенностей их психофизического развития и состояния здоровья, в частности применяется индивидуальный подход к освоению дисциплины, индивидуальные задания: рефераты, письменные работы и, наоборот, только устные ответы и диалоги, индивидуальные консультации, использование диктофона и других записывающих средств для воспроизведения лекционного и семинарского материала.

В целях обеспечения обучающихся инвалидов и лиц с ограниченными возможностями здоровья комплектуется фонд основной учебной литературой, адаптированной к ограничению электронных образовательных ресурсов, доступ к которым организован в БИЦ Академии. В библиотеке проводятся индивидуальные консультации для данной категории пользователей, оказывается помощь в регистрации и использовании сетевых и локальных электронных образовательных ресурсов, предоставляются места в читальном зале.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ «Математические основы защиты информации»

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

«Математические основы защиты информации»

Компетенции, формируемые в процессе изучения дисциплины

Индекс	Формулировка компетенции
ОПК-5	Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения

2. Этапы формирования компетенции в процессе освоения дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой разделов (тем) учебных занятий. Изучение каждого раздела (темы) предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций обучающимися.

Этапность формирования компетенций прямо связана с местом дисциплины в образовательной программе.

Разделы (темы) дисциплины	**Формируемые компетенции (коды)**
	ОПК-5
Раздел 1. Технология защиты информации. Информационная безопасность.	+
Раздел 2. Математическая основа защиты информации	+
Раздел 3. Элементы теория чисел	+
Раздел 4. Криптографические методы и средства обеспечения информационной безопасности	+

1. Показатели, критерии и средства оценивания компетенций, формируемых в процессе изучения дисциплины

ОПК-5

Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения

Индикаторы достижения компетенции	**Критерии оценивания результатов обучения**				**Средства оценивания результатов обучения**	
	неудовлетв	**удовлетв**	**хорошо**	**отлично**	**Текущий контроль**	**Промежуточная аттестация**
ОПК-5.1 Обладает базовыми знаниями в области алгоритмизации и программирования	Допускает существенные ошибки в знаниях стандартных пакетов прикладных программ для решения практических задач защиты информации, отлаживать и тестировать программы по алгоритмам шифрования; пробелы в знаниях элементов теории чисел.	Демонстрирует некоторые способности в знаниях стандартных пакетов прикладных программ для решения практических задач защиты информации, отлаживать и тестировать программы по алгоритмам шифрования, а также криптографическим методам и средств обеспечения информационной безопасности.	Демонстрирует способность в знаниях стандартных пакетов прикладных программ для решения практических задач защиты информации, отлаживать и тестировать программы по алгоритмам шифрования, а также криптографическим методам и средств обеспечения информационной безопасности	Демонстрирует профессиональную способность к языкам программирования, для целей автоматизации шифрования информации; методов кодирования; знания о государственной политике в области безопасности компьютерных систем; знания элементов теории чисел, составляющие математическую основу криптографических	Текущий тестовый контроль, контрольные вопросы	Зачет с оценкой
ОПК-5.2 Использует структурные особенности языков программирования и пакетов прикладных программ при реализации алгоритмов для решения прикладных задач	Допускает частично освоенное умение пользоваться стандартными программами для решения практических задач защиты информации; отлаживать и тестировать программы по алгоритмам шифрования; применять крипто-	Демонстрирует в целом удовлетворительные, но не систематизированные умения пользоваться стандартными программами для решения практических задач защиты информации; отлаживать и тестировать программы по алгоритмам шифрования; применять криптографические мето-	Демонстрирует в целом хорошие, но содержащие отдельные пробелы в использовании стандартных программ для решения практических задач защиты информации; отлаживать и тестировать программы по алгоритмам шифрования; применять элементы теории чисел для мо-	Демонстрирует умения в использовании стандартных программ для решения практических задач защиты информации; отлаживать и тестировать программы по алгоритмам шифрования; применять элементы теории чисел для задач криптографических методов и средств обеспечения ин-	Текущий тестовый контроль, контрольные вопросы	Зачет с оценкой

