МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования «Горно-Алтайский государственный университет»
(ФГБОУ ВО ГАГУ, ГАГУ, Горно-Алтайский государственный университет)

Математические основы криптографии

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **кафедра математики, физики и информатики**

Учебный план 02.03.01_2021_621.plx
02.03.01 Математика и компьютерные науки
Математическое и программное обеспечение компьютерных сетей

Квалификация **бакалавр**

Форма обучения **очная**

Общая трудоемкость **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
аудиторные занятия 36
самостоятельная работа 62,1
часов на контроль 8,85

Виды контроля в семестрах:
зачеты 6

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**6 (3.2)**		Итого	
Недель	15 3/6			
Вид занятий	УП	РП	УП	РП
Лекции	18	18	18	18
Лабораторные	18	18	18	18
Консультации (для студента)	0,9	0,9	0,9	0,9
Контроль самостоятельной работы при проведении аттестации	0,15	0,15	0,15	0,15
В том числе инт.	18	18	18	18
Итого ауд.	36	36	36	36
Контактная работа	37,05	37,05	37,05	37,05
Сам. работа	62,1	62,1	62,1	62,1
Часы на контроль	8,85	8,85	8,85	8,85
Итого	108	108	108	108

Программу составил(и):
кандидат физико-математических наук, доцент, Кайгородов Евгений Владимирович _____

Рабочая программа дисциплины
Математические основы криптографии

разработана в соответствии с ФГОС:
Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 02.03.01 Математика и компьютерные науки (приказ Минобрнауки России от 23.08.2017 г. № 807)

составлена на основании учебного плана:
02.03.01 Математика и компьютерные науки
утвержденного учёным советом вуза от 10.06.2021 протокол № 7.

Рабочая программа утверждена на заседании кафедры
кафедра математики, физики и информатики

Протокол от 22.06.2021 протокол № 10

И.о. зав. кафедрой Часовских Николай Сергеевич

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2023-2024 учебном году на заседании кафедры
кафедра математики, физики и информатики

Протокол от 8 июня 2023 г. № 11
И. о. зав. кафедрой: Богданова Рада Александровна

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	*Цели:* изложение основополагающих принципов защиты информации с помощью криптографических методов и примеров реализации этих методов на практике; изучение математических основ криптографии, истории развития криптографии, включая современные тенденции, основных алгоритмов шифрования и криптографических протоколов обмена информацией.
1.2	*Задачи:* изучение основных арифметических и алгебраических основ криптографии; изучение криптографических алгоритмов; знакомство с криптографическими методами современных криптосистем.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Математический анализ
2.1.2	Алгебра
2.1.3	Теория чисел
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
УК-1: Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач
ИД-1.УК-1: Анализирует задачу, выделяя ее базовые составляющие, осуществляет декомпозицию задачи
анализирует криптографические и теоретико-числовые задачи, выделяя их базовые составляющие, осуществляет декомпозицию задач;
ИД-2.УК-1: Находит и критически анализирует информацию, необходимую для решения поставленной задачи
находит и критически анализирует информацию, необходимую для решения поставленной криптографической или теоретико-числовой задачи;
ИД-3.УК-1: Рассматривает возможные варианты решения задачи, оценивая их достоинства и недостатки
рассматривает возможные варианты решения криптографических и теоретико-числовых задач, оценивая их достоинства и недостатки.
ОПК-1: Способен консультировать и использовать фундаментальные знания в области математического анализа, комплексного и функционального анализа алгебры, аналитической геометрии, дифференциальной геометрии и топологии, дифференциальных уравнений, дискретной математики и математической логики, теории вероятностей, математической статистики и случайных процессов, численных методов, теоретической механики в профессиональной деятельности
ИД-1.ОПК-1: Знает основные понятия, определения, свойства математических объектов, формулировки и методы доказательств математических утверждений
знать основные задачи и понятия криптографии;
ИД-2.ОПК-1: Умеет доказывать утверждения, решать задачи в области математических наук
уметь доказывать основные теоретико-числовые теоремы, пользоваться научно-технической литературой в области криптографии, применять отечественные и зарубежные стандарты в области криптографических методов компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
ИД-3.ОПК-1: Способен консультировать в области фундаментальной математики
владеть методикой построения, анализа и применения математических моделей для оценки степени защищенности информационной системы, качества использованных алгоритмов и технологий;
ОПК-4: Способен находить, анализировать, реализовывать программно и использовать на практике математические алгоритмы, в том числе с применением современных вычислительных систем
ИД-1.ОПК-4: Знает теоретические основы математических алгоритмов, особенности программной реализации математических алгоритмов, в том числе с применением современных вычислительных машин
знать принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах;
ИД-2.ОПК-4: Умеет находить, анализировать, программно реализовывать математические алгоритмы, в том числе с применением современных вычислительных машин
уметь использовать частотные характеристики открытых текстов для анализа простейших шифров замены и перестановки;
ИД-3.ОПК-4: Владеет навыками использования на практике математических алгоритмов, реализованных с применением современных вычислительных машин
владеть навыками использования типовых криптографических алгоритмов;

