МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Нижегородский государственный технический университет им. Р.Е. Алексеева»
АРЗАМАССКИЙ ПОЛИТЕХНИЧЕСКИЙ ИНСТИТУТ (ФИЛИАЛ)

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00B4A6F7AAA383423E375F0ECF5610EF68
Владелец: Глебов Владимир Владимирович
Действителен: с 10.07.2025 до 03.10.2026

УТВЕРЖДАЮ:
Директор института:
_____ Глебов В.В.
«_25_» ___01___ _ 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДВ.03.02 Математические методы защиты информации
(индекс и наименование дисциплины по учебному плану)

для подготовки магистров

Направление подготовки 01.04.04 Прикладная математика
(код и направление подготовки)

Направленность Системы управления и обработки информации в инженерии
(наименование профиля, программы магистратуры)

Форма обучения очная
(очная, очно-заочная, заочная)

Год начала подготовки 2025

Объем дисциплины 108/3
(часов/з.е)

Промежуточная аттестация зачет с оценкой
(экзамен, зачет с оценкой, зачет)

Выпускающая кафедра Прикладная математика
(наименование кафедры)

Кафедра-разработчик Прикладная математика
(*наименование кафедры)*

Разработчик(и): Емельянова Т.В., к.т.н.
(ФИО, ученая степень, ученое звание)

г. Арзамас
2025 г.

Рабочая программа дисциплины разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО 3++) по направлению подготовки 01.04.04 Прикладная математика, утвержденного приказом Минобрнауки России от 10 января 2018 № 15, на основании учебного плана, принятого Ученым советом АПИ НГТУ, протокол от 29.01.2025 г. № 1

Рабочая программа одобрена на заседании кафедры, протокол от 25.12.2024 г. № 9

Заведующий кафедрой _____ Пакшин П.В.

(подпись) *(ФИО)*

Рабочая программа рекомендована к утверждению УМК АПИ НГТУ,

протокол от 29.01.2025 г. № 1

Зам. директора по УР _____ Шурыгин А.Ю.

(подпись)

Рабочая программа зарегистрирована в учебном отделе № 01.04.04-21

Начальник УО _____ Мельникова О.Ю.

(подпись)

Заведующая отделом библиотеки _____ Старостина О.Н.

(подпись)

Оглавление

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Цель освоения дисциплины (модуля)

Целью освоения дисциплины является подготовка студентов к выполнению профессиональных задач в рамках трудовой деятельности по профессиональным стандартам 40.011 «Проведение научно-исследовательских и опытно-конструкторских разработок» и 06.001 «Программист» в рамках обобщенных трудовых функций «Осуществление научного руководства в соответствующей области знаний», «Разработка требований и проектирование программного обеспечения» и изучение математических методов защиты информации, возможности и эффективности их применения в конкретных задачах защиты информации.

1.2. Задачи освоения дисциплины (модуля)

- ознакомление с основами компьютерной безопасности;
- освоение криптографических протоколов;
- изучение математических методов защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Математические методы защиты информации» относится к элективным дисциплинам блока дисциплин, формируемого участниками образовательных ОП ВО.

Дисциплина базируется на следующих дисциплинах: «Защита информации», «Логика и архитектура вычислительных сред».

Результаты обучения, полученные при освоении дисциплины, необходимы при изучении следующих дисциплин «Параллельное и распределенное программирование», «Средства разработки современного программного обеспечения» и при выполнении выпускной квалификационной работы.

Рабочая программа дисциплины «Математические методы защиты информации» для инвалидов и лиц с ограниченными возможностями здоровья разрабатывается индивидуально с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Процесс изучения дисциплины «Математические методы защиты информации» направлен на формирование элементов профессиональных компетенций ПКС-2 и ПКС-3 в соответствии с ОП ВО по направлению подготовки 01.04.04 «Прикладная математика».