	графические методы и средства обеспечения информационной безопасности.	ды и средства обеспечения информационной безопасности; использовать элементы теории чисел для моделирования задач защиты информации.	делирования задач криптографии.	формационной безопасности.		
ОПК-5.3 Разрабатывает компьютерные программы, пригодные для практического использования	Фрагментарно владеет некоторыми пакетами стандартных программ для решения задач защиты информации; не владеет интернет технологиями для организации защиты информации, не владеет возможностями математической основы криптографии теории чисел.	Владеет отдельными навыками работы со стандартными программам для решения задач защиты информации; технологиями отладки и тестирования программ по алгоритмам шифрования; элементов теории чисел для моделирования задач защиты информации.	Демонстрирует в целом успешные знания по стандартным программам для решения практических задач защиты информации; технологии отладки и тестирования программ по алгоритмам шифрования; по криптографическим методам и средствам обеспечения информационной безопасности.	Демонстрирует профессиональные навыки работы в специализированных стандартных пакетах программ для решения практических задач защиты информации; владеет технологиями отладки и тестирования программ по алгоритмам шифрования; владеет способностью применять элементы теории чисел для решения задач криптографии.	Текущий тестовый контроль, контрольные вопросы	Зачет с оценкой

4. Комплект контрольно-оценочных средств по дисциплине

Вопросы к зачету с оценкой
по дисциплине
Математические основы защиты информации

1. Проблема защиты информации и подходы к ее решению.
2. Основные понятия защиты информации.
3. Угрозы безопасности и каналы утечки информации.
4. Классификация методов и средств защиты информации.
5. Способы нарушения защищенности информации и защиты от него в компьютерных системах.
6. Организация базы учетных записей пользователей в ОС Windows
7. Способы аутентификации пользователей.
8. Математические основы защиты ирформации.
9. Протоколы прямой аутентификации.
10. Протоколы непрямой аутентификации.
11. Виртуальные частные сети.
12. Разграничение прав пользователей в ОС Windows.
13. Дискреционное, мандатное и ролевое разграничение доступа к объектам.
14. Подсистема безопасности ОС Windows.
15. Разграничение доступа к объектам в ОС Windows.
16. Средства защиты информации в глобальных компьютерных сетях.
17. Стандарты оценки безопасности компьютерных систем
18. Элементы теории чисел.
19. Способы симметричного шифрования. Абсолютно стойкий шифр.
20. Генерация, хранение и распространение ключей.
21. Криптографическая система DES и ее модификации.
22. Криптографическая система ГОСТ 28147-89.
23. Применение и обзор современных симметричных криптосистем.
24. Принципы построения, свойства и применение асимметричных криптосистем.
25. Криптографическая система RSA.
26. Криптографические системы Диффи-Хеллмана, Эль-Гамаля
27. Электронная цифровая подпись и ее применение. Функции хеширования.
28. Принципы построения систем защиты от копирования.
29. Защита инсталляционных дисков и установленного программного обеспечения.
30. Защита программных средств от изучения.
31. Вредоносные программы, их признаки и классификация.
32. Программные закладки и защита от них.
33. Методы обнаружения и удаления вредоносных программ

Контрольные вопросы к разделам

по дисциплине

Математические основы защиты информации

Раздел 1. В каких формах может быть представлена информация?

1. Что относится к информации ограниченного доступа?

2. Что понимается под защитой информации?
3. Что относится к основным характеристикам защищаемой информации?
4. Что такое угроза безопасности информации? Каковы основные виды угроз?
5. Какие существуют каналы утечки конфиденциальной информации?
10. Почему проблема защиты информации не может быть решена с помощью только формальных методов и средств?
11. В чем сущность организационной защиты информации?
12. Каковы уровни правового обеспечения информационной безопасности?
13. Какие законодательные акты составляют основу российского информационного права?
14. Какие существуют международные и российские стандарты в области безопасности компьютерных систем и информационных технологий?

Раздел 2. Какие существуют способы несанкционированного доступа к информации в компьютерных системах?