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)							
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература**	**Инте ракт.**	**Примечание**
	Раздел 1. Введение в криптографию						
1.1	Введение. История криптографии. Исторические шифры /Лек/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.УК-1 ИД-2.УК-1 ИД-3.УК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	1	проблемная лекция
1.2	Свойства информации. Ситуационные задачи на определение свойств информации, подлежащей криптографическому преобразованию. Исторические шифры и их криптоанализ. Компьютерная реализация и вскрытие шифров замены /Лаб/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.УК-1 ИД-2.УК-1 ИД-3.УК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	2	круглый стол
1.3	Введение. История криптографии. Исторические шифры /Ср/	6	11	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.УК-1 ИД-2.УК-1 ИД-3.УК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
	Раздел 2. Математическая формализация. Виды шифров						
2.1	Математическая модель шифра. Теория секретности Шеннона /Лек/	6	1	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.УК-1 ИД-2.УК-1 ИД-3.УК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	1	лекция с запланированными ошибками

2.2	Блочные шифры /Лек/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.УК-1 ИД-2.УК-1 ИД-3.УК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	2	проблемная лекция
2.3	Псевдослучайные последовательности и поточные шифры /Лек/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.УК-1 ИД-2.УК-1 ИД-3.УК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
2.4	Теория имитостойкости Симмонса и криптографические хэш-функции /Лек/	6	1	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.УК-1 ИД-2.УК-1 ИД-3.УК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
2.5	Асимметричные (с открытым ключом) шифры /Лек/	6	4	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.УК-1 ИД-2.УК-1 ИД-3.УК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	2	проблемная лекция
2.6	Компьютерная реализация и вскрытие шифров перестановки и гаммирования. Построение моделей шифров /Лаб/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.УК-1 ИД-2.УК-1 ИД-3.УК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	2	круглый стол

2.7	Вероятностные характеристики текстов. Определение избыточности текста, языка. Вероятностные характеристики простых шифров. Расчет параметров шифров. Расстояние единственности, определение количества ложных ключей /Лаб/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.УК-1 ИД-2.УК-1 ИД-3.УК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
2.8	Блочные шифры. ГОСТ 28147-89, IDEA и DES. Многочлены над Z2 и блочный шифр AES /Лаб/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.УК-1 ИД-2.УК-1 ИД-3.УК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	2	кластер
2.9	Псевдослучайные генераторы на основе РСЛОС. Оценка свойств гаммы шифра. Изучение современных поточных криптосистем /Лаб/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.УК-1 ИД-2.УК-1 ИД-3.УК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
2.10	Вычисление параметров имитостойкости, помехоустойчивости шифров. Построение криптографической хэш-функции на основе блочного шифра и исследование ее свойств методами математической статистики и теории информации /Лаб/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.УК-1 ИД-2.УК-1 ИД-3.УК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	2	кластер
2.11	Вычисления в Zn. Шифр с открытым ключом: RSA, Эль-Гамаля, Шамира, Диффи-Хэллмана, Рабина, Гольдвассер-Микали, Блюма-Гольдвассер, Меркла-Хэллмана. Генерация больших простых чисел для асимметричных криптосистем /Лаб/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.УК-1 ИД-2.УК-1 ИД-3.УК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	

