МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

УТВЕРЖДАЮ
Проректор по учебной работе

_____ С.Т. Князев
«___» _____ 2018 г.

РАБОЧАЯ ПРОГРАММА МОДУЛЯ
МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОГРАФИИ

Перечень сведений о рабочей программе модуля	**Учетные данные**
Модуль **Математические основы криптографии**	Код модуля **1117699** **Учебный план № 5347**
Образовательная программа **Компьютерная безопасность**	Код ОП **10.05.01/01.02**
Траектория образовательной программы	**Не предусмотрена**
Направление подготовки **Компьютерная безопасность**	Код направления и уровня подготовки **10.05.01**
Уровень подготовки **Специалитет**	
ФГОС ВО	Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО: **1 декабря 2016 г., № 1512**

Екатеринбург, 2018

Программа модуля составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Кафедра	Подпись
1	Ананичев Дмитрий Сергеевич	К. ф.-м. н., доцент	доцент	Кафедра алгебры и дискретной математики	

Руководитель модуля Д.С. Ананичев

Рекомендовано учебно-методическим советом института математики и компьютерных наук

Председатель учебно-методического совета А.Ю. Коврижных
Протокол № 12 от 15 декабря 2016 г.

Согласовано:

Дирекция образовательных программ Р.Х. Токарева

Руководитель образовательной программы (ОП), для которой реализуется модуль
В.А. Баранский

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ МАТЕМАТИЧЕСКИЕ ОСНОВЫ КРИПТОГРАФИИ

1.1. Объем модуля, 8 з.е.

1.2. Аннотация содержания модуля

Модуль состоит из трех дисциплин «Теория чисел», «Теория конечных полей» (вариативная часть ВУЗа) и «Теоретико-числовые методы в криптографии» (базовая часть). Цель изучения данных дисциплин — дать студентам фундаментальные знания о математических понятиях, конструкциях, алгоритмах и алгоритмических проблемах, на основе которых строятся современные технологии защиты информации.

2. СТРУКТУРА МОДУЛЯ И РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ ПО ДИСЦИПЛИНАМ

Наименования дисциплин с указанием, к какой части образовательной программы они относятся: базовой (Б), вариативной – по выбору вуза (ВВ), вариативной - по выбору студента (ВС).		Семестр изучения	Объем времени, отведенный на освоение дисциплин модуля							
			Аудиторные занятия, час.				Самостоятельная работа, включая все виды текущей аттестации, час.	Промежуточная аттестация (зачет, экзамен), час.	Всего по дисциплине	
			Лекции	Практические занятия	Лабораторные работы	Всего			Час.	Зач. ед.
1.	**(Б)** Теоретико-числовые методы в криптографии	5	34	17		51	75	18(Э)	144	4
2.	**(ВВ)** Теория чисел	4	34			34	34	4(З)	72	2
3.	**(ВВ)** Теория конечных полей	4	34			34	34	4(З)	72	2
Всего на освоение модуля			**102**	**17**		**119**	**143**	**26**	**288**	**8**

3. ПОСЛЕДОВАТЕЛЬНОСТЬ ОСВОЕНИЯ ДИСЦИПЛИН В МОДУЛЕ

3.1.	**Пререквизиты и постреквизиты в модуле**	Теория чисел, Теоретико-числовые методы в криптографии
3.2.	**Кореквизиты**	Теория чисел, Теория конечных полей

4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ МОДУЛЯ

4.1. Планируемые результаты освоения модуля и составляющие их компетенции

Коды ОП, для которых реализуется модуль	Планируемые в ОХОП результаты обучения -РО, которые формируются при освоении модуля	Компетенции в соответствии с ФГОС ВО, а также дополнительные из ОХОП, формируемые при освоении модуля
10.05.01/01.02	РО2. Способность применять основополагающие принципы и современные достижения физико-математических наук,	ПК-4, способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем;

	математического описания и построения компьютерных систем, а также современные информационные технологии в разработке технологических решений с использованием программного кода.	ОПК-1, способность анализировать физические явления и процессы при решении профессиональных задач; ОПК-2, способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов; ОПК-8, способностью использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач; ПСК-2.2, способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах; ПСК-2.3, способностью строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов; ПСК-2.5, способность проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации.
	РО3. Способность осуществлять проектирование систем защиты информации с учётом актуальных информационных угроз и с использованием современных достижений науки и техники.	ОК-2, способность использовать основы экономических знаний в различных сферах деятельности; ОПК-4, способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами; ОПК-7, способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения;

		ОПК-10, способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах; ПК-7, способностью проводить анализ проектных решений по обеспечению защищенности компьютерных систем; ПСК-2.2, способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах; ПСК-2.3, способность строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов.
	РО4. Способность обеспечивать защищенность и функциональность компьютерных систем, производить их администрирование и профилактику работоспособности.	ПК-10, способностью оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации; ПСК-2.4, способностью разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации; ПСК-2.5, способность проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации; ДПК-1, способность разрабатывать планы и программы проведения научных исследований и технических разработок, подготавливать отдельные задания для исполнителей и контролировать их выполнение;
	РО8. Способность к разработке, анализу и обоснованию адекватности математических	ОПК-2, способность корректно применять при решении профессиональных задач аппарат

	моделей процессов, возникающих при функционировании программно-аппаратных средств защиты информации, а также к разработке математических моделей для оценки безопасности компьютерных систем.	математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов; ОПК-7, способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения; ОПК-10, способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах; ПК-4, способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем; ПСК-2.1, способностью разрабатывать вычислительные алгоритмы, реализующие современные методы защиты информации; ПСК-2.2, способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах; ПСК-2.3, способность строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов; ПСК-2.4, способность разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации; ПСК-2.5, способностью проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации.

4.2.Распределение формирования компетенций по дисциплинам модуля

Дисциплины модуля		ОПК 1	ОПК 2,4,10	ОПК 7	ПК 4,7,10	ПСК 2.1,2.2,2.3, 2.4	ПСК 2.5	ДПК 1
1	**(Б)** Теоретико-числовые методы в криптографии	*	*	*	*	*	*	
2	**(ВВ)** Теория чисел		*			*	*	*
3	**(ВВ)** Теория конечных полей		*	*		*		*

5. ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО МОДУЛЮ

Не предусмотрено

6. ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ В РАБОЧЕЙ ПРОГРАММЕ МОДУЛЯ

Номер листа изменений	Номер протокола заседания проектной группы модуля	Дата заседания проектной группы модуля	Всего листов в документе	Подпись руководителя проектной группы модуля

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

Перечень сведений о рабочей программе дисциплины	**Учетные данные**
Модуль **Математические основы криптографии**	Код модуля **1117699** **Учебный план № 5347**
Образовательная программа **Компьютерная безопасность**	Код ОП **10.05.01/01.02**
Направление подготовки **Компьютерная безопасность**	Код направления и уровня подготовки **10.05.01**
Уровень подготовки **Специалитет**	
ФГОС ВО	Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО: **1 декабря 2016 г., № 1512**

Екатеринбург, 2018

Рабочая программа дисциплины составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Кафедра	Подпись
1	Ананичев Дмитрий Сергеевич	К. ф.-м. н., доцент	доцент	Кафедра алгебры и дискретной математики	

Руководитель модуля Д.С.Ананичев

Рекомендовано учебно-методическим советом института математики и компьютерных наук

Председатель учебно-методического совета А.Ю.Коврижных
Протокол № 12 от 15 декабря 2016 г.