1. Какие способы аутентификации пользователей могут применяться в компьютерных системах?
2. В чем заключаются основные недостатки парольной аутентификации и как она может быть усилена?
3. В чем сущность, достоинства и недостатки аутентификации на основе модели «рукопожатия»?
4. Какие биометрические характеристики пользователей могут применяться для их аутентификации? В чем преимущества подобного способа подтверждения подлинности?
5. В чем специфика аутентификации пользователей на основе их клавиатурного почерка и росписи мышью?
6. Какие элементы аппаратного обеспечения могут применяться для хранения идентифицирующей информации для пользователей компьютерных систем?
10. Почему с помощью только программных средств нельзя обеспечить необходимую степень защищенности от локального несанкционированного доступа к информации в компьютерных системах?
13. Какие применяются разновидности межсетевых экранов?
14. Что такое VPN и для чего они предназначены?
15. Каковы общие недостатки всех межсетевых экранов?
16. В чем сущность, достоинства и недостатки дискреционного управления доступом к объектам КС?

Раздел 3.

1. Что называется вычетом целого числа по некоторому модулю?
2. Почему операции над вычетами находят широкое применение в криптографии?
3. В чем разница между симметричными и асимметричными криптографическими системами?
4. Какие основные способы применяются при создании алгоритмов симметричной криптографии?
5. В чем разница между потоковыми и блочными шифрами?
6. Какие симметричные криптосистемы используются сегодня?
7. В каких режимах может использоваться криптосистема DES?
8. Какие из режимов DES могут использоваться для проверки аутентичности и целостности шифротекста?
9. В каких режимах может использоваться криптосистема ГОСТ 28147-89? Как в ней обеспечивается аутентичность и целостность шифротекстов.
10. Что лежит в основе асимметричной криптографии?
11. В чем особенности и основные сферы применения асимметричных криптосистем?
12. На чем основана криптостойкость систем RSA и Эль-Гамаля?
13. Что такое электронная цифровая подпись, как она получается и проверяется?

14. Какова роль в системах ЭЦП функций хеширования?

15. Какую роль исполняют удостоверяющие центры? Что такое сертификат открытого ключа?

16. Какие функции CryptoAPI используются для получения и проверки электронной цифровой подписи?

17. Каков порядок вызова функций CryptoAPI при получении ЭЦП?

Раздел 4.

Какие программы относят к разряду вредоносных?

1. Что такое компьютерный вирус?
2. Какие существуют виды компьютерных вирусов?
3. В чем разница между загрузочными и файловыми вирусами?
5. Как происходит заражение и функционирование загрузочных вирусов?
6. Какие типы файлов могут заражаться файловыми вирусами?
7. Как происходит заражение программных файлов?
8. Почему файлы документов могут содержать вирусы?
9. Как обеспечивается автоматическое получение управления макровирусами?
10. Как включить встроенную защиту от вирусов в макросах в программах Microsoft Office? В чем недостатки этой защиты?
11. Какие существуют основные каналы заражения вирусами объектов компьютерной системы?
12. Какие существуют методы автоматического обнаружения и удаления вирусов? В чем их достоинства и недостатки?
13. В чем заключается профилактика заражения компьютерными вирусами?
14. Какие виды программных закладок существуют?
15. Как может происходить проникновение программной закладки в компьютерную систему?
16. Как осуществляется взаимодействие внедренной в КС программной закладки и нарушителя?
17. Какие существуют методы защиты от программных закладок? Что такое изолированная программная среда?
18. Что называется защитой программных продуктов от несанкционированного копирования?
19. На каких принципах должна основываться разработка системы защиты от копирования?
20. Какие требования предъявляются к системам защиты от копирования?
21. Из каких основных компонентов состоит типовая система защиты от копирования?
22. Какие характеристики компьютера могут использоваться для настройки защищаемого программного продукта?
23. В чем заключается достоинства и недостатки программно-аппаратной защиты от копирования на основе электронных ключей?