Таблица 3.1 – Формирование компетенций дисциплинами

Код компетенции / наименование дисциплин, формирующих компетенцию совместно	Семестры формирования дисциплины Компетенции берутся из УП по направлению подготовки магистра			
	1	2	3	4
ПКС-2				
Навигационные системы	✔			
Принципы построения математических моделей	✔			
Моделирование в среде LabView		✔		
Технологическая (проектно-технологическая) практика		✔		
Вычислительная математика		✔		
Нечеткие модели			✔	
Анализ временных рядов			✔	
Средства разработки современного программного обеспечения			✔	

Код компетенции / наименование дисциплин, формирующих компетенцию совместно	Семестры формирования дисциплины Компетенции берутся из УП по направлению подготовки магистра			
	1	2	3	4
Математические методы защиты информации			✔	
Современная теория управления			✔	
Научно-исследовательская работа			✔	
Стохастическое моделирование			✔	
Научно-исследовательская работа				✔
Научно-производственная практика				✔
Преддипломная практика				✔
Выполнение и защита ВКР				✔
ПКС-3				
Защита информации		✔		
Средства разработки современного программного обеспечения			✔	
Математические методы защиты информации			✔	
Научно-исследовательская работа				✔
Преддипломная практика				✔
Выполнение и защита ВКР				✔

Перечень планируемых результатов обучения по дисциплине «Математические методы защиты информации», соотнесенных с планируемыми результатами освоения ОП, представлен в табл. 3.2.

Таблица 3.2 – Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОП

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине		
ПКС-2 Способен разрабатывать и исследовать математические модели, объектов, систем, процессов и технологий, предназначенных для проведения расчетов, анализа подготовки решений	ИПКС-2.1. Изучает методы математического моделирования, предназначенные для решения исследовательских задач, и современные математические и научные пакеты программ.	**Знать:** математические методы защиты информации и алгоритмы оценивания эффективности средств защиты информации	**Уметь:** самостоятельно осваивать новые математические методы защиты информации	**Владеть:** навыками применения математических методов защиты информации и оценивания эффективности применения их в прикладных задачах
ПКС-3 Способен разрабатывать наукоемкое программное обеспечение работы конкретного предприятия	ИПКС-3.2. Проектирует и разрабатывает программные комплексы для решения задач профессиональной деятельности.	**Знать:** современные алгоритмы реализации методов и способов защиты информации	**Уметь:** учитывать требования стандартов при разработке алгоритмов защиты информации	**Владеть:** методами обеспечения защищенности компьютерных систем от вредоносных программно-технических и информационных воздействий

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

4.1 Распределение трудоемкости дисциплины по видам работ по семестрам

Общая трудоемкость дисциплины составляет 3 зач. ед. или 108 часов, распределение часов по видам работ по семестрам представлено в таблице 4.1.

Таблица 4.1 – Распределение трудоемкости дисциплины по видам работ по семестрам для студентов очной формы обучения

Вид учебной работы	Трудоемкость в час	
	Всего час.	В т.ч. по семестрам 3 семестр
Формат изучения дисциплины	с использованием элементов электронного обучения	
Общая трудоемкость дисциплины по учебному плану	**108**	**108**
1. Контактная работа:	**54**	**54**
1.1. Аудиторная работа, в том числе:	**50**	**50**
занятия лекционного типа (Л)		
занятия семинарского типа (ПЗ – семинары, практические занятия и др.)	26	26
лабораторные работы (ЛР)	24	24
1.2. Внеаудиторная, в том числе	**4**	**4**
курсовая работа (проект) (КР/КП) (консультация, защита)		
текущий контроль, консультации по дисциплине	4	4
контактная работа на промежуточном контроле (КРА)		
2. Самостоятельная работа (СРС)	**54**	**54**
реферат/эссе (подготовка)		
расчётно-графическая работа (РГР) (подготовка)		
контрольная работа		
курсовая работа/проект (КР/КП) (подготовка)		
самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиум и т.д.)	36	36
Подготовка к экзамену (контроль)*		
Подготовка к зачету / зачету с оценкой (контроль)	18	18

4.2 Содержание дисциплины, структурированное по разделам, темам

Таблица 4.2 – Содержание дисциплины, структурированное по темам, для студентов очной формы обучения

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	**Наименование разделов, тем**	**Виды учебной работы (час)**				**Вид СРС**
		Контактная работа			**Самостоятельная работа студентов**	
		Лекции	**Лабораторные работы**	**Практические занятия**		
1	**2**	**3**	**4**	**5**	**6**	**7**
3 семестр						
ПКС-2 ИПКС-2.1 ПКС-3 ИПКС-3.2	**Раздел 1. Общие вопросы информационной безопасности**					
	Практическая работа №1. Теоретические основы методов защиты информационных систем			4	14	Подготовка к практическим занятиям [6.1.1], [6.1.2], [6.1.3]
	Практическая работа №2. Угрозы безопасности			4		
	Практическая работа №3. Методы защиты средств вычислительной техники			4		
	Итого по 1 разделу			**12**	**14**	