Согласовано:

Дирекция образовательных программ Р.Х.Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

1.1.Аннотация содержания дисциплины

Дисциплина «Теоретико-числовые методы в криптографии» (базовая часть) является одной из трех дисциплин модуля «Математические основы криптографии» и основывается на базе дисциплины «Теория чисел».

Курс «Теоретико-числовые методы в криптографии» посвящен изучению с теоретической и алгоритмической точек зрения базовых задач теории чисел, на которых основывается большинство современных асимметричных криптосистем с разработки, функционирования, оценок стойкости и эффективности современных симметричных и асимметричных криптосистем. Подробно рассматриваются вопросы временной сложности, проверки простоты чисел, факторизации чисел, дискретного логарифмирования в наиболее важных для криптографии абелевых группах.

1.2. Язык реализации программы - русский

1.3. Планируемые результаты обучения по дисциплине

Результатом обучения в рамках дисциплины является формирование у студента следующих компетенций:

ОПК-1, способность анализировать физические явления и процессы при решении профессиональных задач;

ОПК-2, способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов;

ОПК-4, способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами;

ОПК-7, способность учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения;

ОПК-10, способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах;

ПК-4, способность проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем;

ПК-7, способность проводить анализ проектных решений по обеспечению защищенности компьютерных систем;

ПК-10, способность оценивать эффективность реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;

ПСК-2.1, способность разрабатывать вычислительные алгоритмы, реализующие современные методы защиты информации;

ПСК-2.2, способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах;

ПСК-2.3, способность строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов;

ПСК-2.4, способность разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации;

ПСК-2.5, способность проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации.

В результате освоения дисциплины студент должен:

Знать:

- основные задачи, на сложности которых основана надежность современных систем криптографической защиты информации;
- основные теоретико-числовые алгоритмы, применяемые в современных системах криптографической защиты информации (методы факторизации, дискретного логарифмирования, проверки простоты чисел и построения сертифицированных простых чисел, алгоритмы работы с эллиптическими кривыми).

Уметь:

- вычислять сложности теоретико-числовых алгоритмов;
- решать сравнения второй степени по простому модулю, сравнения произвольной степени по модулю степени малого простого числа, системы сравнений.

Владеть:

- методами проверки простоты чисел Соловея-Штрассена и Рабина-Миллера;
- методами Диемитко, Поклингтона и Маурера построения сертифицированных простых чисел;
- методами факторизации Ферма, Полларда и Диксона;
- навыками сложения точек эллиптической кривой над простым полем;
- навыками решения задач по теории чисел.

1.4. Объем дисциплины

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)
		Всего часов	В т.ч. контактная работа (час.)*	5 семестр
1.	**Аудиторные занятия**	**51**	**51**	**51**
2.	Лекции	34	34	34
3.	Практические занятия	17	17	17
4.	Лабораторные работы			
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	**75**	**7,65**	**75**
6.	**Промежуточная аттестация**	**18**	**2,33**	**Экзамен (18)**
7.	**Общий объем по учебному плану, час.**	**144**	**60,98**	**144**
8.	**Общий объем по учебному плану, з.е.**	**4**		**4**

*Контактная работа составляет:

в п/п 2,3,4 - количество часов, равное объему соответствующего вида занятий;

в п.5 – количество часов, равное сумме объема времени, выделенного преподавателю на консультации в группе (15% от объема аудиторных занятий) и объема времени, выделенного преподавателю на руководство курсовой работой/проектом одного студента, если она предусмотрена.

в п.6 – количество часов, равное сумме объема времени, выделенного преподавателю на проведение соответствующего вида промежуточной аттестации одного студента и объема времени, выделенного в рамках дисциплины на руководство проектом по модулю (если он предусмотрен) одного студента.

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела, темы	Раздел, тема дисциплины	Содержание
Р1	**Сложность арифметических операций.**	Свойства функции сложности. Сложность операций с целыми числами. Сложность алгоритма Евклида. Дискретное преобразование Фурье. Умножение и деление многочленов.
Р2	**Проверка чисел на простоту.**	Элементарные методы. Тест на основе малой теоремы Ферма. Числа Кармайкла. Эйлеровы псевдопростые числа. Тест Соловея-Штрассена. Сильнопсевдопростые числа. Тест Рабина-Миллера. Тест Агравала-Кайала-Саксены и его модификация Ленстры-Померанца.
Р3	**Построение больших простых чисел.**	Критерий Люка. Понятие сертификата простоты. Теорема Поклингтона. Метод Маурера. (n+1)-методы построения простых чисел.
Р4	**Факторизация.**	(p-1)-метод Полларда. ρ-метод Полларда. Метод Полларда-Штрассена. Метод Ферма. Алгоритм Диксона. Модификация Билхарта-Моррисона. Метод квадратичного решета. Алгоритмы решета числового поля.
Р5	**Дискретное логарифмирование.**	Детерминированные методы. ρ-метод Полларда. Дискретное логарифмирование в простых полях: алгоритмы Адлемана и Копперсмита-Одлыжко-Шреппеля. Алгоритм исчисления индексов.
Р6	**Эллиптические кривые.**	Свойства эллиптических кривых. Алгоритм Ленстры для факторизации с помощью эллиптических кривых. Тестирова-ние чисел на простоту с помощью эллиптических кривых.

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

3.1. Распределение аудиторной нагрузки и мероприятий самостоятельной работы по разделам дисциплины

5 семестр

Объем модуля (зач.ед.): 4
Объем дисциплины (зач.ед.): 4

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
Код раздела, темы	Наименование раздела, темы	**Всего по разделу, теме (час.)**	**Всего аудиторной работы (час.)**	Лекции	Практические занятия	Лабораторные работы	**Всего самостоятельной работы студентов (час.)**	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)																	
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	**Всего (час.)**	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод иноязычной литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
Р1	Сложность арифметических операций.	**22**	**8**	6	2		**14**	**4**	1,2	2,8			**10**	1															
Р2	Проверка чисел на простоту.	**21**	**10**	8	2		**11**	**5**	1,6	3,4													**6**	1					
Р3	Построение больших простых чисел.	**20**	**6**	4	2		**14**	**4**	0,8	3,2			**10**	1															
Р4	Факторизация.	**17**	**10**	6	4		**7**	**7**	1,2	5,8																			
Р5	Дискретное логарифмирование.	**21**	**9**	6	3		**12**	**6**	1,2	4,8													**6**	1					
Р6	Эллиптические кривые.	**25**	**8**	4	4		**17**	**7**	0,8	6,2			**10**	1															
	Всего (час), без учета промежуточной аттестации**:**	**126**	**51**	**34**	**17**	**0**	**75**	**33**	**6,8**	**26,2**	**0**	**0**	**30**	**30**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**12**	**12**	**0**				
	Всего по дисциплине (час.):	**144**	**51**				**93**	В т.ч. промежуточная аттестация																		**0**	**18**	**0**	**0**

*Суммарный объем в часах на мероприятие
указывается в строке «Всего (час.) без учета промежуточной аттестации

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

4.1. Лабораторные работы

«не предусмотрено»

4.2. Практические занятия

Код раздела, темы	Номер заня-тия	Тема занятия	Время на проведение занятия (час.)
P1	1	Вычисление функций сложности алгоритмов.	2
P2	2	Проверка чисел на простоту.	2
P3	3	Построение сертифицированных простых чисел.	2
P4	4	Факторизация методами Полларда.	2
P4	5	Факторизация методом Диксона.	2
P5	6	Дискретное логарифмирование методом Похлига-Хеллмана и ρ−методом Полларда.	2
P5	7	Дискретное логарифмирование методом Адлемана.	1
P6	8	Сложение точек эллиптической кривой.	2
P6	9	Метод согласования на эллиптической кривой.	2
		Всего:	17

4.3.Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

1. Оценка временной сложности задачи.
2. Построение сертифицированного простого числа.
3. Решение задачи дискретного логарифмирования на эллиптической кривой.

