МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

«СОГЛАСОВАНО»
Руководитель ОП

Добржинский Ю.В
(подпись) (Ф.И.О.)

«УТВЕРЖДАЮ»
И.о. заведующего кафедрой
информационной безопасности

Добржинский Ю.В
(подпись) (Ф.И.О.)

« 15 » июня 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Теоретико-числовые методы в криптографии
Специальность 10.05.01 Компьютерная безопасность
(Математические методы защиты информации)
Форма подготовки очная

курс 3 семестр 5
лекции 36 час.
практические занятия 36 час.
лабораторные работы 00 час.
в том числе с использованием МАО лек. 9 / пр. 12 / лаб. 00 час.
всего часов аудиторной нагрузки 72 час.
в том числе с использованием МАО 21 час.
самостоятельная работа 36 час.
в том числе на подготовку к экзамену 27 час.
контрольные работы (количество) не предусмотрены
курсовая работа / курсовой проект не предусмотрены
зачет не предусмотрен
экзамен 5 семестр

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования, утвержденного приказом Министерства образования и науки РФ от 01.12.2016 № 1512

Рабочая программа обсуждена на заседании кафедры информационной безопасности
протокол № 10 от « 15 » июня 2019 г.

И.о. заведующего кафедрой: Добржинский Ю.В., к.т.н., с.н.с.
Составитель: Боршевников А.Е., ассистент штатный

Владивосток
2019

Оборотная сторона титульного листа РПД

I. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

II. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

III. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

IV. Рабочая программа пересмотрена на заседании кафедры:

Протокол от «_____» ___ _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

ABSTRACT

Specialist's degree in 10.05.01 Computer Security
Specialization "Mathematical Methods for Information Security"
Course title: Networks and information transfer systems
Basic part of Block, 3 credits
Instructor: Borshevnikov A.E.
At the beginning of the course a student should be able to:
• ability to use regulatory legal documents in their professional activities (OPK-5);
• the ability to develop formal models of security policies, access control and information flow control policies in computer systems, taking into account information security threats (OPK-9);
Learning outcomes:
- (OPK-2) with the ability to correctly apply the apparatus of mathematical analysis, geometry, algebra, discrete mathematics, mathematical logic, theory of algorithms, theory

Course description:
The content of the discipline covers a range of issues related to the basic principles of construction and mathematical justification of cryptographic systems. The course of the discipline's lectures is built on step-by-step narration from the properties of the functions of estimating the complexity of arithmetic operations and elements of number theory to discrete logarithmic algorithms and testing numbers for simplicity.
Main course literature:
1. Глухов, М.М. Введение в теоретико-числовые методы криптографии [Электронный ресурс] : учебное пособие / М.М. Глухов, И.А. Круглов, А.Б. Пичкур, А.В. Черемушкин. — Электрон. дан. — Санкт-Петербург : Лань, 2011. — 400 с. — Режим доступа: https://e.lanbook.com/book/68466#book_name
2. Рябко, Б.Я. Основы современной криптографии и стеганографии [Электронный ресурс] : монография / Б.Я. Рябко, А.Н. Фионов. — Электрон. дан. — Москва : Горячая линия-Телеком, 2011. — 232 с. — Режим доступа: https://e.lanbook.com/book/5192#book_name
3. Червяков, Н.И. Применение искусственных нейронных сетей и системы остаточных классов в криптографии [Электронный ресурс] : монография / Н.И. Червяков, А.А. Евдокимов, А.И. Галушкин, И.Н. Лавриненко. — Электрон. дан. — Москва : Физматлит, 2012. — 280 с. — Режим доступа: https://e.lanbook.com/book/5300#book_name
Form of final control: *exam.*

Аннотация к рабочей программе дисциплины
«Теоретико-числовые методы в криптографии»

Курс учебной дисциплины «Теоретико-числовые методы в криптографии» разработана для студентов, обучающихся по специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в базовую часть дисциплин учебного плана Б1.Б.6.7.

Общая трудоемкость освоения дисциплины составляет 108 часов (3 з.е.). Учебным планом предусмотрены лекционные занятия (36 час.), практические занятия (36 час.), самостоятельная работа студентов (9 час. в том числе 27 часов на подготовку к экзамену). Дисциплина реализуется на 3 курсе в 5 семестре. Форма контроля по дисциплине – экзамен в 5 семестре.

Дисциплина "Теоретико-числовые методы в криптографии" логически и содержательно связана с такими курсами, как «Математический анализ», «Алгебра», «Дискретная математика», «Основы информационной безопасности».

Содержание дисциплины охватывает круг вопросов, связанных с базовыми принципами построения и математического обоснования криптографических систем.

Курс лекций дисциплины построен на пошаговом повествовании от свойств функций оценки сложности арифметических операций и элементов теории чисел к алгоритмам дискретного логарифмирования и тестирования чисел на простоту.

Дисциплина направлена на формирование общекультурных, общепрофессиональных и профессиональных компетенций выпускника.

Целью изучения дисциплины «Теоретико-числовые методы в криптографии» является формирование у студентов знаний в области современной алгоритмической теории чисел и ее применении в криптологии.