2.12	Математическая модель шифра. Теория секретности Шеннона /Ср/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.УК-1 ИД-2.УК-1 ИД-3.УК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
2.13	Блочные шифры /Ср/	6	6,1	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.УК-1 ИД-2.УК-1 ИД-3.УК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
2.14	Псевдослучайные последовательности и поточные шифры /Ср/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.УК-1 ИД-2.УК-1 ИД-3.УК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
2.15	Теория имитостойкости Симмонса и криптографические хэш-функции /Ср/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.УК-1 ИД-2.УК-1 ИД-3.УК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
2.16	Асимметричные (с открытым ключом) шифры /Ср/	6	13	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.УК-1 ИД-2.УК-1 ИД-3.УК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
	Раздел 3. Электронная цифровая подпись						

3.1	Схемы цифровой подписи /Лек/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.УК-1 ИД-2.УК-1 ИД-3.УК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	2	проблемная лекция
3.2	Эллиптические кривые над конечным полем. Шифры и ЭЦП на их основе /Лек/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.УК-1 ИД-2.УК-1 ИД-3.УК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	2	лекция-визуализация
3.3	Реализация схемы ЭЦП: RSA, Эль-Гамаля и ее варианты, Фиата-Шамира, Онга-Шнорра-Шамира, Шнорра. Неотрицаемая подпись Шаума-ван-Антверпена. Эллиптические кривые над конечным полем. Преобразование криптосистемы над Zp в криптосистему на эллиптической кривой /Лаб/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.УК-1 ИД-2.УК-1 ИД-3.УК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
3.4	Схемы цифровой подписи /Ср/	6	11	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.УК-1 ИД-2.УК-1 ИД-3.УК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
3.5	Эллиптические кривые над конечным полем. Шифры и ЭЦП на их основе /Ср/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.УК-1 ИД-2.УК-1 ИД-3.УК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
	Раздел 4. Криптографические протоколы						

4.1	Введение в криптографические протоколы /Лек/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.УК-1 ИД-2.УК-1 ИД-3.УК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
4.2	Изучение примитивных протоколов. Изучение криптосистемы Kerberos /Лаб/	6	2	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.УК-1 ИД-2.УК-1 ИД-3.УК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
4.3	Введение в криптографические протоколы /Ср/	6	13	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.УК-1 ИД-2.УК-1 ИД-3.УК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
	Раздел 5. Консультации						
5.1	Консультация по дисциплине /Конс/	6	0,9	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.УК-1 ИД-2.УК-1 ИД-3.УК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	
	Раздел 6. Промежуточная аттестация (зачёт)						
6.1	Подготовка к зачёту /Зачёт/	6	8,85	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.УК-1 ИД-2.УК-1 ИД-3.УК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	

6.2	Контактная работа /КСРАтт/	6	0,15	ИД-1.ОПК-1 ИД-2.ОПК-1 ИД-3.ОПК-1 ИД-1.УК-1 ИД-2.УК-1 ИД-3.УК-1 ИД-1.ОПК-4 ИД-2.ОПК-4 ИД-3.ОПК-4	Л1.1 Л1.2Л2.1	0	

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Пояснительная записка

Фонд оценочных средств формируется отдельным документом в соответствии с Положением о фонде оценочных средств в Горно-Алтайском государственном университете

5.2. Оценочные средства для текущего контроля

5.3. Темы письменных работ (эссе, рефераты, курсовые работы и др.)

Темы сообщений и докладов

1. Концепция и основные направления обеспечения информационной безопасности. Правовая и техническая защита информации.
2. Защита информации от утечки по техническим каналам.
3. Компьютерная безопасность.
4. Шифрование данных симметричным алгоритмом.
5. Защита программ от несанкционированной эксплуатации за счет привязки к носителю информации.
6. Программирование изменений характеристик файла.