4.3.2. Примерный перечень тем графических работ

«не предусмотрено»

4.3.3. Примерный перечень тем рефератов (эссе, творческих работ)

«не предусмотрено»

4.3.4 Примерная тематика индивидуальных или групповых проектов

«не предусмотрено»

4.3.5. Примерный перечень тем расчетных работ (программных продуктов)

«не предусмотрено»

4.3.6. Примерный перечень тем расчетно-графических работ

«не предусмотрено»

4.3.7. Примерный перечень тем курсовых проектов (курсовых работ)

«не предусмотрено»

4.4.1. Примерная тематика контрольных работ

1. Поиск эйлерового псевдопростого числа, не являющегося сильно псевдопростым по тому же основанию.
2. Дискретное логарифмирование методом Похлига-Хеллмана.

4.3.9. Примерная тематика коллоквиумов

«не предусмотрено»

5. СООТНОШЕНИЕ РАЗДЕЛОВ, ТЕМ ДИСЦИПЛИНЫ И ПРИМЕНЯЕМЫХ ТЕХНОЛОГИЙ ОБУЧЕНИЯ

Код раздела, темы дисциплины	Активные методы обучения						Дистанционные образовательные технологии и электронное обучение					
	Проектная работа	Кейс-анализ	Деловые игры	Проблемное обучение	Командная работа	Другие (указать, какие)	Сетевые учебные курсы	Виртуальные практикумы и тренажеры	Вебинары и видеоконференции	Асинхронные web-конференции и семинары	Совместная работа и разработка контента	Другие (указать, какие)
Р1		+		+	+							
Р2		+		+	+							
Р3		+		+	+							
Р4		+		+	+							
Р5		+		+	+							
Р6		+		+	+							

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ (Приложение 1)

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ (Приложение 2)

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (Приложение 3)

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1.Рекомендуемая литература

9.1.1.Основная литература

1. Василенко, О.Н. Теоретико-числовые алгоритмы в криптографии. М : МЦНМО, 2006. — 336 с. — http://window.edu.ru/resource/845/23845/files/book.pdf.

2. Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии. - М., МЦНМО, 2002. http://window.edu.ru/resource/004/24004/files/cherem.pdf

9.1.2.Дополнительная литература

Granville A. It is easy to determine whether a given integer is prime.// Bull. Of A. Math. Soc., Vol. 42., № 1, 2005, pp. 3-38. http://www.ams.org/journals/bull/2005-42-01/S0273-0979-04-01037-7/S0273-0979-04-01037-7.pdf

9.2. Методические разработки

Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии. - М., МЦНМО, 2002. http://window.edu.ru/resource/004/24004/files/cherem.pdf

9.3.Программное обеспечение

Не используется

9.4. Базы данных, информационно-справочные и поисковые системы

Общероссийский математический портал http://www.mathnet.ru/
Научная электронная библиотека eLibrary.ru http://www.elibrary.ru/
Сайт издательства Elsevier http://www.sciencedirect.com/
Сайт кафедры: http://kma.imkn.urfu.ru
Сайт кафедры: http://kadm.imkn.urfu.ru/pages.php?id=index
Сайт библиотеки университета http://lib.urfu.ru/

9.5.Электронные образовательные ресурсы

Не используются

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Аудитория с проектором

ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Весовой коэффициент значимости дисциплины –

6.2.Процедуры текущей и промежуточной аттестации по дисциплине

1.Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0,6		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Домашняя работа № 3	**6, 1-17**	**100**
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,4		
Промежуточная аттестация по лекциям – *экзамен* **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,6**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0,4		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Домашняя работа № 1	**1, 1-10**	**20**
Домашняя работа № 2	**1, 1-14**	**20**
Контрольная работа № 1	**1, 1-10**	**30**
Контрольная работа № 2	**1, 1-17**	**30**
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям–1		
Промежуточная аттестация по практическим/семинарским занятиям– не предусмотрено **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– 0**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –не предусмотрены		

6.3. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

Не предусмотрены

6.4. Коэффициент значимости семестровых результатов освоения дисциплины

Порядковый номер семестра по учебному плану, в котором осваивается дисциплина	**Коэффициент значимости результатов освоения дисциплины в семестре**
Семестр 5	1

ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

Не применяется

ПРИЛОЖЕНИЕ 3
к рабочей программе дисциплины

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

8.1. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ В РАМКАХ БРС

В рамках БРС применяются утвержденные на кафедре критерии оценивания достижений студентов по каждому контрольно-оценочному мероприятию. Система критериев оценивания, как и при проведении промежуточной аттестации по модулю, опирается на три уровня освоения компонентов компетенций: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

8.2. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПРИ ИСПОЛЬЗОВАНИИ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

НТК не проводится

8.3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.3.1. Примерные задания для проведения мини-контрольных в рамках учебных занятий

«не предусмотрено»

8.3.2. Примерные контрольные задачи в рамках учебных занятий

Контрольная работа № 1.

Задание. Найдите в интервале от 1000 до 2000 число и основание, по которому найденное число эйлерово псевдопростое, но не сильно псевдопростое.

Контрольная работа № 2.

Задание. Решите методом Похлига-Хеллмана сравнение $\mathbf{11^x=100 (mod\ 769)}$, используя разложение $\mathbf{768=2^8*3}$.

8.3.3. Примерные контрольные кейсы

«не предусмотрено»

8.3.4. Перечень примерных вопросов для зачета

«не предусмотрено»

8.3.5. Перечень примерных вопросов для экзамена

1. Сложность элементарных операций.
2. Умножение методом Шенхаге-Штрассена.
3. Теорема Кармайкла.
4. Тест простоты Соловея-Штрассена.
5. Псевдопростые, эйлеровы псевдопростые и сильнопсевдопростые числа по основанию a.
6. Теорема Рабина. Тест простоты Рабина-Миллера.
7. Теорема Агравала-Кайала-Саксены.
8. Тест простоты Агравала-Кайала-Саксены.
9. Дискретное преобразование Фурье.
10. Умножение и деление многочленов с помощью дискретного преобразования Фурье.
11. Критерий Люка и теорема Поклингтона.
12. Метод Маурера построения простых чисел.
13. Методы факторизации Ферма и (p-1)-метод Полларда.
14. Факторизация методом Полларда-Штрассена.
15. Факторизация методами Диксона и Биллхарта-Моррисона.
16. Факторизация методом квадратичного решета Померанца.
17. Дискретное логарифмирование методом согласования и методом Похлига-Хеллмана.
18. Метод исчисления индексов.
19. Теорема о 8 точках и ее следствия.
20. Сложение точек на эллиптической кривой.
21. Алгоритм Ленстры для факторизации с помощью эллиптических кривых.
22. Тестирование чисел на простоту с помощью эллиптических кривых.

8.3.6. Ресурсы АПИМ УрФУ, СКУД УрФУ для проведения тестового контроля в рамках текущей и промежуточной аттестации

«не используются»

8.3.7. Ресурсы ФЭПО для проведения независимого тестового контроля

«не используются»

8.3.8. Интернет-тренажеры

«не используются»

8.3.9. Примерные задания для домашних работ

Домашняя работа № 1.

Задание 1. Доказать, что сложность вычисления НОД двух целых чисел $O(n^2)$.