1	2	3	4	5	6	7
	Раздел 2. Методы защиты информации					
	Лабораторная работа №1. Реализация методов защиты информации		4		22	Подготовка к лабораторным и практическим занятиям [6.1.1] - [6.1.3], [6.2.1], [6.2.2], [6.3.1], [6.3.2]
	Практическая работа №4. Основы криптографии			4		
	Лабораторная работа №2. Асимметричные системы шифрования		8			
	Практическая работа №5. Способы шифрования			4		
	Лабораторная работа №3. Реализация способов шифрования		8			
	Практическая работа №6. Алгоритмы безопасности в компьютерных сетях			4		
	Лабораторная работа №4. Реализация алгоритмов безопасности в компьютерных сетях		4			
	Практическая работа №7. Модулярная арифметика			2		
	Итого по 2 разделу		**24**	**14**	**22**	
ИТОГО по дисциплине			**24**	**26**	**36**	

Используемые активные и интерактивные технологии приведены в таблице 4.3.

Таблица 4.3 - Используемые активные и интерактивные образовательные технологии

Вид занятий	Наименование используемых активных и интерактивных образовательных технологий
Практические занятия, лабораторные работы	Технология развития критического мышления Дискуссионные технологии Тестовые технологии Технологии работы в малых группах Технология коллективной работы Информационно-коммуникационные технологии

5. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1. Описание показателей и критериев контроля успеваемости, описание шкал оценивания

Критерии оценивания результатов обучения и процедуры оценивания компетенций, формируемых в рамках данной дисциплины, приводятся в табл. 5.4.

Оценочные процедуры в рамках текущего контроля проводятся преподавателем дисциплины. Лабораторные и практические занятия проводятся в форме выполнения индивидуальных заданий. При выполнении индивидуального лабораторного или практического задания преподавателем оценивается качество выполненного задания, срок его выполнения, качество и срок оформления отчета, ответы на вопросы преподавателя.

Описание показателей и критериев контроля успеваемости, описание шкал оценивания на этапе текущей аттестации представлены в табл. 5.1.

Промежуточная аттестация проводится в форме зачета с оценкой.

Описание показателей и критериев контроля успеваемости, описание шкал оценивания на этапе промежуточной аттестации представлены в табл. 5.2.

Возможно проведение итогового тестирования с использованием СДО MOODLE. Итоговое тестирование по дисциплине проводится в рамках самостоятельной работы. Итоговый тест содержит 20 тестовых вопросов (оценивание 60% показателей, время на проведение тестирования 30 минут).

В таблице 5.3 представлена шкала соответствия набранных баллов по промежуточной аттестации и оценок на зачете с оценкой по дисциплине.

Таблица 5.1 – Описание показателей и критериев контроля успеваемости, описание шкал оценивания на этапе текущей аттестации

Код и наименование компетенции	Код и наименование индикатора компетенции	Показатели контроля успеваемости	Критерии и шкала оценивания		Форма контроля
			0 баллов	1 баллов	
ПКС-2 Способен разрабатывать и исследовать математические модели, объектов, систем, процессов и технологий, предназначенных для проведения расчетов, анализа подготовки решений	ИПКС-2.1. Изучает методы математического моделирования, предназначенные для решения исследовательских задач, и современные математические и научные пакеты программ.	**Знать:** математические методы защиты информации и алгоритмы оценивания эффективности средств защиты информации	Теоретический материал не изучен или изучен частично.	Теоретический материал изучен.	Контроль участия в дискуссиях на занятиях
		Уметь: самостоятельно осваивать новые математические методы защиты информации	Лабораторные и практические задания не выполнены или выполнены частично.	Лабораторные и практические задания выполнены полностью.	Контроль выполнения лабораторных и практических заданий (см. табл. 4.2)
		Владеть: навыками применения математических методов защиты информации и оценивания эффективности применения их в прикладных задачах	Лабораторные и практические задания выполнены некачественно и/или не в срок.	Лабораторные и практические задания выполнены качественно и в срок.	Контроль выполнения лабораторных и практических заданий (см. табл. 4.2)
ПКС-3 Способен разрабатывать наукоемкое программное обеспечение работы конкретного предприятия	ИПКС-3.2. Проектирует и разрабатывает программные комплексы для решения задач профессиональной деятельности.	**Знать:** современные алгоритмы реализации методов и способов защиты информации	Теоретический материал не изучен или изучен частично.	Теоретический материал изучен.	Контроль участия в дискуссиях на занятиях
		Уметь: учитывать требования стандартов при разработке алгоритмов защиты информации	Лабораторные и практические задания не выполнены или выполнены частично.	Лабораторные и практические задания выполнены полностью.	Контроль выполнения лабораторных и практических заданий (см. табл. 4.2)
		Владеть: методами обеспечения защищенности компьютерных систем от вредоносных программно-технических и информационных воздействий	Лабораторные и практические задания выполнены некачественно и/или не в срок.	Лабораторные и практические задания выполнены качественно и в срок.	Контроль выполнения лабораторных и практических заданий (см. табл. 4.2)