5.4. Оценочные средства для промежуточной аттестации

Контрольные вопросы к зачету

1. Основные понятия и определения криптографии.
2. Виды криптосистем. Задачи, решаемые методами криптографии.
3. Виды информации, подлежащие закрытию, их модели и свойства. Частотные характеристики открытых сообщений. Критерии на открытый текст. Особенности нетексто¬вых сообщений.
4. История криптографии. Основные этапы становления науки криптографии.
5. Классификация шифров замены. Шифр Цезаря. Шифр простой замены. Шифр Плейфера. Полибианский квадрат. Шифр Хилла. Шифр Виженера. Частотный анализ. Тест Казиски.
6. Классификация шифров перестановки. Примеры шифров перестановки и их криптоанализ.
7. Шифры гаммирования. Шифр Вернама. Подходы к его криптоанализу.
8. Композиции шифров. Enigma. Шифр Хейглина.
9. Математическая модель шифра.
10. Атаки и угрозы шифрам.
11. Блочные шифры и их ключевая система. Замены и перестановки.
12. Сеть Фейстеля. Шифры DES, ГОСТ 28147-89.
13. Шифр AES
14. Шифр IDEA.
15. Подходы к криптоанализу блочных шифров. Дифференциальный криптоанализ. Линейный криптоанализ.
16. Режимы шифрования.
17. Многократное шифрование. Композиция блочных шифров.
18. Совершенные шифры. Пример совершенного шифра.
19. Энтропийные характеристики шифров. Идеальные шифры.
20. Избыточность языка.
21. Оценка числа ложных ключей и расстояние единственности.
22. Безусловно стойкие и вычислительно стойкие шифры.
23. Псевдослучайные последовательности (ПСП). Характеристики генераторов ПСП (ПСГ). Требования к криптографическим ПСП. Примеры ПСГ и криптографических ПСГ.
24. Поточные шифры. Общая схема поточного шифра. Синхронные и самосинхронизирующиеся шифры.
25. Регистры сдвига с обратной линейной связью (РСЛОС).
26. ПСГ на основе РСЛОС.
27. Шифр A5.
28. Нелинейные регистры сдвига.
29. Шифр RC4.

30. Теория имитостойкости Симмонса. Имитация и подмена сообщения. Характеристики имитостойкости. Совершенная имитостойкость.
31. Коды аутентификации сообщений.
32. Защитные контрольные суммы.
33. Криптографические хэш-функции и требования к ним.
34. Подходы к проектированию хэш-функций.
35. Хэш-функции на основе блочного шифра.
36. Ключевые хэш-функции.
37. Понятие односторонней функции и односторонней функции с "лазейкой". Проблемы факторизации целых чисел и логарифмирования в конечных полях.
38. Криптосистема Диффи-Хэллмана. Пример.
39. Криптосистема RSA. Пример.
40. Криптосистема Эль-Гамаля. Пример.
41. Криптосистема Рабина. Пример.
42. Криптосистема Гольдвассер-Микали. Пример.
43. Криптосистема Блюма-Гольдвассер. Пример.
44. Рюкзачные шифры. Криптосистема Меркла-Хэллмана.
45. Понятие электронной цифровой подписи и требования к ней. Атаки и угрозы схемам ЭЦП.
46. Подпись RSA, Эль-Гамаля.
47. Подпись Фиата-Шамира.
48. Подпись Онга-Шнорра-Шамира.
49. Неотрицаемая подпись Шаума-ван-Антверпена.
50. Стандарты ЭЦП: DSS, ГОСТ Р 34.10-94.
51. Эллиптическая кривая над конечным полем. Операции на эллиптической кривой. Сумма точек. Кратная точка.
52. Проблема дискретного логарифмирования на эллиптической кривой. Переход от шифра (ЭЦП) в Zp к шифру (ЭЦП) на эллиптической кривой.
53. Шифр Эль-Гамаля на эллиптической кривой.
54. Стандарты ЭЦП на эллиптической кривой: ГОСТ Р 34.10-2001, ECDSA.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Эл. адрес
Л1.1	Тебуева Ф.Б., Антонов В.О.	Теоретико-числовые методы в криптографии: учебное пособие : электронный учебник	Ставрополь : Северо-Кавказский федеральный университет, 2017	http://www.iprbookshop.ru/75601.html
Л1.2	Басалова Г.В.	Основы криптографии: учебное пособие	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020	http://www.iprbookshop.ru/89455.html

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Эл. адрес
Л2.1	Кирпичников А.П., Хайбуллина З.М.	Криптографические методы защиты компьютерной информации: учебное пособие	Казань: Казанский национальный исследовательский технологический университет, 2016	http://www.iprbookshop.ru/79313.html

6.3.1 Перечень программного обеспечения

6.3.1.1	Adobe Reader
6.3.1.2	Dev-C++
6.3.1.3	Moodle
6.3.1.4	WinDjView
6.3.1.5	Яндекс.Браузер

6.3.1.6	Kaspersky Endpoint Security для бизнеса СТАНДАРТНЫЙ
6.3.1.7	MS Office
6.3.1.8	MS WINDOWS
6.3.1.9	NVDA
6.3.2 Перечень информационных справочных систем	
6.3.2.1	База данных «Электронная библиотека Горно-Алтайского государственного университета»
6.3.2.2	Электронно-библиотечная система IPRbooks