Тестовые задания

по дисциплине
Математические основы защиты информации

1. Формы представления информации в плане защиты информации

1. Цифровая, документированная, графическая
2. Программная, алгоритмическая, телекоммуникационная
3.Электронная, реквизитная, текстовая
4. Речевая, документированная, телекоммуникационная

2. Документированной называется информация

1. Представленная на материальных носителях вместе с идентифицирующими ее реквизитами
2. Представленная в виде кодов и сохраненная на лазерных дисках объемом 1,5 Мб.
3.Представленная только на жестких магнитных дисках вместе с идентифицирующими ее реквизитами
4. Закодированная и защищенная паролем, и представленная на носителях вместе с идентифицирующими ее реквизитами

3. К информации ограниченного доступа относится

1. Служебные сведения, не подлежащие распространению в сети интернет
2.Конфиденциальная информация, хранимая в государственных архивах данных
3.Информация, запрашиваемая гражданами в органах государственной власти
4.Государственная тайна и конфиденциальная информация.

4. Под защитой информации понимается

1. Комплекс мероприятий, направленных на обеспечение важнейших аспектов информационной безопасности
2. Комплекс мероприятий, направленных на обеспечение целостности информации
3. Комплекс мероприятий, направленных на обеспечение хранения информации
4. Комплекс мероприятий, направленных на ввод, хранения, обработки и передачи данных

5. К основным характеристикам защищаемой информации относится

1. Кодируемость, корректность, целостность
2. Государственность, служебность, доступность
3. Конфиденциальность, целостность и доступность
4. Целостность, защищенность и доступность

6. Угроза безопасности информации это

1.Событие или действие, которое может вызвать изменение функционирования компьютерных систем, связанное с нарушением защищенности, обрабатываемой в ней информации
2. Действие, которое может вызвать искажение обрабатываемой информации
3. Событие, которое может послужить потере конфиденциальной информации
4. Событие или действие, которое может вызвать изменение функционирования физического канала связи в компьютерных системах, по которому передается защищаемая информация

7. ПЭМИН –это утечка информации через_____

8. Уровни правового обеспечения информационной безопасности

1.Международные договоры, подзаконные акты, государственные стандарты, локальные нормативные акты

2. Международные договоры, Федеральные законы, государственные стандарты, Указы Президента РФ

3. Подзаконные акты, государственные стандарты, Постановления Правительства РФ

4. Локальные нормативные акты, письма Арбитражного Суда РФ, международные договоры

9.Комплексная система защиты информации

1. Это совокупность методов и средств, объединенных единым целевым назначением и обеспечивающих необходимую эффективность защиты информации в КС.

2. Это совокупность объединенных единым целевым назначением средств, для обеспечения защиты информации в КС.

3. Это совокупность правил, законов и писем, в которых прописаны методы и средства обеспечивающих необходимую эффективность защиты информации в КС.

4. Это свод правил утвержденные законодательно в целях организации эффективной защиты информации в КС

Раздел 2. Методы защиты информации от несанкционированного доступа

10. Основные способы защиты от несанкционированного доступа к информации в компьютерных системах

1. Идентификация, авторизация, шифрование
2. Аутентификация, авторизация, шифрование
3. Шифрование, аутентификация, электронная цифровая подпись
4. Электронная цифровая подпись, авторизация, шифрование

11.Основные недостатки парольной аутентификации

1.Сложно обеспечить реальную уникальность и сложность каждого вновь выбираемого пользователем пароля

2. Возможность перехвата пароля в открытом виде или его подбора по хеш-значению
3. Возможность получения или смены пароля в результате обмана
4. Все вышеперечисленные недостатки

12.Сущность модели рукопожатия_____

13. Биометрические характеристики пользователей, которые могут применяться для их аутентификации

1.Отпечатки пальцев, геометрическая форма руки, узор радужной оболочки глаза
2. Рисунок сетчатки глаза, геометрическая форма и размеры лица
3. Тембр голоса, геометрическая форма и размеры уха
4. Все выше перечисленные биометрические характеристики

14.Характерные особенности аутентификации пользователей на основе их клавиатурного почерка и росписи мышью?

1. Стабильность их характеристик для всех пользователей независимо от возраста и эмоционально- психологического состояния

2. Нестабильность их характеристик у одного и того же пользователя, связанными с улучшением навыков по работе с клавиатурой и мышью или наоборот из-за старения организма, а также с изменениями, связанными с эмоциональным состоянием пользователя.