Таблица 5.2 – Описание показателей и критериев контроля успеваемости, описание шкал оценивания на этапе промежуточной аттестации (зачет с оценкой)

Код и наименование компетенции	Код и наименование индикатора компетенции	Показатели контроля успеваемости	Критерии и шкала оценивания			Форма контроля
			0 баллов	1 балл	2 балла	
ПКС-2 Способен разрабатывать и исследовать математические модели, объектов, систем, процессов и технологий, предназначенных для проведения расчетов, анализа подготовки решений	ИПКС-2.1. Изучает методы математического моделирования, предназначенные для решения исследовательских задач, и современные математические и научные пакеты программ.	**Знать:** математические методы защиты информации и алгоритмы оценивания эффективности средств защиты информации	Ответ на вопрос отсутствует	Представлен не полный ответ на вопрос	Представлен развернутый ответ на вопрос	Ответ на теоретический вопрос билета
			Ответ на вопрос отсутствует	Представлен не полный ответ на вопрос	Представлен развернутый ответ на вопрос	Ответы на дополнительные вопросы
		Уметь: самостоятельно осваивать новые математические методы защиты информации **Владеть:** навыками применения математических методов защиты информации и оценивания эффективности применения их в прикладных задачах	Задание не решено	Задание решено с ошибками	Задание решено верно	Решение задач билета
ПКС-3 Способен разрабатывать наукоемкое программное обеспечение работы конкретного предприятия	ИПКС-3.2. Проектирует и разрабатывает программные комплексы для решения задач профессиональной деятельности.	**Знать:** современные алгоритмы реализации методов и способов защиты информации	Ответ на вопрос отсутствует	Представлен не полный ответ на вопрос	Представлен развернутый ответ на вопрос	Ответ на теоретический вопрос билета
			Ответ на вопрос отсутствует	Представлен не полный ответ на вопрос	Представлен развернутый ответ на вопрос	Ответы на дополнительные вопросы
		Уметь: учитывать требования стандартов при разработке алгоритмов защиты информации **Владеть:** методами обеспечения защищенности компьютерных систем от вредоносных программно-технических и информационных воздействий	Задание не решено	Задание решено с ошибками	Задание решено верно	Решение задач билета

Таблица 5.3 – Соответствие набранных баллов и оценки за промежуточную аттестацию

Баллы за текущую успеваемость*	Баллы за промежуточную аттестацию		Оценка
	Суммарное количество баллов**	Баллы за решение задач**	
0	0-1	0-1	«неудовлетворительно»
1	1	1	«удовлетворительно»
1	1-2	1-2	«хорошо»
1	2	2	«отлично»

**) количество баллов рассчитывается в соответствии с таблицей 5.1.*
***) количество баллов рассчитывается в соответствии с таблицей 5.2.*

5.2. Оценочные средства для контроля освоения дисциплины

5.2.1 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности в ходе текущего контроля успеваемости

Типовые задания к практическим занятиям

Практическая работа №3. Методы защиты средств вычислительной техники

Задание: Построить систему шифрования Диффи и Хеллмана для a=(количество согласных букв в фамилии студента), p больше или равно количеству всех букв в фамилии. Подобрать a и p самостоятельно методом проб и ошибок, выбрать два секретных числа X_i и X_j и для связи пользователей сети i и j вычислить числа Z_{ij} и $Z_{ji.}$

Практическая работа №4. Основы криптографии

Задание: Построить двухключевую систему с использованием алгоритма RSA и выполнить в ней операцию шифрования и дешифрования трех первых букв фамилии студента (при количестве букв меньше 3, недостающие буквы берутся из имени). Пара простых чисел P и Q выбирается из диапазона ближайших к количеству букв в фамилии и имени студента.