Задание 2. Доказать, что сложность вычисления определителя двоичной матрицы $O(n^{1.5})$.

Домашняя работа № 2.

Задание 1. Найти сертификат простоты числа **222199** по критерию Люка.

Задание 2. Построить цепь сертифицированных по теореме Диемитко простых чисел, начинающуюся однозначным и заканчивающимся (не менее, чем) пятизначным десятичным числом.

Домашняя работа № 3.

Задание 1. С помощью алгоритма согласования решите в группе точек эллиптической кривой $\mathbf{E_{4,2}(Z_{47})}$ уравнение **(0,7)*x=(17,46).**

Задание 2. Найдите порядок точки **(0,14)** в группе точек эллиптической кривой $\mathbf{E_{4,2}(Z_{97})}$, если известно, что порядок этой группы равен **91**.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ТЕОРИЯ КОНЕЧНЫХ ПОЛЕЙ

Перечень сведений о рабочей программе дисциплины	**Учетные данные**
Модуль **Математические основы криптографии**	Код модуля **1117699** **Учебный план № 5347**
Образовательная программа **Компьютерная безопасность**	Код ОП **10.05.01/01.02**
Направление подготовки **Компьютерная безопасность**	Код направления и уровня подготовки **10.05.01**
Уровень подготовки **Специалитет**	
ФГОС ВО	Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО: **1 декабря 2016 г., № 1512**

Екатеринбург, 2018

Рабочая программа дисциплины составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Кафедра	Подпись
1	Баранский Виталий Анатольевич	Д. ф.-м. н., профессор	Профессор	Кафедра алгебры и дискретной математики	

Руководитель модуля Д.С.Ананичев

Рекомендовано учебно-методическим советом института математики и компьютерных наук

Председатель учебно-методического совета А.Ю.Коврижных
Протокол № 12 от 15 декабря 2016 г.

Согласовано:

Дирекция образовательных программ Р.Х.Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В КРИПТОГРАФИИ

1.1.Аннотация содержания дисциплины

Дисциплина «Теория конечных полей» является одной из трех дисциплин модуля «Математические основы криптографии» и не зависима от других дисциплин модуля.

Курс «Теория конечных полей» посвящен изучению базовых понятий и задач теории полей. Подробно рассматриваются свойства расширений полей, свойства автоморфизмов конечных полей, неприводимые многочлены над конечными полями.

1.2. Язык реализации программы - русский

1.3. Планируемые результаты обучения по дисциплине

Результатом обучения в рамках дисциплины является формирование у студента следующих компетенций:

ОПК-2, способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов;

ОПК-4, способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами;

ОПК-7, способностью учитывать современные тенденции развития информатики и вычислительной техники, компьютерных технологий в своей профессиональной деятельности, работать с программными средствами общего и специального назначения;

ОПК-10, способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах;

ДПК-1, способность разрабатывать планы и программы проведения научных исследований и технических разработок, подготавливать отдельные задания для исполнителей и контролировать их выполнение;

ПСК-2.1, способность разрабатывать вычислительные алгоритмы, реализующие современные методы защиты информации;

ПСК-2.2, способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах;

ПСК-2.3, способность строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов;

ПСК-2.4, способность разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации;

В результате освоения дисциплины студент должен:

Знать:

- основные понятия теории полей;
- основные результаты теории цепных дробей.

Уметь:

- решать стандартные вычислительные задачи в конечном поле;
- применять теорию конечных полей при построении математических моделей;
- разлагать многочлен на неприводимые множители над конечным полем.

Владеть:

- методами, построения минимального многочлена элемента и примитивного многочлена конечного расширения;

– методами изучения связей фундаментальных математических проблем с проблемами теории полей.

1.4. Объем дисциплины

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)
		Всего часов	В т.ч. контактная работа (час.)*	4 семестр
1.	**Аудиторные занятия**	**34**	**34**	**34**
2.	Лекции	34	34	34
3.	Практические занятия			
4.	Лабораторные работы			
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	**34**	**5,10**	**34**
6.	**Промежуточная аттестация**	**4**	**0,25**	**Зачет (4)**
7.	**Общий объем по учебному плану, час.**	**72**	**39,35**	**72**
8.	**Общий объем по учебному плану, з.е.**	**2**		**2**

*Контактная работа составляет:

в п/п 2,3,4 - количество часов, равное объему соответствующего вида занятий;

в п.5 – количество часов, равное сумме объема времени, выделенного преподавателю на консультации в группе (15% от объема аудиторных занятий) и объема времени, выделенного преподавателю на руководство курсовой работой/проектом одного студента, если она предусмотрена.

в п.6 – количество часов, равное сумме объема времени, выделенного преподавателю на проведение соответствующего вида промежуточной аттестации одного студента и объема времени, выделенного в рамках дисциплины на руководство проектом по модулю (если он предусмотрен) одного студента.

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела, темы	Раздел, тема дисциплины	Содержание
Р1	**Расширения полей.**	Вложение областей целостности в поля. Поле рациональных дробей. Китайская теорема об остатках. Алгебраический расширения полей. Конечные расширения полей, алгебраические и трансцедентные элементы, минимальный многочлен, простое расширение поля. Поле разложения многочлена, существование и единственность.
Р2	**Конечные поля и неприводимые многочлены.**	Характеризация конечных полей, подполя конечного поля, поле F_{p^∞} , примитивные элементы и примитивные многочлены. Корни неприводимых многочленов, автоморфизм Фробениуса, сопряженные элементы. Группа автоморфизмов конечного поля.
Р3	**Вычисления в конечных полях.**	Формула обращения Мёбиуса. Корни из единицы и круговые многочлены, формулы для вычисления круговых

		многочленов, разложение кругового многочлена на неприводимые множители. Представление элементов в конечных полях, таблицы индексов и примитивные элементы, представление конечных полей матрицами. Многочлены без кратности неприводимых множителей, алгоритм Берлекэмпа разложения многочлена на неприводимые множители. Порядок многочлена, характеризация примитивных многочленов. Методы построения минимальных многочленов. Методы построения примитивных многочленов. Семейство нормированных неприводимых многочленов данной степени над конечным полем, $I_q(n)$ и $I(q; n; x)$, разложение многочлена $I(q; n; x)$ в произведение круговых многочленов.

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

3.1. Распределение аудиторной нагрузки и мероприятий самостоятельной работы по разделам дисциплины

5 семестр

Объем модуля (зач.ед.): 4
Объем дисциплины (зач.ед.): 4

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																							
Код раздела, темы	Наименование раздела, темы	**Всего по разделу, теме (час.)**	**Всего аудиторной работы (час.)**	Лекции	Практические занятия	Лабораторные работы	**Всего самостоятельной работы студентов (час.)**	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)											Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	**Всего (час.)**	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод инояз. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
Р1	Расширения полей.	18,4	10	10			8,4	2	2				6,4	1																
Р2	Конечные поля и неприводимые многочлены.	22,4	10	10			12,4	2	2				6,4	1										4	1					
Р3	Вычисления в конечных полях.	27,2	14	14			13,2	2,8	2,8				6,4	1										4	1					
	Всего (час), без учета промежуточной аттестации**:**	**68**	**34**	**34**	**0**	**0**	**34**	**6,8**	**6,8**	**0**	**0**	**0**	**19,2**	**19,2**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**8**	**8**	**0**				
	Всего по дисциплине (час.):	**72**	**34**				**34**	В т.ч. промежуточная аттестация																			**4**	**0**	**0**	**0**

*Суммарный объем в часах на мероприятие
указывается в строке «Всего (час.) без учета промежуточной аттестации

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

4.1. Лабораторные работы

«не предусмотрено»

4.2. Практические занятия

«не предусмотрено»

4.3.Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

1. Расширения полей.
2. Конечные поля и неприводимые многочлены.
3. Вычисления в конечных полях.