3. Нарушение навыков по работе с клавиатурой и мышью или наоборот из-за старения орга-

низма, а также с изменениями, связанными с эмоциональным состоянием пользователя.

4. Нестабильность их характеристик у одного и того же пользователя, связанными с улучшением их психологического состояния

15.Элементы аппаратного обеспечения, которые могут применяться для хранения идентифицирующей информации для пользователей компьютерных систем

1. Магнитные диски, пластиковые карты с магнитной полосой, Touch Mamory, карты со штрих-кодом, смарт-карты, маркеры eToken (USB-брелки)
2. Магнитные диски, пластиковые карты, iButton, карты со штрих-кодом, смарт-карты, USB-брелки
3. Магнитные диски, пластиковые карты с магнитной полосой, карты со штрих-кодом, карты с памятью, смарт-карты, маркеры eToken
4. 2. Магнитные диски, пластиковые карты, Touch Mamory, карты со штрих-кодом, смарт-карты с паролем, USB-брелки с памятью

16.Touch Memory представляет собой

1. Миниатюрную батарейку с определенным диаметром и толщиной, имеющий один сигнальный контакт и один контакт заземления
2. Миниатюрную батарейку с определенным диаметром 16мм и толщиной в пределах от 3 до 6 мм, имеющий один сигнальный контакт и один контакт заземления
3. Миниатюрную батарейку с определенным диаметром 15 мм и толщиной в пределах от 4 до 6 мм, имеющий один сигнальный контакт и один контакт заземления
4. Миниатюрную батарейку с ПЗУ и ОЗУ со встроенным элементом питания

17.Двухфакторная аутентификация это_____

18. В основе работы протокола S/Key лежит протокол PAP для _____

19.Протокол CHAP основан на модели _____

20. Протокол Kerberos предназначен для_____

21.Применяемые разновидности межсетевых экранов

1.фильтрующие маршрутизаторы
2. шлюзы сеансового уровня
3.шлюзы прикладного уровня
4. все вышеперечисленные

22.VPN предназначены_____

23. Пароли пользователей в открытых версиях операционной системы Windows сохраняются в файле с расширением _____

24. Достоинства дискреционного управления доступом к объектам КС

1. простота идентификации, возможность описания пользователем доступ к своим ресурсам

2. детализированность и назначение прав доступа
3. простата реализации доступом к объектам КС и гибкость
4. простота администрирования и гибкость

25. Достоинства мандатного управления доступом к объектам КС

1. простата построения общей схемы доступа и простата администрирования, высокая надежность работы с КС
2. гибкость программной реализации и простота администрирования
3. назначение прав доступа без разграничения пользователей всех уровней
4. правило доступа к объекту осуществляется через специальные модели матрицы доступа

26. Что называется вычетом целого числа a по некоторому модулю n?

1. Если $b \geq 0$, a = b {mod n} и $|b| < n$, то b называют вычетом числа a по модулю n.
2. Если $b \leq 0$, a = b {mod n} и $|b| < n$, то b называют вычетом числа a по модулю n.
3. Если $b = 1$, a = b {mod n} и $|b| < n$, то b называют вычетом числа a по модулю n.
4. Если $b \geq 0$, a = b {div n} и $|b| < n$, то b называют вычетом числа a по модулю n.

27. В чем разница между симметричными и асимметричными криптографическими системами?

1. Симметричные криптосистемы применяют один ключ и для шифрования и расшифровывания, а асимметричные – разные ключи
2. Симметричные криптосистемы применяют разные ключи, а асимметричные - один ключ и для шифрования и расшифровывания
3. Симметричные криптосистемы применяют один ключ и для шифрования и расшифровывания и он является несекретным, а асимметричные – разные ключи, которые являются секретными
4. Симметричные криптосистемы применяют один ключ и для шифрования и расшифровывания, а асимметричные – разные ключи являющиеся в свою очередь открытыми и закрытыми

28. Основные способы, которые применяются при создании алгоритмов симметричной криптографии

1. перестановки, сочетание и гаммирование
2. перестановки, подстановки и гаммирование
3. перестановки, замещение и гаммирование
4. перемещение, замещение и гаммирование

29 Какие из режимов DES могут использоваться для проверки аутентичности и целостности шифротекста?_____

30. К асимметричным криптографическим системам относятся _____

Комплект заданий для практической работы

по дисциплине Математические основы защиты информации

Раздел 1. Технология защиты информации. Информационная безопасность.