Типовые задания для лабораторных работ

Лабораторная работа №1. Реализация методов защиты информации

Задание: Подобрать хэш-функции h (T) и используя секретный ключ E и зашифрованное сообщение (три буквы) вычислить m=h(T) и $S=(m^E)$ mod N. Далее, пользуясь открытым ключом Д вычислить m из соотношения (S^D)=m mod N и убедиться в его совпадении с m владельца секретного ключа. В конечном виде передаваемое m<n).

Лабораторная работа №3. Реализация способов шифрования

Задание: Проверить штрих-код любого предприятия. Предложить скрытую часть (пломбируемую или защищенную краской), например, какую-то функцию от серийного номера изделия m=h(T), RSA – кодирование № передаваемое в двоичной форме для гамирования серийного номера изделия. В этом случае передающая и принимающая стороны знают начальную строку и позицию цифры в ней, с которой начинать отсчет.

5.2.2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта в ходе промежуточной аттестации по дисциплине

Форма проведения промежуточной аттестации по дисциплине: зачет с оценкой.

Возможно проведение промежуточной аттестации в устно-письменной форме по вопросам и задачам или в форме компьютерного тестирования в системе MOODLE.

Перечень вопросов и заданий для подготовки к зачету (ПКС-2 ИПКС-2.1, ПКС-3 ИПКС-3.2):

1. Понятие информационной безопасности.
2. Физические методы защиты информации.
3. Организационно-правовые методы информации.
4. Технические средства защиты.
5. Угрозы информационной безопасности.
6. Классификация криптографических методов защиты информации.
7. Операции модульной арифметики.
8. Малая теорема Ферма.
9. Функция Эйлера.
10. Алгоритм RSA.
11. Расширенный алгоритм Евклида.
12. Алгоритм быстрого возведения в степень по модулю.
13. Генерация простых чисел. Решето Эратосфена.
14. Метод пробных делений.
15. Решето Аткина.
16. Тест Поклингтона.
17. Тест простоты Миллера–Рабина.
18. Вероятностный тест простоты Соловея–Штрассена.
19. Полиномиальный критерий простоты AKS.
20. Китайская теорема об остатках.
21. Метод Ферма.
22. Метод Полларда.
23. Метод Вильямса.
24. Односторонние функции.
25. Алгоритм создания электронной цифровой подписи.
26. Эллиптические кривые в проективных координатах.
27. Эллиптические кривые в якобиановых проективных координатах.
28. Алгоритм факторизации Ленстры ECF.

29. Рекордные разложения метода ECFM.

30. Кривые Эдвардса.

31. Вычисление кратного точки ЭК с помощью MOV–алгоритма.

32. Дивизоры.

33. Алгоритм Миллера вычисления функции Вейля.

34. Протокол Диффи-Хеллмана для трех участников.

35. Шифрование на основе идентификационных данных пользователей.

Итоговый тест для проведения промежуточной аттестации (ОПК-3, ИОПК-3.3):

Итоговый тест для проведения промежуточной аттестации обучающихся сформирован в системе MOODLE и находятся в свободном доступе на странице курса «Математические методы защиты информации» по адресу: https://sdo.api.nntu.ru/course.

Регламент проведения промежуточной аттестации в форме тестирования в MOODLE

Кол-во заданий в банке вопросов	Кол-во заданий, предъявляемых студенту	Время на тестирование, мин.
81	20	30

5.3. Процедура оценивания результатов обучения по дисциплине

Процедура оценивания формируемых в рамках дисциплины компетенций (элементов компетенций) состоит из следующих этапов:

1. Текущий контроль (описание показателей и критериев контроля успеваемости, описание шкал оценивания на этапе текущей аттестации представлены в табл. 5.1, задания в п. 5.2.1).

2. Промежуточная аттестация (описание показателей и критериев контроля успеваемости, описание шкал оценивания на этапе промежуточной аттестации представлены в табл. 5.2, задания в п. 5.2.2).

Для всего перечня формируемых компетенций (элементов компетенций) дисциплины приводится процедура оценки результатов обучения (табл. 5.4).