4.3.2. Примерный перечень тем графических работ

«не предусмотрено»

4.3.3. Примерный перечень тем рефератов (эссе, творческих работ)

«не предусмотрено»

4.3.4 Примерная тематика индивидуальных или групповых проектов

«не предусмотрено»

4.3.5. Примерный перечень тем расчетных работ (программных продуктов)

«не предусмотрено»

4.3.6. Примерный перечень тем расчетно-графических работ

«не предусмотрено»

4.3.7. Примерный перечень тем курсовых проектов (курсовых работ)

«не предусмотрено»

4.4.1. Примерная тематика контрольных работ

1. Конечные поля и неприводимые многочлены.
2. Вычисления в конечных полях.

4.3.9. Примерная тематика коллоквиумов

«не предусмотрено»

4. СООТНОШЕНИЕ РАЗДЕЛОВ, ТЕМ ДИСЦИПЛИНЫ И ПРИМЕНЯЕМЫХ ТЕХНОЛОГИЙ ОБУЧЕНИЯ

Код раздела, темы дисциплины	Активные методы обучения						Дистанционные образовательные технологии и электронное обучение					
	Проектная работа	Кейс-анализ	Деловые игры	Проблемное обучение	Командная работа	Другие (указать, какие)	Сетевые учебные курсы	Виртуальные практикумы и тренажеры	Вебинары и видеоконференции	Асинхронные web-конференции и семинары	Совместная работа и разработка контента	Другие (указать, какие)
Р1		+		+	+							
Р2		+		+	+							
Р3		+		+	+							
Р4		+		+	+							
Р5		+		+	+							

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ (Приложение 1)

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ (Приложение 2)

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (Приложение 3)

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1.Рекомендуемая литература

9.1.1.Основная литература

1. Баранский, Виталий Анатольевич. Общая алгебра и ее приложения : [учеб. пособие для вузов] / В. А. Баранский, В. В. Кабанов. — Екатеринбург : Изд-во Урал. ун-та, 2008. — 243 с. : ил. — (Приоритетный национальный проект "Образование") (Информационная безопасность). — Библиогр.: с. 233-234. — ISBN 978-5-7996-0378-6.

2. Кабанов, Владислав Владимирович. Учебно-методический комплекс дисциплины "Конечные поля" [Электронный ресурс] / В. В. Кабанов ; Федер. агентство по образованию, Урал. гос. ун-т им. А. М. Горького, ИОНЦ "Информационная безопасность" [и др.]. — Электрон. дан. (1,15 Мб). — Екатеринбург : [б. и.], 2008. — 1 электрон. опт. диск (CD-ROM). — Загл. с этикетки диска. — <URL: http://elar.urfu.ru/handle/10995/1657>.

9.1.2.Дополнительная литература

1. Лидл Р., Пильц Г. Прикладная абстрактная алгебра: Учебное пособие / Перевод с английского. – Екатеринбург: Изд-во УрГУ, 1996.
2. Баранский, Виталий Анатольевич. Введение в общую алгебру и ее приложения : Учеб. пособие / В. А. Баранский. — Екатеринбург : Изд-во Урал. гос. ун-та, 1998. — 170 с. — Библиогр.: с. 166-167. — ISBN 5-7996-0006-1 : 10-00. — 13-00. — 11-00. — 12-00. — 30-00.
3. Варден, Бартел Лендерт ван дер. Алгебра / Б. Л. ван дер Варден ; Пер. с нем. А. А. Бельского. — 3-е изд., стер. — СПб. ; М. ; Краснодар : Лань, 2004. — 624 с. — (Учебники для вузов. - Специальная литература). — ISBN 5-8114-0552-9 : 276-00. — 318-00. — 311-00.
4. Ленг, С. Алгебра : Пер. с англ. / С. Ленг ; Под ред. А. И. Кострина. — М. : Мир, 1968. — 564 с. — ISBN 5-03-000640-0 : 2-41. — 17-00

9.2. Методические разработки

1. Баранский, Виталий Анатольевич. Общая алгебра и ее приложения : [учеб. пособие для вузов] / В. А. Баранский, В. В. Кабанов. — Екатеринбург : Изд-во Урал. ун-та, 2008. — 243 с. : ил. — (Приоритетный национальный проект "Образование") (Информационная безопасность). — Библиогр.: с. 233-234. — ISBN 978-5-7996-0378-6.

2. Кабанов, Владислав Владимирович. Учебно-методический комплекс дисциплины "Конечные поля" [Электронный ресурс] / В. В. Кабанов ; Федер. агентство по образованию, Урал. гос. ун-т им. А. М. Горького, ИОНЦ "Информационная безопасность" [и др.]. — Электрон. дан.

(1,15 Мб). — Екатеринбург : [б. и.], 2008. — 1 электрон. опт. диск (CD-ROM). — Загл. с этикетки диска. — <URL: http://elar.urfu.ru/handle/10995/1657>.

3. Баранский, Виталий Анатольевич. Введение в общую алгебру и ее приложения : Учеб. пособие / В. А. Баранский. — Екатеринбург : Изд-во Урал. гос. ун-та, 1998. — 170 с. — Библиогр.: с. 166-167. — ISBN 5-7996-0006-1 : 10-00. — 13-00. — 11-00. — 12-00. — 30-00.

9.3.Программное обеспечение

Не используется

9.4. Базы данных, информационно-справочные и поисковые системы

Общероссийский математический портал http://www.mathnet.ru/
Научная электронная библиотека eLibrary.ru http://www.elibrary.ru/
Сайт издательства Elsevier http://www.sciencedirect.com/
Сайт кафедры: http://kma.imkn.urfu.ru
Сайт кафедры: http://kadm.imkn.urfu.ru/pages.php?id=index
Сайт библиотеки университета http://lib.urfu.ru/

9.5.Электронные образовательные ресурсы

Не используются

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Аудитория с проектором

ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Весовой коэффициент значимости дисциплины –

6.2.Процедуры текущей и промежуточной аттестации по дисциплине

1.Лекции: коэффициент значимости совокупных результатов лекционных занятий – 1		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Контрольная работа № 1	**1, 1-10**	**20**
Контрольная работа № 2	**1, 1-17**	**20**
Домашняя работа № 1	**1, 1-10**	**20**
Домашняя работа № 2	**1, 1-14**	**20**
Домашняя работа № 3	**6, 1-17**	**20**
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,4		
Промежуточная аттестация по лекциям – *зачет* **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,6**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – не предусмотрены		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий – не предусмотрены		

6.3. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

Не предусмотрены

6.4. Коэффициент значимости семестровых результатов освоения дисциплины

Порядковый номер семестра по учебному плану, в котором осваивается дисциплина	**Коэффициент значимости результатов освоения дисциплины в семестре**
Семестр 4	1

*В случае проведения промежуточной аттестации по дисциплине (экзамена, зачета) методом тестирования используются официально утвержденные ресурсы: АПИМ УрФУ, СКУД УрФУ, имеющие статус ЭОР УрФУ; ФЭПО (www.фэпо.рф); Интернет-тренажеры (www.i-exam.ru).

ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

Не применяется

ПРИЛОЖЕНИЕ 3
к рабочей программе дисциплины

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

8.1. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ В РАМКАХ БРС

В рамках БРС применяются утвержденные на кафедре критерии оценивания достижений студентов по каждому контрольно-оценочному мероприятию. Система критериев оценивания, как и при проведении промежуточной аттестации по модулю, опирается на три уровня освоения компонентов компетенций: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

8.2. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПРИ ИСПОЛЬЗОВАНИИ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

НТК не проводится

8.3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.3.1. Примерные задания для проведения мини-контрольных в рамках учебных занятий

«не предусмотрено»

8.3.2. Примерные контрольные задачи в рамках учебных занятий

Контрольная работа № 1.

Задание 1. Отправляясь от представления **GF(16)** как поля разложения неприводимого над $\mathbf{Z_2}$ многочлена $x^4 + x + 1$, найти многочлен над $\mathbf{Z_2}$ наименьшей степени, имеющий корень $x^3 + x^2$.

Задание 2. Построить решетку подполей поля **GF(64)**.

Контрольная работа № 2.

Задание 1. Разложить на неприводимые над $\mathbf{Z_2}$ множители многочлен $x^{11} + x^3 + 1$

Задание 2. Пусть a — примитивный элемент поля **GF(31)**, такой что $a^5 + a^2 + 1 = 0$. Найти многочлен наименьшей степени (над $\mathbf{Z_2}$), среди корней которого встречаются a^3 и a^7.

8.3.3. Примерные контрольные кейсы

«не предусмотрено»

8.3.4. Перечень примерных вопросов для зачета

1. Теорема о вложение областей целостности в поля.
2. Строение поля рациональных дробей.
3. Китайская теорема об остатках.
4. Алгебраический расширения полей.
5. Конечные расширения полей.
6. Поле разложения многочлена, его существование
7. Поле разложения многочлена, его единственность.
8. Характеризация конечных полей.
9. Подполя конечного поля.
10. Поле $F_{p\infty}$.
11. Примитивные элементы и примитивные многочлены.
12. Корни неприводимых многочленов.
13. Автоморфизм Фробениуса, сопряженные элементы.
14. Группа автоморфизмов конечного поля.
15. Формула обращения Мёбиуса.
16. Корни из единицы и круговые многочлены.
17. Формулы для вычисления круговых многочленов.
18. Разложение кругового многочлена на неприводимые множители.
19. Представление элементов в конечных полях.
20. Таблицы индексов и примитивные элементы.
21. Представление конечных полей матрицами.
22. Алгоритм Берлекэмпа разложения многочлена на неприводимые множители.
23. Порядок многочлена.
24. Характеризация примитивных многочленов.
25. Методы построения минимальных многочленов.

26. Методы построения примитивных многочленов.
27. Семейство нормированных неприводимых многочленов данной степени над конечным полем.
28. Разложение многочлена I(q; n; x) в произведение круговых многочленов.

8.3.5. Перечень примерных вопросов для экзамена

«не предусмотрено»

8.3.6. Ресурсы АПИМ УрФУ, СКУД УрФУ для проведения тестового контроля в рамках текущей и промежуточной аттестации

«не используются»

8.3.7. Ресурсы ФЭПО для проведения независимого тестового контроля

«не используются»

8.3.8. Интернет-тренажеры

«не используются»

8.3.9. Примерные задания для домашних работ

Домашняя работа № 1.

Задание 1. Решить систему линейных уравнений

$x + 2z = 1$;

$y + 2z = 2$;

$2x + z = 1$

а) в поле Z_3, б) в поле Z_5.

Задание 2. Пусть $\boldsymbol{a}$ — корень многочлена $\boldsymbol{x^5 + x^2 + 1}$ над $\mathbf{Z_2}$, такой что $\boldsymbol{a^5 + a^2 + 1 = 0}$.

Разложить все степени $\boldsymbol{a}$ по базису $\mathbf{1, a, a^2, a^3, a^4}$ над полем $\mathbf{Z_2}$.

Задание 3. Найти в поле $\mathbf{Z_2}[x]/\ \boldsymbol{x^8 + x^4 + x^3 + x + 1}$ элемент, обратный к $\boldsymbol{x^4 + 1}$.

Домашняя работа № 2.

Задание 1. Отправляясь от представления GF(16) как поля разложения неприводимого над $\mathbf{Z_2}$ многочлена $\boldsymbol{x^4 + x + 1}$, найти все примитивные элементы этого поля.

Задание 2. Разложить многочлен $\boldsymbol{x^{63} - 1}$ на неприводимые множители над полем $\mathbf{Z_2}$.

Задание 3. Отправляясь от представления GF(32) как поля разложения неприводимого над $\mathbf{Z_2}$ многочлена $\boldsymbol{x^5 + x^2 + 1}$, найти многочлен над $\mathbf{Z_2}$ наименьшей степени, имеющий корень $\boldsymbol{x^3 + x^2}$.

Домашняя работа № 3.

Задание 1. Разложить на неприводимые над $\mathbf{Z_3}$ множители многочлен $\boldsymbol{x^{23} - x^{11} - x^3 + 1}$

Задание 2. Найти минимальные многочлены для каждого ненулевого элемента поля GF(64).

Задание 3. Пусть a — примитивный элемент поля **GF(127)**, такой что $\boldsymbol{a^7 + a + 1 = 0}$. Найти многочлен наименьшей степени (над $\mathbf{Z_2}$), среди корней которого встречаются:

а) a, a^2, a^3 и a^4 б) a, a^3, a^5 и a^7,

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ТЕОРИЯ ЧИСЕЛ

Перечень сведений о рабочей программе дисциплины	**Учетные данные**
Модуль **Математические основы криптографии**	Код модуля **1117699** **Учебный план № 5347**
Образовательная программа **Компьютерная безопасность**	Код ОП **10.05.01/01.02**
Направление подготовки **Компьютерная безопасность**	Код направления и уровня подготовки **10.05.01**
Уровень подготовки **Специалитет**	
ФГОС ВО	Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО: **1 декабря 2016 г., № 1512**

Екатеринбург, 2018

Рабочая программа дисциплины составлена авторами:

№ п/п	ФИО	Ученая степень, ученое звание	Должность	Кафедра	Подпись
1	Сизый Сергей Викторович	Д. т. н., профес-сор	Профессор	Кафедра алгебры и дискрет-ной мате-матики	

Руководитель модуля Д.С.Ананичев

Рекомендовано учебно-методическим советом института математики и компьютерных наук

Председатель учебно-методического совета А.Ю.Коврижных
Протокол № 12 от 15 декабря 2016 г.

Согласовано:

Дирекция образовательных программ Р.Х.Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ ТЕОРИЯ ЧИСЕЛ

1.1.Аннотация содержания дисциплины

Дисциплина «Теория чисел» является одной из трех дисциплин модуля «Математические основы криптографии» и на ней основывается дисциплина «Теоретико-числовые методы в криптографии».

Курс «Теория чисел» посвящен изучению базовых понятий и задач теории чисел. Подробно рассматриваются свойства отношения делимости в Евклидовом кольце, свойства и основные приложения цепных дробей, важнейшие мультипликативные, теория сравнений первой и второй степени и систем сравнений, важнейшие результаты об алгебраических и трансцендентных числах.

1.2. Язык реализации программы - русский

1.3. Планируемые результаты обучения по дисциплине

Результатом обучения в рамках дисциплины является формирование у студента следующих компетенций:

ОПК-2, способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов;

ОПК-4, способность применять методы научных исследований в профессиональной деятельности, в том числе в работе над междисциплинарными и инновационными проектами;

ОПК-10, способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах;

ДПК-1, способность разрабатывать планы и программы проведения научных исследований и технических разработок, подготавливать отдельные задания для исполнителей и контролировать их выполнение;

ПСК-2.1, способностью разрабатывать вычислительные алгоритмы, реализующие современные методы защиты информации;

ПСК-2.2, способность на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах;

ПСК-2.3, способность строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов;

ПСК-2.4, способность разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации;

ПСК-2.5, способностью проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации.