7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ		
	проблемная лекция	
	лекция-визуализация	
	кластер	
	лекция с запланированными ошибками	
	круглый стол	

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Номер аудитории	**Назначение**	**Основное оснащение**
206 Б1	Кабинет методики преподавания математики. Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Ученическая доска, интерактивная доска, экран,проектор, компьютер, посадочные места обучающихся (по количеству обучающихся), рабочее место преподавателя
102 Б1	Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Ученическая доска, мультимедиапроектор, экран, компьютер. Рабочее место преподавателя, посадочные места обучающихся (по количеству обучающихся), кафедра
200 Б1	Компьютерный класс. Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Помещение для самостоятельной работы	Рабочее место преподавателя. Посадочные места обучающихся (по количеству обучающихся), компьютеры с доступом к Интернет

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Методические указания по освоению дисциплин (модулей)

Лекции, с одной стороны – это одна из основных форм учебных занятий в высших учебных заведениях, представляющая собой систематическое, последовательное устное изложение преподавателем определенного раздела конкретной науки или учебной дисциплины, с другой – это особая форма самостоятельной работы с учебным материалом. Лекция не заменяет собой книгу, она только подталкивает к ней, раскрывая тему, проблему, выделяя главное, существенное, на что следует обратить внимание, указывает пути, которым нужно следовать, добиваясь глубокого понимания поставленной проблемы, а не общей картины.

Работа на лекции – это сложный процесс, который включает в себя такие элементы как слушание, осмысление и собственно конспектирование. Для того, чтобы лекция выполнила свое назначение, важно подготовиться к ней и ее записи еще до прихода преподавателя в аудиторию. Без этого дальнейшее восприятие лекции становится сложным. Лекция в университете рассчитана на подготовленную аудиторию. Преподаватель излагает любой вопрос, ориентируясь на те знания, которые должны быть у студентов, усвоивших материал всех предыдущих лекций.Важно научиться слушать преподавателя во время лекции, поддерживать непрерывное внимание к выступающему.

Однако, одного слушания недостаточно. Необходимо фиксировать, записывать тот поток информации, который сообщается во время лекции – научиться вести конспект лекции, где формулировались бы наиболее важные моменты, основные положения, излагаемые лектором. Для ведения конспекта лекции следует использовать тетрадь. Ведение конспекта на