Таблицы 5.4 – Процедура, критерии и методы оценивания результатов обучения

Планируемые результаты обучения	Критерии оценивания результатов				Методы оценивания
	1 критерий – отсутствие усвоения «неудовлетворительно»	2 критерий – не полное усвоение «удовлетворительно»	3 критерий – хорошее усвоение «хорошо»	4 критерий – отличное усвоение «отлично»	
ПКС-2 ИПКС-2.1					
Знать: математические методы защиты информации и алгоритмы оценивания эффективности средств защиты информации	Отсутствие усвоения знаний	Недостаточно уверенно понимает и может объяснять полученные знания	На достаточно высоком уровне понимает и может объяснять полученные знания	Отлично понимает и может объяснять полученные знания, демонстрирует самостоятельную познавательную деятельность	Участие в обсуждении дискуссионных материалов на занятиях Промежуточная аттестация или тестирование
Уметь: самостоятельно осваивать новые математические методы защиты информации	Не демонстрирует умения	Не уверенно демонстрирует умения	Достаточно уверенно демонстрирует умения	Отлично демонстрирует умения	Выполнение лабораторных и практических работ Промежуточная аттестация или тестирование
Владеть: навыками применения математических методов защиты информации и оценивания эффективности применения их в прикладных задачах	Не демонстрирует навыки	Не уверенно демонстрирует навыки	Достаточно уверенно демонстрирует навыки	Отлично демонстрирует самостоятельные навыки	Выполнение лабораторных и практических работ Промежуточная аттестация или тестирование
ПКС-3 ИПКС-3.2					
Знать: современные алгоритмы реализации методов и способов защиты информации	Отсутствие усвоения знаний	Недостаточно уверенно понимает и может объяснять полученные знания	На достаточно высоком уровне понимает и может объяснять полученные знания	Отлично понимает и может объяснять полученные знания, демонстрирует самостоятельную познавательную деятельность	Участие в обсуждении дискуссионных материалов на занятиях Промежуточная аттестация или тестирование
Уметь: учитывать требования стандартов при разработке алгоритмов защиты информации	Не демонстрирует умения	Не уверенно демонстрирует умения	Достаточно уверенно демонстрирует умения	Отлично демонстрирует умения	Выполнение лабораторных и практических работ Промежуточная аттестация или тестирование
Владеть: методами обеспечения защищенности компьютерных систем от вредоносных программно-технических и информационных воздействий	Не демонстрирует навыки	Не уверенно демонстрирует навыки	Достаточно уверенно демонстрирует навыки	Отлично демонстрирует самостоятельные навыки	Выполнение лабораторных и практических работ Промежуточная аттестация или тестирование

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Основная литература

6.1.1 Методы и средства инженерно-технической защиты информации : учебное пособие / В. И. Аверченков, М. Ю. Рытов, А. В. Кувыклин, Т. Р. Гайнулин. — Брянск : Брянский государственный технический университет, 2012. — 187 c. — ISBN 5-89838-357-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/7000.html. — Режим доступа: для авторизир. пользователей

6.1.2 Бескид, П. П. Криптографические методы защиты информации. Часть 1. Основы криптографии : учебное пособие / П. П. Бескид, Т. М. Тагарникова. — Санкт-Петербург : Российский государственный гидрометеорологический университет, 2010. — 95 c. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/17925.html. — Режим доступа: для авторизир. пользователей

6.1.3 Бескид, П. П. Криптографические методы защиты информации. Часть 2. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации : учебное пособие / П. П. Бескид, Т. М. Тагарникова. — Санкт-Петербург : Российский государственный гидрометеорологический университет, 2010. — 104 c. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/17926.html. — Режим доступа: для авторизир. пользователей

6.2 Дополнительная литература

6.2.1 Бурняшов, Б. А. Меры защиты информации на уровне пользователя информационно-технологическими средствами : методические указания к самостоятельной работе студентов. Учебно-методическое пособие / Б. А. Бурняшов. — Саратов : Вузовское образование, 2014. — 55 c. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/23077.html. — Режим доступа: для авторизир. пользователей

6.2.2 Алешников, С. И. Математические методы защиты информации. Часть 4. Вычислительный практикум по эллиптическим кривым и криптографии на эллиптических кривых : практическое пособие / С. И. Алешников, Ю. Ф. Болтнев. — Калининград : Балтийский федеральный университет им. Иммануила Канта, 2007. — 58 c. — ISBN 978-5-88874-803-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/23795.html. — Режим доступа: для авторизир. пользователей

6.3 Методические указания, рекомендации и другие материалы к занятиям

6.3.1 Методические рекомендации для практических работ по освоению дисциплины «Математические методы защиты информации». Рекомендованы заседанием кафедры «Прикладная математика» АПИ НГТУ, протокол №3 от 29.04.2021 г.