В результате освоения дисциплины студент должен:

Знать:

- области применимости методов доказательства алгебраичности и трансцендентности действительных чисел;
- основные понятия арифметики целых чисел и теории делимости целых чисел;
- основные результаты теории цепных дробей.

Уметь:

- решать стандартные задачи на применение теории делимости и теории сравнений;
- решать сравнения первой степени и диофантовы уравнения.

Владеть:

- методами, основанными на использовании теоретико-числовых (мультипликативных) функций;
- методами элементарной теории чисел, основанных на теории делимости и теории сравнений.

1.4. Объем дисциплины

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины по семестрам (час.)
		Всего часов	В т.ч. контактная работа (час.)*	4 семестр
1.	**Аудиторные занятия**	**34**	**34**	**34**
2.	Лекции	34	34	34
3.	Практические занятия			
4.	Лабораторные работы			
5.	**Самостоятельная работа студентов, включая все виды текущей аттестации**	**34**	**5,10**	**34**
6.	**Промежуточная аттестация**	**4**	**0,25**	**Зачет (4)**
7.	**Общий объем по учебному плану, час.**	**72**	**39,35**	**72**
8.	**Общий объем по учебному плану, з.е.**	**2**		**2**

*Контактная работа составляет:

в п/п 2,3,4 - количество часов, равное объему соответствующего вида занятий;

в п.5 – количество часов, равное сумме объема времени, выделенного преподавателю на консультации в группе (15% от объема аудиторных занятий) и объема времени, выделенного преподавателю на руководство курсовой работой/проектом одного студента, если она предусмотрена.

в п.6 – количество часов, равное сумме объема времени, выделенного преподавателю на проведение соответствующего вида промежуточной аттестации одного студента и объема времени, выделенного в рамках дисциплины на руководство проектом по модулю (если он предусмотрен) одного студента.

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела, темы	Раздел, тема дисциплины	Содержание
Р1	**Основные понятия и теоремы.**	Деление с остатком. Наибольший общий делитель. Взаимно простые числа. Простые числа и основная теорема арифметики. Распределение простых чисел. Алгоритм Евклида. Линейные диофантовы уравнения.
Р2	**Цепные дроби.**	Разложение чисел в цепные дроби. Вычисление подходящих дробей. Свойства подходящих дробей. Континуанты, их связь с цепными дробями. Анализ алгоритма Евклида. Приближение чисел цепными дробями. Периодичность цепных дробей. Теорема Эрмита.

Р3	**Важнейшие функции в теории чисел.**	Целая и дробная части. Мультипликативные функции и их основные свойства. Примеры мультипликативных функций. Дзета-функция Римана, ее свойства и применения.
Р4	**Теория сравнений.**	Определения и простейшие свойства сравнений. Полная и приведенная системы вычетов. Теорема Эйлера и теорема Ферма. Сравнения первой степени. Сравнения любой степени по простому модулю. Сравнения любой степени по составному модулю. Сравнения второй степени, символ Лежандра, его свойства. Закон взаимности Гаусса.
Р5	**Трансцендентные числа.**	Мера и категория на прямой. Числа Лиувилля. Алгебраические числа, их свойства. Трансцендентность числа e. Трансцендентность числа π. Трансцендентность значений показательной функции, теорема Линдемана.

3. РАСПРЕДЕЛЕНИЕ УЧЕБНОГО ВРЕМЕНИ

3.1. Распределение аудиторной нагрузки и мероприятий самостоятельной работы по разделам дисциплины

5 семестр

Объем модуля (зач.ед.): 4
Объем дисциплины (зач.ед.): 4

Раздел дисциплины			Аудиторные занятия (час.)				Самостоятельная работа: виды, количество и объемы мероприятий																						
Код раздела, темы	Наименование раздела, темы	**Всего по разделу, теме (час.)**	**Всего аудиторной работы (час.)**	Лекции	Практические занятия	Лабораторные работы	**Всего самостоятельной работы студентов (час.)**	Подготовка к аудиторным занятиям (час.)					Выполнение самостоятельных внеаудиторных работ (колич.)											Подготовка к контрольным мероприятиям текущей аттестации (колич.)			Подготовка к промежуточной аттестации по дисциплине (час.)		Подготовка в рамках дисциплины к промежуточной аттестации по модулю (час.)	
								Всего (час.)	Лекция	Практ., семинар. занятие	Лабораторное занятие	Н/и семинар, семинар-конфер., коллоквиум (магистратура)	**Всего (час.)**	Домашняя работа*	Графическая работа*	Реферат, эссе, творч. работа*	Проектная работа*	Расчетная работа, разработка программного продукта*	Расчетно-графическая работа*	Домашняя работа на иностр. языке*	Перевод иностр. литературы*	Курсовая работа*	Курсовой проект*	**Всего (час.)**	Контрольная работа*	Коллоквиум*	Зачет	Экзамен	Интегрированный экзамен по модулю	Проект по модулю
Р1	Основные понятия и теоремы.	**11,2**	**4**	4			**7,2**	**0,8**	0,8				6,4	1										0						
Р2	Цепные дроби.	**20**	**8**	8			**12**	**1,6**	1,6				6,4	1										4	1					
Р3	Важнейшие функции в теории чисел.	**7,2**	**6**	6			**1,2**	**1,2**	1,2				0											0						
Р4	Теория сравнений.	**20**	**8**	8			**12**	**1,6**	1,6				6,4	1										4	1					
Р5	Трансцендентные числа.	**9,6**	**8**	8			**1,6**	**1,6**	1,6				0											0						
	Всего (час), без учета промежуточной аттестации**:**	**68**	**34**	**34**	**0**	**0**	**34**	**6,8**	**6,8**	**0**	**0**	**0**	**19,2**	**19,2**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**8**	**8**	**0**				
	Всего по дисциплине (час.):	**72**	**34**				**34**	В т.ч. промежуточная аттестация																			**4**	**0**	**0**	**0**

*Суммарный объем в часах на мероприятие
указывается в строке «Всего (час.) без учета промежуточной аттестации

4. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

4.1. Лабораторные работы

«не предусмотрено»

4.2. Практические занятия

«не предусмотрено»

4.3.Примерная тематика самостоятельной работы

4.3.1. Примерный перечень тем домашних работ

1. Делимость и НОД.
2. Цепные дроби.
3. Решение сравнений и вычисление символа Якоби.

4.3.2. Примерный перечень тем графических работ

«не предусмотрено»

4.3.3. Примерный перечень тем рефератов (эссе, творческих работ)

«не предусмотрено»

4.3.4 Примерная тематика индивидуальных или групповых проектов

«не предусмотрено»

4.3.5. Примерный перечень тем расчетных работ (программных продуктов)

«не предусмотрено»

4.3.6. Примерный перечень тем расчетно-графических работ

«не предусмотрено»

4.3.7. Примерный перечень тем курсовых проектов (курсовых работ)

«не предусмотрено»

4.4.1. Примерная тематика контрольных работ

1. Цепные дроби.
2. Решение сравнений и вычисление символа Якоби.