Практическая работа № 1

Тема: Теория чисел. Деление по модулю. Арифметика часов.
Программирование алгоритма шифрования
Цель: Изучить алгоритм шифрования методом гаммирования
Краткое содержание:
1. Алгоритм шифрования открытого текста методом гаммирования. Листинг программы
2. Ознакомиться с алгоритмом шифрования
3. Автоматизировать на одном из языков программирования
Рекомендации по организации самостоятельной работы:
- изучение поставленной задачи в практической работе
- изучение электронных источников по теме практической работы.
Содержание отчёта:
подготовка отчета в соответствии с заданием к практической работе.
Форма отчёта: устная защита практической работы

Практическая работа № 2

Тема: Шифрование методом одноалфавитной подстановки. Программная реализация.
Цель: Изучить алгоритм шифрования методом одноалфавитной подстановки.
Краткое содержание:
2. Ознакомиться с алгоритмом шифрования одноалфавитной подстановки.
3. Автоматизировать на одном из языков программирования
Рекомендации по организации самостоятельной работы:
- изучение поставленной задачи в практической работе
- изучение электронных источников по теме практической работы.
Содержание отчёта:
подготовка отчета в соответствии с заданием к практической работе.
Форма отчёта: устная защита практической работы

Практическая работа № 3

Тема: Настройка программного генератора паролей
Цель: Научиться создавать в системе Lazarus генератор паролей
Краткое содержание:
1. Создание генератора паролей в среде Lazarus.
2. Представить листинг программы
3. Шифрование текстового файла методом Вижинера.
4.Написать программу шифрование и дешифрования текстового файла методом Вижинера на одном из языков программирования
Рекомендации по организации самостоятельной работы:
- изучение поставленной задачи
- изучение задания к практической работе
- изучение электронных источников по теме практической работы.

Содержание отчёта:
подготовка отчета в соответствии с заданием к практической работе.
Форма отчёта: устная защита практической работы.

Раздел 2. Математическая основа защиты информации

Практическая работа № 4

Тема: Криптографические системы

Цель: Изучение алгоритма Эль-Гамаля.

Краткое содержание:

1. Алгоритм Эль-Гамаля. Решение задачи.
2. Работа в системе Lazarus по программированию криптосистемы Эль-Гамаля

Рекомендации по организации самостоятельной работы:

- изучение поставленной задачи
- изучение задания к практической работе
- изучение электронных источников по теме работы.

Содержание отчёта:

подготовка отчета в соответствии с заданием к практической работе.

Практическая работа № 5

Тема: Электронная цифровая подпись. Вычисление ЭЦП.

Цель: Изучить алгоритм шифрования электронной подписи

Краткое содержание:

1.Разобраться с алгоритмом шифрования электронной подписи на примере одной задачи

2. Автоматизировать на одном из языков программирования

Рекомендации по организации самостоятельной работы:

- изучение поставленной задачи в практической работе
- изучение электронных источников по теме практической работы.

Содержание отчёта:

подготовка отчета в соответствии с заданием к практической работе.

Форма отчёта: устная защита практической работы

Практическая работа № 6

Тема: Шифр Цезаря

Цель: Изучить алгоритм шифрования Цезаря

Краткое содержание:

1.Разобраться с алгоритмом шифрования Цезаря

2. Автоматизировать на одном из языков программирования

Рекомендации по организации самостоятельной работы:

- изучение поставленной задачи в практической работе
- изучение электронных источников по теме практической работы.

Содержание отчёта:

подготовка отчета в соответствии с заданием к практической работе.

Форма отчёта: устная защита практической работы

Раздел 3. Элементы теории чисел

Практическая работа № 7

Тема: Симметричное шифрование

Цель: Изучение алгоритма симметричного шифрования

Краткое содержание:

1. Алгоритм симметричного шифрования
2. Шифрование методом блочной перестановки.
3. Автоматизировать задачу шифрования в системе Lazarus шифра Гронсфельда.