листочках не рекомендуется, поскольку они не так удобны в использовании и часто теряются. При оформлении конспекта лекции необходимо оставлять поля, где студент может записать свои собственные мысли, возникающие параллельно с мыслями, высказанными лектором, а также вопросы, которые могут возникнуть в процессе слушания, чтобы получить на них ответы при самостоятельной проработке материала лекции, при изучении рекомендованной литературы или непосредственно у преподавателя в конце лекции. Составляя конспект лекции, следует оставлять значительный интервал между строчками. Это связано с тем, что иногда возникает необходимость вписать в первоначальный текст лекции одну или несколько строчек, имеющих принципиальное значение и почерпнутых из других источников. Расстояние между строками необходимо также для подчеркивания слов или целых групп слов (такое подчеркивание вызывается необходимостью привлечь внимание к данному месту в тексте при повторном чтении). Обычно подчеркивают определения, выводы.
Также важно полностью без всяких изменений вносить в тетрадь схемы, таблицы, чертежи и т.п., если они предполагаются в лекции. Для того, чтобы совместить механическую запись с почти дословным фиксированием наиболее важных положений, можно использовать системы условных сокращений. В первую очередь сокращаются длинные слова и те, что повторяются в речи лектора чаще всего. При этом само сокращение должно быть по возможности кратким.
Семинарские (практические) занятия Самостоятельная работа студентов по подготовке к семинарскому (практическому) занятию должна начинаться с ознакомления с планом семинарского (практического) занятия, который включает в себя вопросы, выносимые на обсуждение, рекомендации по подготовке к семинару (практическому занятию), рекомендуемую литературу к теме. Изучение материала следует начать с просмотра конспектов лекций. Восстановив в памяти материал, студент приводит в систему основные положения темы, вопросы темы, выделяя в ней главное и новое, на что обращалось внимание в лекции. Затем следует внимательно прочитать соответствующую главу учебника.
Для более углубленного изучения вопросов рекомендуется конспектирование основной и дополнительной литературы. Читая рекомендованную литературу, не стоит пассивно принимать к сведению все написанное, следует анализировать текст, думать над ним, этому способствуют записи по ходу чтения, которые превращают чтение в процесс. Записи могут вестись в различной форме: развернутых и простых планов, выписок (тезисов), аннотаций и конспектов.
Подобрав, отработав материал и усвоив его, студент должен начать непосредственную подготовку своего выступления на семинарском (практическом) занятии для чего следует продумать, как ответить на каждый вопрос темы.
По каждому вопросу плана занятий необходимо подготовиться к устному сообщению (5-10 мин.), быть готовым принять участие в обсуждении и дополнении докладов и сообщений (до 5 мин.).
Выступление на семинарском (практическом) занятии должно удовлетворять следующим требованиям: в нем излагаются теоретические подходы к рассматриваемому вопросу, дается анализ принципов, законов, понятий и категорий; теоретические положения подкрепляются фактами, примерами, выступление должно быть аргументированным.
Лабораторные работы являются основными видами учебных занятий, направленными на экспериментальное (практическое) подтверждение теоретических положений и формирование общепрофессиональных и профессиональных компетенций. Они составляют важную часть теоретической и профессиональной практической подготовки.
В процессе лабораторной работы как вида учебного занятия студенты выполняют одно или несколько заданий под руководством преподавателя в соответствии с изучаемым содержанием учебного материала.
При выполнении обучающимися лабораторных работ значимым компонентом становятся практические задания с использованием компьютерной техники, лабораторно - приборного оборудования и др. Выполнение студентами лабораторных работ проводится с целью: формирования умений, практического опыта (в соответствии с требованиями к результатам освоения дисциплины, и на основании перечня формируемых компетенций, установленными рабочей программой дисциплины), обобщения, систематизации, углубления, закрепления полученных теоретических знаний, совершенствования умений применять полученные знания на практике.
Состав заданий для лабораторной работы должен быть спланирован с расчетом, чтобы за отведенное время они могли быть выполнены качественно большинством студентов.
При планировании лабораторных работ следует учитывать, что в ходе выполнения заданий у студентов формируются умения и практический опыт работы с различными приборами, установками, лабораторным оборудованием, аппаратурой, программами и др., которые могут составлять часть профессиональной практической подготовки, а также исследовательские умения (наблюдать, сравнивать, анализировать, устанавливать зависимости, делать выводы и обобщения, самостоятельно вести исследование, оформлять результаты).
Выполнению лабораторных работ предшествует проверка знаний студентов - их теоретической готовности к выполнению задания.
Формы организации студентов при проведении лабораторных работ: фронтальная, групповая и индивидуальная. При фронтальной форме организации занятий все студенты выполняют одновременно одну и ту же работу. При групповой форме организации занятий одна и та же работа выполняется группами по 2 - 5 человек. При индивидуальной форме организации занятий каждый студент выполняет индивидуальное задание.
Текущий контроль учебных достижений по результатам выполнения лабораторных работ проводится в соответствии с системой оценивания (рейтинговой, накопительной и др.), а также формами и методами (как традиционными, так и инновационными, включая компьютерные технологии), указанными в рабочей программе дисциплины (модуля). Текущий контроль проводится в пределах учебного времени, отведенного рабочим учебным планом на освоение дисциплины, результаты заносятся в журнал учебных занятий.
Объем времени, отводимый на выполнение лабораторных работ, планируется в соответствии с учебным планом ОПОП.
Перечень лабораторных работ в РПД, а также количество часов на их проведение должны обеспечивать реализацию требований к знаниям, умениям и практическому опыту студента по дисциплине (модулю) соответствующей ОПОП.
Самостоятельная работа обучающихся– это планируемая учебная, учебно-исследовательская, научно-исследовательская работа, выполняемая во внеаудиторное время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.
Объем самостоятельной работы определяется учебным планом основной профессиональной образовательнойпрограммы (ОПОП), рабочей программой дисциплины (модуля).