6.3.2 Методические рекомендации для лабораторных работ по освоению дисциплины «Математические методы защиты информации». Рекомендованы заседанием кафедры «Прикладная математика» АПИ НГТУ, протокол №3 от 29.04.2021 г.

7. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

7.1 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля), включая электронные библиотечные и информационно-справочные системы

7.1.1 Электронно-библиотечная система издательства «IPRbooks». Режим доступа: www.iprbookshop.ru.

7.2.1 Электронно-библиотечная система издательства «Лань». Режим доступа: https://e.lanbook.com

7.2 Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства необходимого для освоения дисциплины

7.2.2 Microsoft Windows
7.2.3 Microsoft Office
7.2.4 Microsoft Visual Studio

8. ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОВЗ

В таблице 8.1 указан перечень образовательных ресурсов, имеющих формы, адаптированные к ограничениям здоровья, а также сведения о наличии специальных технических средств обучения коллективного и индивидуального пользования.

Таблица 8.1 – Образовательные ресурсы для инвалидов и лиц с ОВЗ

Перечень образовательных ресурсов, приспособленных для использования инвалидами и лицами с ОВЗ	Сведения о наличии специальных технических средств обучения коллективного и индивидуального пользования
ЭБС «IPRbooks»	Специальное мобильное приложение **IPR BOOKS WV-Reader**
ЭБС «Лань»	Синтезатор речи, который воспроизводит тексты книг и меню навигации

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ, НЕОБХОДИМОЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Учебные аудитории для проведения занятий по дисциплине (модулю), оснащены оборудованием и техническими средствами обучения.

В таблице 9.1 перечислены:

- учебные аудитории для проведения учебных занятий, оснащенные оборудованием и техническими средствами обучения;

- помещения для самостоятельной работы обучающихся, которые оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду АПИ НГТУ.

Таблица 9.1 – Оснащенность аудиторий и помещений для проведения занятий и самостоятельной работы студентов по дисциплине (модулю)

Наименование аудиторий и помещений для проведения занятий и самостоятельной работы	Оснащенность аудиторий и помещений для проведения занятий и самостоятельной работы
206 – Учебная лаборатория математического моделирования г. Арзамас, ул. Калинина, дом 19	Компьютеров конфигурация 2 – 11 шт. Рабочих мест студентов – 20 шт. Доска аудиторная маркерная – 1 шт.
316 - Кабинет самоподготовки студентов г. Арзамас, ул. Калинина, дом 19	рабочих мест студента – 26 шт; ПК, с выходом на телевизор LG - 1 шт. ПК с подключением к интернету -5шт.

10. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ОБУЧАЮЩИМСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

10.1 Общие методические рекомендации для обучающихся по освоению дисциплины, образовательные технологии

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

Контактная работа проводится в аудиторной и внеаудиторной форме, а также в электронной информационно-образовательной среде института (далее – ЭИОС). В случае проведения части контактной работы по дисциплине в ЭИОС (в соответствии с расписанием учебных занятий), трудоемкость контактной работа в ЭИОС эквивалентна аудиторной работе.

При преподавании дисциплины используются современные образовательные технологии, позволяющие повысить активность студентов при освоении материала курса и предоставить им возможность эффективно реализовать часы самостоятельной работы.

Весь материал курса находится в свободном доступе в СДО MOODLE на странице курса по адресу: https://sdo.api.nntu.ru/course и могут быть проработаны студентами в ходе самостоятельной работы. Это дает возможность обсудить материал со студентами, активировать их деятельность при освоении материала.

На лабораторных и практических занятиях реализуются интерактивные технологии, приветствуются вопросы и обсуждения, используется личностно-ориентированный подход, дискуссионные технологии, технологии работы в малых группах, что позволяет студентам проявить себя, получить навыки самостоятельного изучения материала, выровнять уровень знаний в группе.

Все вопросы, возникшие при самостоятельной работе над домашним заданием, подробно разбираются на практических и лабораторных занятиях. Проводятся индивидуальные и групповые консультации с использованием, как встреч со студентами, так и современных информационных технологий, таких как форум, чат, внутренняя электронная почта СДО MOODLE.

Инициируется активность студентов, поощряется задание любых вопросов по материалу, практикуется индивидуальный ответ на вопросы студента.

Для оценки знаний, умений и уровня сформированности компетенции в процессе текущего контроля применяется система контроля и оценки успеваемости студентов, представленная в табл. 5.1. Промежуточная аттестация проводится в форме зачета с использованием системы контроля и оценки успеваемости студентов, представленной в табл. 5.2.

