Министерство науки и высшего образования РФ
Федеральное государственное автономное образовательное учреждение высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.О.08 Прикладные вопросы теории чисел

наименование дисциплины (модуля) в соответствии с учебным планом

Направление подготовки / специальность

01.04.01 Математика

Направленность (профиль)

01.04.01.02 Алгебра, логика и дискретная математика

Форма обучения очная

Год набора 2023

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Программу составили

Кандидат физико-математических наук, Доцент, Жданов Олег Николаевич;андидат физико-математических наук, Доент, Моисеенкова Татьяна Владимировна

должность, инициалы, фамилия

1 Цели и задачи изучения дисциплины

1.1 Цель преподавания дисциплины

Целью учебной дисциплины «Прикладные вопросы теории чисел» является формирование мировоззрения, основанного на важнейших результатах теории чисел, полученных выдающимися предшественниками.

1.2 Задачи изучения дисциплины

Задачами дисциплины являются освоение и творческое осмысление результатов теории чисел и наработка умения применять результаты в прикладных задачах, в частности, в такой актуальной области, как защита информации.

1.3 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Код и наименование индикатора достижения компетенции	Запланированные результаты обучения по дисциплине
ОПК-1: Способен формулировать и решать актуальные и значимые проблемы математики	
ОПК-1.1: Использует фундаментальные математические знания в своей профессиональной деятельности	основные понятия и фундаментальные результаты теории чисел применять результаты теории чисел в прикладных задачах навыками работы с теоретико-числовыми конструкциями
ОПК-1.2: Формулирует математические постановки задач	основы математического моделирования формулировать математические задачи умением формулировать математические задачи
ОПК-1.3: Решает актуальные и значимые проблем математики	фундаментальные результаты и нерешенные проблемы проводить исследования самостоятельно навыками исследовательской, творческой работы по самым современным и актуальным проблемам математики 21 столетия
ОПК-2: Способен строить и анализировать математические модели в современном естествознании, технике, экономике и управлении	
ОПК-2.1: Создает и исследует математические модели в естествознании, технике, экономике и управлении	математические модели современного естествознания строить математические модели навыками построения и глубокого, всестороннего анализа математических моделей на основе современной методологии научного познания

ОПК-2.2: Использует математическое моделирование в своей профессиональной деятельности	актуальные проблемы своей профессиональной деятельности применять моделирование в своей профессиональной деятельности навыками глубокого проникновения в суть профессиональных проблем и
	высокопрофессионально исследовать соответствующие модели

1.4 Особенности реализации дисциплины

Язык реализации дисциплины: Русский.

Дисциплина (модуль) реализуется без применения ЭО и ДОТ.

2. Объем дисциплины (модуля)

Вид учебной работы	Всего, зачетных единиц (акад.час)	е 1
Контактная работа с преподавателем:	**1,06 (38)**	
занятия лекционного типа	0,53 (19)	
практические занятия	0,53 (19)	
Самостоятельная работа обучающихся:	**1,94 (70)**	
курсовое проектирование (КП)	Нет	
курсовая работа (КР)	Нет	

3 Содержание дисциплины (модуля)

3.1 Разделы дисциплины и виды занятий (тематический план занятий)

№ п/п	Модули, темы (разделы) дисциплины	Контактная работа, ак. час.							
		Занятия лекционного типа		Занятия семинарского типа				Самостоятельная работа, ак. час.	
				Семинары и/или Практические занятия		Лабораторные работы и/или Практикумы			
		Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС	Всего	В том числе в ЭИОС
1. Введение в прикладные вопросы теории чисел									
	1. Из истории криптографии. История криптографии. Простейшие шифры и их свойства. Шифры замены и перестановки. Композиции шифров. Основные этапы становления криптографии как науки.	1							
	2.			1					
	3. Открытые сообщения и их характеристики. Виды информации, подлежащей закрытию, её модели и свойства. Частотные характеристики открытых сообщений. Критерии на открытый текст. Особенности нетекстовых сообщений.	1							
	4.			1					

5. Основные понятия криптографии. Модели шифров. Блочные и поточные шифры. Понятие криптосистемы. Ручные и машинные шифры. Ключевая система шифра. Основные требования к шифрам.	1							
6.			1					
7.							10	
2. Основные классы шифров и их свойства.								
1. Шифры перестановки. Разновидности шифров перестановки: маршрутные, вертикальные перестановки, решетки и лабиринты. Криптоанализ шифров перестановки.	1							
2.			1					
3. Шифры замены. Одноалфавитные и многоалфавитные замены. Вопросы криптоанализа простейших шифров замены. Стандартные алгоритмы криптографической защиты данных.	1							
4.			1					
5. Поточные цифры Табличное и модульное гаммирование. Случайные и псевдослучайные гаммы. Криптограммы, полученные при повторном использовании ключа. Анализ криптограмм, полученных применением неравновероятной гаммы.	1							
6.			1					
7.							20	
3. Надёжность шифров								

1. Теория К. Шеннона Теоретико-информационный подход к оценке криптостойкости шифров. Криптографическая стойкость шифров. Надежность ключей и сообщений. Совершенные шифры. Характеризация совершенных шифров с минимальным числом ключей. Безусловно стойкие и вычислительно стойкие шифры. Вопросы практической стойкости. Избыточность языка и расстояние единственности.	1							
2.			1					
3. Имитостойкость шифров. Имитация и подмена сообщения. Характеристики имитостойкости. Методы обеспечения имитостойкости шифров. Совершенная имитостойкость. Коды аутентификации.	1							
4.			1					
5. Помехоустойчивость шифров. Характеристики помехоустойчивости. Характеризация шифров, не размножающих искажений типа замены и пропуска букв.	1							
6.			1					
7.							10	
4. Принципы построения криптографических алгоритмов с симметричными и несимметричными ключами.								