4.3.9. Примерная тематика коллоквиумов

«не предусмотрено»

5. СООТНОШЕНИЕ РАЗДЕЛОВ, ТЕМ ДИСЦИПЛИНЫ И ПРИМЕНЯЕМЫХ ТЕХНОЛОГИЙ ОБУЧЕНИЯ

Код раздела, темы дисциплины	Активные методы обучения						Дистанционные образовательные технологии и электронное обучение					
	Проектная работа	Кейс-анализ	Деловые игры	Проблемное обучение	Командная работа	Другие (указать, какие)	Сетевые учебные курсы	Виртуальные практикумы и тренажеры	Вебинары и видеоконференции	Асинхронные web-конференции и семинары	Совместная работа и разработка контента	Другие (указать, какие)
Р1		+		+	+							
Р2		+		+	+							
Р3		+		+	+							
Р4		+		+	+							
Р5		+		+	+							

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ (Приложение 1)
7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ (Приложение 2)

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (Приложение 3)

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

9.1.Рекомендуемая литература

9.1.1.Основная литература

1. Сизый, Сергей Викторович. Лекции по теории чисел : учеб. пособие для вузов / С. В. Сизый. — М. : ФИЗМАТЛИТ, 2007. — 192 с. : ил. — Рек. Науч.-метод. советом по мат. и мех. Учеб.-метод. об-ния ун-тов России. — Библиогр.: с. 189. — ISBN 978-5-9221-0741-9.

2. Виноградов, Иван Матвеевич. Основы теории чисел : учеб. пособие / И. М. Виноградов. — 11-е изд., стер. — СПб. [и др.] : Лань, 2006. — 176 с. — (Классическая учебная литература по математике) (Лучшие классические учебники, Математика).

9.1.2.Дополнительная литература

Арнольд, В.И. Цепные дроби : учеб. пособие — Москва : МЦНМО, 2009. — 40 с. https://www.mccme.ru/free-books/mmmf-lectures/book.14-full.pdf

9.2. Методические разработки

Сизый, Сергей Викторович. Лекции по теории чисел : учеб. пособие для вузов / С. В. Сизый. — М. : ФИЗМАТЛИТ, 2007. — 192 с. : ил. — Рек. Науч.-метод. советом по мат. и мех. Учеб.-метод. об-ния ун-тов России. — Библиогр.: с. 189. — ISBN 978-5-9221-0741-9.

9.3.Программное обеспечение

Не используется

9.4. Базы данных, информационно-справочные и поисковые системы

Общероссийский математический портал http://www.mathnet.ru/
Научная электронная библиотека eLibrary.ru http://www.elibrary.ru/
Сайт издательства Elsevier http://www.sciencedirect.com/
Сайт кафедры: http://kma.imkn.urfu.ru
Сайт кафедры: http://kadm.imkn.urfu.ru/pages.php?id=index
Сайт библиотеки университета http://lib.urfu.ru/

9.5.Электронные образовательные ресурсы

Не используются

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Аудитория с проектором

ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

6. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Весовой коэффициент значимости дисциплины –

6.2.Процедуры текущей и промежуточной аттестации по дисциплине

1.Лекции: коэффициент значимости совокупных результатов лекционных занятий – 1		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Контрольная работа № 1	**1, 1-10**	**20**
Контрольная работа № 2	**1, 1-17**	**20**
Домашняя работа № 1	**1, 1-10**	**20**
Домашняя работа № 2	**1, 1-14**	**20**
Домашняя работа № 3	**6, 1-17**	**20**
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0,4		
Промежуточная аттестация по лекциям – *зачет* **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0,6**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – не предусмотрены		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий – не предусмотрены		

6.3. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

Не предусмотрены

6.4. Коэффициент значимости семестровых результатов освоения дисциплины

Порядковый номер семестра по учебному плану, в котором осваивается дисциплина	**Коэффициент значимости результатов освоения дисциплины в семестре**
Семестр 4	1

ПРИЛОЖЕНИЕ 2
к рабочей программе дисциплины

7. ПРОЦЕДУРЫ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

Не применяется

ПРИЛОЖЕНИЕ 3
к рабочей программе дисциплины

8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

8.1. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ В РАМКАХ БРС

В рамках БРС применяются утвержденные на кафедре критерии оценивания достижений студентов по каждому контрольно-оценочному мероприятию. Система критериев оценивания, как и при проведении промежуточной аттестации по модулю, опирается на три уровня освоения компонентов компетенций: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	пороговый	**повышенный**	**высокий**
Знания	Студент демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Студент демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Студент может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Студент умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Студент умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Студент имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Студент имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Студент имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

8.2. КРИТЕРИИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПРИ ИСПОЛЬЗОВАНИИ НЕЗАВИСИМОГО ТЕСТОВОГО КОНТРОЛЯ

НТК не проводится

8.3. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.3.1. Примерные задания для проведения мини-контрольных в рамках учебных занятий

«не предусмотрено»

8.3.2. Примерные контрольные задачи в рамках учебных занятий

Раздел 1. Основы традиционной криптографии

Контрольная работа № 1.
Задание 1. Разложить число **51/41** в цепную дробь.

Задание 2. Представить квадратный корень из 5 в виде цепной дроби. .

Контрольная работа № 2.
Задание 1. Решить линейное сравнение **17*X=12 (mod 127)**

Задание 2. Найти наименьшее натуральное число, дающее
при делении на **21** остаток **1**,
при делении на **33** остаток **3**,
при делении на **6** остаток **5**.

Задание 3. Вычислить символ Якоби **(232/339)**.

8.3.3. Примерные контрольные кейсы

«не предусмотрено»

8.3.4. Перечень примерных вопросов для зачета

1. Цепные подходящие дроби.
2. Свойства подходящих дробей.
3. Квадратичные иррациональности. Теорема Лагранжа.
4. Теорема о наилучшем приближении.
5. Алгебраические числа.
6. Приближение алгебраических чисел рациональными. Теорема Лиувилля.
7. Теорема Эрмитта о трансцендентности числа e.
8. Полная и приведенная системы вычетов. Функция Эйлера и теорема Эйлера.
9. Линейные сравнения с одним неизвестным.
10. Системы линейных сравнений.
11. Символ Лежандра. Критерий Эйлера.
12. Свойства числа Лежандра.
13. Квадратичный закон взаимности.
14. Свойства числа Якоби.
15. Дзета-функция Римана.
16. Теорема Линдемана.

8.3.5. Перечень примерных вопросов для экзамена

«не предусмотрено»

8.3.6. Ресурсы АПИМ УрФУ, СКУД УрФУ для проведения тестового контроля в рамках текущей и промежуточной аттестации

«не используются»

8.3.7. Ресурсы ФЭПО для проведения независимого тестового контроля

«не используются»

8.3.8. Интернет-тренажеры

«не используются»

8.3.9. Примерные задания для домашних работ

Домашняя работа № 1.

Задание 1. Найти наибольший общий делитель, чисел 357 и 854.

Задание 2. Найти наибольший общий делитель, целых гауссовых чисел 23+71i и 13-4i.

Задание 3. Найти такие целые числа A и B, что 231A+499B=1.

Задание 4. Найти такие целые гауссовы числа A и B, что (19+13i)A+(11-7i)B=1 (или доказать, что таких нет).

Домашняя работа № 2.

Задание 1. Разложить число **251/133** в цепную дробь.

Задание 2. Представить корни квадратного уравнения $\mathbf{x^2+3x-1=0}$ в виде цепных дробей. .

Задание 3. Построить пять наилучших приближений числа $\mathbf{e^2}$.

Домашняя работа № 3.

Задание 1. Решить линейное сравнение **1679*X=3412 (mod 9849)**

Задание 2. Найти наименьшее натуральное число, дающее
при делении на **17** остаток **1**,
при делении на **21** остаток **2**,
при делении на **33** остаток **4**,
при делении на **6** остаток **1**.

Задание 3. Вычислить символ Якоби **(2728/22139)**.