Самостоятельная работа организуется и проводится с целью формирования компетенций, понимаемых как способность применять знания, умения и личностные качества для успешной практической деятельности, в том числе:
- формирования умений по поиску и использованию нормативной, правовой, справочной и специальной литературы, а также других источников информации;
- качественного освоения и систематизации полученных теоретических знаний, их углубления и расширения по применению на уровне межпредметных связей;
- формирования умения применять полученные знания на практике (в профессиональной деятельности) и закрепления практических умений обучающихся;
- развития познавательных способностей, формирования самостоятельности мышления обучающихся;
- совершенствования речевых способностей обучающихся;
- формирования необходимого уровня мотивации обучающихся к систематической работе для получения знаний, умений и владений в период учебного семестра, активности обучающихся, творческой инициативы, самостоятельности, ответственности и организованности;
- формирования способностей к саморазвитию (самопознанию, самоопределению, самообразованию, самосовершенствованию, самореализации и саморегуляции);
- развития научно-исследовательских навыков;
- развития навыков межличностных отношений.
К самостоятельной работе по дисциплине (модулю) относятся: проработка теоретического материала дисциплины (модуля);подготовка к семинарским и практическим занятиям, в т.ч. подготовка к текущему контролю успеваемости обучающихся(текущая аттестация); подготовка к лабораторным работам; подготовка к промежуточной аттестации (зачётам, экзаменам).
Виды, формы и объемы самостоятельной работы обучающихсяпри изучении дисциплины (модуля) определяются:
- содержанием компетенций, формируемых дисциплиной (модулем);
- спецификой дисциплины (модуля), применяемыми образовательными технологиями;
- трудоемкостью СР, предусмотренной учебным планом;
- уровнем высшего образования (бакалавриат, специалитет, магистратура, аспирантура), на котором реализуется ОПОП;
- степенью подготовленности обучающихся.
Курсовая работа является самостоятельным творческим письменным научным видом деятельности студента по разработке конкретной темы. Она отражает приобретенные студентом теоретические знания и практические навыки. Курсовая работа выполняется студентом самостоятельно под руководством преподавателя.
Курсовая работа, наряду с экзаменами и зачетами, является одной из форм контроля (аттестации), позволяющей определить степень подготовленности будущего специалиста. Курсовые работы защищаются студентами по окончании изучения указанных дисциплин, определенных учебным планом.
Оформление работы должно соответствовать требованиям. Объем курсовой работы: 25–30 страниц. Список литературы и Приложения в объем работы не входят. Курсовая работа должна содержать: титульный лист, содержание, введение, основную часть, заключение, список литературы, приложение (при необходимости). Курсовая работа подлежит рецензированию руководителем курсовой работы. Рецензия является официальным документом и прикладывается к курсовой работе.
Тематика курсовых работ разрабатывается в соответствии с учебным планом. Руководитель курсовой работы лишь помогает студенту определить основные направления работы, очертить её контуры, указывает те источники, на которые следует обратить главное внимание, разъясняет, где отыскать необходимые книги.
Составленный список источников научной информации, подлежащий изучению, следует показать руководителю курсовой работы.
Курсовая работа состоит из глав и параграфов. Вне зависимости от решаемых задач и выбранных подходов структура работы должна содержать: титульный лист, содержание, введение, основную часть; заключение; список литературы; приложение(я).
Во введении необходимо отразить: актуальность; объект; предмет; цель; задачи; методы исследования; структура работы.
Основную часть работы рекомендуется разделить на 2 главы, каждая из которых должна включать от двух до четырех параграфов.
Содержание глав и их структура зависит от темы и анализируемого материала.
Первая глава должна иметь обзорно–аналитический характер и, как правило, является теоретической.
Вторая глава по большей части раскрывает насколько это возможно предмет исследования. В ней приводятся практические данные по проблематике темы исследования.
Выводы оформляются в виде некоторого количества пронумерованных абзацев, что придает необходимую стройность изложению изученного материала. В них подводится итог проведённой работы, непосредственно выводы, вытекающие из всей работы и соответствующие выявленным проблемам, поставленным во введении задачам работы; указывается, с какими трудностями пришлось столкнуться в ходе исследования.
Правила написания и оформления курсовой работы регламентируются Положением о курсовой работе (проекте), утвержденным решением Ученого совета ФГБОУ ВО ГАГУ от 27 апреля 2017 г.