1. Реализация криптографических алгоритмов. Принципы построения блочных шифров. Режимы работы блочных шифров. Основные способы реализации криптографических алгоритмов и требования, предъявляемые к ним. Различия между программными и аппаратными реализациями. Программные реализации шифров. Современные криптографические интерфейсы. Криптографические стандарты.	1							
2.			1					
3. Вопросы синтеза генераторов случайных и псевдослучайных последовательностей. Методы получения случайных и псевдослучайных последовательностей. Регистры сдвига с обратной связью. Линейный контурный метод. Мультиплексорные последовательности. Вопросы периодичности и распределения элементов в псевдослучайных последовательностях.	1							
4.			1					
5. Методы усложнения последовательностей псевдослучайных чисел. Связь между качеством последовательностей, полученных с помощью нелинейных регистров сдвига и характеристиками функции усложнения. Применение дискретных функций для усложнения последовательностей.	1							
6.			1					

7. Методы анализа криптографических алгоритмов. Понятие криптоатаки. Классификация криптоатак. Методы анализа криптографических алгоритмов перебор ключей, метод «встречи посередине», линеаризация уровней шифрования, бесключевые методы. Особенности криптоанализа блочных шифров. Основы разностного анализа блочных шифров.	1							
8.			1					
9. Системы шифрования с открытыми ключами. Понятие односторонней функции и односторонней функции с «лазейкой». Криптосистемы RSA и Эль-Гамаля. Проблемы факторизации целых чисел и логарифмирования в конечных полях. Шифрование на основе эллиптических кривых. Криптосистемы с открытым ключом, основанные на задаче об укладке рюкзака и линейных кодах. Преимущество асимметричных систем шифрования. Криптографические хеш-функции. Ха-рактеристики и алгоритмы выработки хэш-функций.	1							
10.			1					
11.							15	
5. Криптографические протоколы.								
1. Модели криптографического протокола. Понятие криптографического протокола. Основные примеры. Связь стойкости протокола со стойкостью базовой криптографической системы. Классификация криптографических протоколов.	1							
2.			1					

3. Электронная цифровая подпись Понятие электронной цифровой подписи. Стандарты электронной цифровой подписи. Действующий Стандарт РФ.	1							
4.			1					
5. Протоколы аутентификации Парольные системы и протоколы «рукопожатия». Взаимосвязь между протоколами аутентификации и цифровой подписи.	1							
6.			1					
7. Протоколы управления ключами Протоколы сертификации ключей. Протоколы предварительного распределения ключей. Протоколы выработки сеансовых ключей. Открытое распределение ключей Диффи-Хеллмана и его модификация. Вопросы организации сетей засекреченной связи.	1							
8.			1					
9. Протоколы с нулевым знанием. Доказательство с нулевым знанием. Разделение секрета. Протоколы подбрасывания монеты. Построение протоколов с нулевым знанием на основе NP-сложных задач. Проблемы и перспективы исследований в области современной криптографии. Нерешенные задачи. Итоги изучения курса.	1							
10.			1					
11.							15	
Всего	19		19				70	

4 Учебно-методическое обеспечение дисциплины

4.1 Печатные и электронные издания:

1. Нестеренко Ю.В., Аматов М.А. Теория чисел: учебник для вузов.; допущено УМО по классическому университетскому образованию(М.: Академия).
2. Ященко В. В. Введение в криптографию: учеб. пособие(Москва: МЦНМО-ЧеРо).
3. Шеннон К. Э., Добрушин Р. Л., Лупанов О. Б., Колмогоров А. Н. Работы по теории информации и кибернетике: [сборник](Москва: Издательство иностранной литературы).
4. Жданов О. Н. Методика выбора ключевой информации для алгоритма блочного шифрования: Монография(Москва: ООО "Научно-издательский центр ИНФРА-М").
5. Жельников В. Криптография от папируса до компьютера: научно-популярная литература(Москва: ABF).

4.2 Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства (программное обеспечение, на которое университет имеет лицензию, а также свободно распространяемое программное обеспечение):

1. Пакет Microsoft Office, ОС Windows XP/7/8/10, браузер Google Chrome/Opera/Mozilla Firefox, информационные справочные системы: google.com, yandex.ru и т.д.
2.
3.
4.

4.3 Интернет-ресурсы, включая профессиональные базы данных и информационные справочные системы:

1. Для самостоятельной работы у студентов должен быть доступ к электронному каталогу НБ СФУ.

5 Фонд оценочных средств

Оценочные средства находятся в приложении к рабочим программам дисциплин.

6 Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)

Для проведения занятий требуется мультимедиа класс: (проектор NEC NP216, системный блок, монитор, клавиатура, колонки Genius SP-F350), а так же лекционный мультимедийный класс, включающий проекционное оборудование (проектор EB-X02 Epson портативный, Screen Media проекционный экран, мультимедийный компьютер, колонки).

Парк ЭВМ должен составлять 60 единиц классом не ниже Pentium IV. Необходимо, чтобы локальная компьютерная сеть, объединяющая все ЭВМ филиала имела выход в сеть Internet.

Освоение дисциплины инвалидами и лицами с ограниченными возможностями здоровья, в зависимости от нозологий, осуществляется с использованием средств обучения общего и специального назначения.