10.2 Методические указания по освоению дисциплины на лабораторных работах

Подготовку к каждой лабораторной работе студент должен начать с ознакомления с планом занятия, который отражает содержание предложенной темы. Каждая выполненная работа с оформленным отчетом и подлежит защите у преподавателя.

При оценивании лабораторных работ учитывается следующее:

- качество выполнения экспериментально-практической части работы и степень соответствия результатов работы заданным требованиям;
- качество оформления отчета по работе;
- качество устных ответов на контрольные вопросы при защите работы.

10.3 Методические указания по освоению дисциплины на практических занятиях

Практические занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы. Основной формой проведения практических занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение задач и разбор примеров в аудиторных условиях.

Практические занятия обеспечивают:

- проверку и уточнение знаний, полученных на лекциях;
- развитие умений и навыков дискуссионного обсуждения вопросов по учебному материалу дисциплины, выработки собственной позиции по актуальным вопросам (проблемам);
- подведение итогов занятий (результаты тестирования, готовность отчетов по практическим занятиям, готовность домашних заданий, выполненных в ходе самостоятельной работы).

10.4 Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обеспечивает подготовку обучающегося к аудиторным занятиям и мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине. Результаты этой подготовки проявляются в активности обучающегося на занятиях и в качестве выполненных практических заданий и других форм текущего контроля.

В процессе самостоятельной работы рекомендуется проработка материалов лекций по каждой пройденной теме, а также изучение основной учебной и справочно-библиографической литературы, представленной в разделе 6.

Для выполнения самостоятельной работы при изучении дисциплины студенты могут использовать специализированные аудитории (см. табл. 9.1), оборудование которых обеспечивает доступ через «Интернет» к электронной информационно-образовательной среде института и электронной библиотечной системе, где располагаются учебные и учебно-методические материалы, которые могут быть использованы для самостоятельной работы.

10.5 Методические указания по обеспечению образовательного процесса

1. Методические рекомендации по организации аудиторной работы. Приняты Учебно-методическим советом НГТУ им. Р.Е. Алексеева, протокол № 2 от 22 апреля 2013 г. Электронный адрес:https://www.nntu.ru/frontend/web/ngtu/files/org_structura/upravleniya/umu/docs/metod_docs_ngtu/metod_rekom_auditorii.PDF.

2. Методические рекомендации по организации и планированию самостоятельной работы студентов по дисциплине. Приняты Учебно-методическим советом НГТУ им. Р.Е. Алексеева, протокол № 2 от 22 апреля 2013 г. Электронный адрес: https://www.nntu.ru/frontend/web/ngtu/files/org_structura/upravleniya/umu/docs/metod_docs_ngtu/metod_rekom_srs.PDF.

3. Учебное пособие «Проведение занятий с применением интерактивных форм и методов обучения», Ермакова Т.И., Ивашкин Е.Г., 2013 г. Электронный адрес: https://www.nntu.ru/frontend/web/ngtu/files/org_structura/upravleniya/umu/docs/metod_docs_ngtu/provedenie-zanyatij-s-primeneniem-interakt.pdf.

4. Учебное пособие «Организация аудиторной работы в образовательных организациях высшего образования», Ивашкин Е.Г., Жукова Л.П., 2014 г. Электронный адрес: https://www.nntu.ru/frontend/web/ngtu/files/org_structura/upravleniya/umu/docs/metod_docs_ngtu/organizaciya-auditornoj-raboty.pdf.

Дополнения и изменения в рабочей программе дисциплины
на 20____/20____ уч. г.

УТВЕРЖДАЮ:
Директор института:
_____ Глебов В.В.
«____»_____ 20___ г.

В рабочую программу вносятся следующие изменения:
1)
2)
или делается отметка о нецелесообразности внесения каких-либо изменений на данный учебный год

Рабочая программа пересмотрена на заседании кафедры, протокол от _____№ ____
Заведующий кафедрой _____ _____
(подпись) *(ФИО)*

Утверждено УМК АПИ НГТУ, протокол от _____№ _____

Зам. директора по УР _____Шурыгин А.Ю.
(подпись)

Согласовано:

Начальник УО _____Мельникова О.Ю.
(подпись)

(в случае, если изменения касаются литературы):

Заведующая отделом библиотеки _____Старостина О.Н.
(подпись)