Рекомендации по организации самостоятельной работы:

- изучение поставленной задачи в практической работе.
- изучение электронных источников по теме практической работы.

Содержание отчёта:
подготовка отчета в соответствии с заданием к практической работе.

Форма отчёта: представить листинг программ шифрования на одном из языков программирования методами Гронсфельда и Вижинера. Устная защита. Преподавателю сдать электронный вариант программы.

Практическая работа № 8
Тема: Асимметричное шифрование
Цель: Изучение алгоритма асимметричного шифрования
Краткое содержание:
1. Использование двух ключей: открытый и закрытый.
2. Электронная цифровая подпись с помощью шифра RSA.
3. Шифр Диффи-Хелмана
Рекомендации по организации самостоятельной работы:
- изучение поставленной задачи в практической работе
- изучение электронных источников по теме практической работы.
Содержание отчёта:
подготовка отчета в соответствии с заданием к практической работе.
Форма отчёта: представить листинг программ шифрования на одном из языков программирования для шифров RSA, Диффи-Хелмана и Электронная цифровая подпись. Защитить устно. Преподавателю сдать электронный вариант программ шифрования.

Раздел 4. Криптографические методы и средства обеспечения информационной безопасности
Тема: Методика использования антивирусных программ
Цель: Изучение интерфейса антивирусных программ
Краткое содержание:
1. Изучение функциональных возможностей антивирусной программы «Антивирус Касперского».
2. Проверка на вирус всех критических областей ПК.
Рекомендации по организации самостоятельной работы:
- изучение поставленной задачи в практической работе
- изучение электронных источников по теме практической работы.

5. Методические материалы, определяющие процедуры оценивания компетенции

5.1 Критерии оценивания качества выполнения практических работ

Оценка **«зачтено»** выставляется обучающемуся, если практическая работа выполнена правильно и обучающийся ответил на все вопросы, поставленные преподавателем на защите.
Оценка **«не зачтено»** выставляется обучающемуся, если практическая работа выполнена не правильно или обучающийся не проявил глубоких теоретических знаний при защите работы

5.2 Критерии оценивания качества устного ответа

Оценка **«отлично»** выставляется за глубокое знание предусмотренного программой материала, за умение четко, лаконично и логически последовательно отвечать на поставленные вопросы.
Оценка **«хорошо»** – за твердое знание основного (программного) материала, за грамотные, без существенных неточностей ответы на поставленные вопросы.
Оценка **«удовлетворительно»** – за общее знание только основного материала, за ответы, содержащие неточности или слабо аргументированные, с нарушением последовательности изложения материала.
Оценка **«неудовлетворительно»** – за незнание значительной части программного материала, за существенные ошибки в ответах на вопросы, за неумение ориентироваться в материале, за незнание основных понятий дисциплины.

5.3 Критерии оценивания тестирования

При тестировании все верные ответы берутся за 100%.
90%-100% отлично
75%-90% хорошо
60%-75% удовлетворительно
менее 60% неудовлетворительно

5.4 Критерии оценивания результатов освоения дисциплины

Оценка **«отлично»** выставляется за глубокое знание предусмотренного программой материала, содержащегося в основных и дополнительных рекомендованных литературных источниках, за умение четко, лаконично и логически последовательно отвечать на поставленные вопросы, за умение анализировать изучаемые явления в их взаимосвязи и диалектическом развитии, применять теоретические положения при решении практических задач.
Оценка **«хорошо»** – за твердое знание основного (программного) материала, включая расчеты (при необходимости), за грамотные, без существенных неточностей ответы на поставленные вопросы, за умение применять теоретические положения для решения практических задач.
Оценка **«удовлетворительно»** – за общее знание только основного материала, за ответы, содержащие неточности или слабо аргументированные, с нарушением последовательности изложения материала, за слабое применение теоретических положений при решении практических задач.
Оценка **«неудовлетворительно»** – за незнание значительной части программного материала, за существенные ошибки в ответах на вопросы, за неумение ориентироваться в расчетах, за незнание основных понятий дисциплины.