Задачи дисциплины:

- четкое осознание необходимости и важности математической подготовки для специалиста по компьютерной безопасности;
- ознакомление с основами классической и современной теории чисел, имеющими практические приложения к решению некоторых важных криптографических задач;
- умение давать строгую с математической точки зрения оценку применяемых алгоритмов.

Для успешного изучения дисциплины «Теоретико-числовые методы в криптографии» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность использовать нормативные правовые документы в своей профессиональной деятельности (ОПК-5);
- способностью разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации (ОПК-9);

В результате изучения данной дисциплины у студентов формируются следующие компетенции:

Код и формулировка компетенции	**Этапы формирования компетенции**	
(ОПК-2) способностью корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории	Знает	разделы курса «Математический анализ» необходимые для дальнейшего изучения курсов, функционального анализа, дифференциальных уравнений, дифференциальной геометрии, методов оптимизации, численных методов, теоретической механики, и других разделов математики, а также других дисциплин естественно-научного цикла
	Умеет	применять изученные математические методы при решении профессиональных задач и задач с практическим содержанием
	Владеет	математическим аппаратом, изученным в данном курсе и необходимым для дальнейшего

вероятностей, математической статистики, теории информации, теоретико-числовых методов		совершенствования профессиональной деятельности

Для формирования вышеуказанных компетенций в рамках дисциплины «Теоретико-числовые методы в криптографии» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах, собеседование по итогам выполнения практических заданий. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), конспект (ПР-7).

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Тема 1. Оценка сложности арифметических операций (7 час.)

Свойства функций оценки сложности. Сложность арифметических операций с целыми числами. Сложность алгоритма Евклида. Сложность операций в кольце вычетов.

Тема 2. Элементы теории чисел (7 час.)

Непрерывные дроби и их свойства. Квадратичные вычеты и невычеты. Теорема Чебышева о распределении простых чисел. Использование модульной арифметики. Вычисления с многочленами. Дискретное преобразование Фурье.

Тема 3. Факторизация целых чисел (7 час.)

Метод пробных делений. Факторизация Ферма. Алгоритм Диксона. Алгоритм Брилхарта-Моррисона. Метод квадратичного решета. Метод Полларда. Алгоритм Полларда-Штрассена. $(p-1)$-метод Полларда.

Тема 4. Алгоритмы дискретного логарифмирования (7 час.)

Метод Полига-Хеллмана. Шаги младенца и шаги гиганта. ρ-метод Полларда. λ-метод Полларда. Параллельный ρ-метод.

Тема 5. Тестирование чисел на простоту (8 час.)

Решето Эратосфена. Критерий Вильсона. Тест на основе малой теоремы Ферма. Тест Соловея-Штрассена. Тест Рабина-Миллера. Полиномиальный тест распознавания простоты.

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Тема 1. Реализуйте тесты Ферма и Миллера-Рабина и найдите с их помощью свидетелей делимости числа $2^{1024}-3$. **(9 час.)**

Тема 2. Напишите программу для $(P-1)$-метода факторизации. Насколько большие составные числа Ваша программа сможет разложить на множители? **(9 час.)**

Тема 3. Реализуйте ρ-метод Полларда и поэкспериментируйте с разными определениями детерминированных случайных блужданий. Какой из них наиболее эффективен? (Эффективность здесь означает более быстрое в среднем решение задачи о дискретных логарифмах). **(9 час.)**

Тема 4. Разработайте программу для параллельного метода Полларда решения задачи дискретного логарифмирования в конечных полях. Насколько сложную задачу дискретного логарифмирования Вы сможете решить с помощью этой программы в течение 24 часов? **(9 час.)**

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Название дисциплины» представлено в Приложении 1 и включает в себя:

план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;

характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

требования к представлению и оформлению результатов самостоятельной работы;

критерии оценки выполнения самостоятельной работы

IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Оценка сложности арифметических операций	ОПК-2	знает	собеседование (ОУ-1)	
			умеет	коллоквиум (ОУ-2)	
			владеет	конспект (ПР-7)	
2	Элементы теории чисел	ОПК-2	знает	собеседование (ОУ-1)	
			умеет	коллоквиум (ОУ-2)	
			владеет	конспект (ПР-7)	
3	Факторизация целых чисел	ОПК-2	знает	собеседование (ОУ-1)	
			умеет	коллоквиум (ОУ-2)	
			владеет	конспект (ПР-7)	
4	Алгоритмы дискретного логарифмирования	ОПК-2	знает	собеседование (ОУ-1)	
			умеет	коллоквиум (ОУ-2)	
			владеет	конспект (ПР-7)	
5	Тестирование чисел на простоту	ОПК-2	знает	собеседование (ОУ-1)	
			умеет	коллоквиум (ОУ-2)	
			владеет	конспект (ПР-7)	

Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 2.

V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература

1. Глухов, М.М. Введение в теоретико-числовые методы криптографии [Электронный ресурс] : учебное пособие / М.М. Глухов, И.А. Круглов, А.Б. Пичкур, А.В. Черемушкин. — Электрон. дан. — Санкт-Петербург : Лань, 2011. — 400 с. — Режим доступа: https://e.lanbook.com/book/68466#book_name

2. Рябко, Б.Я. Основы современной криптографии и стеганографии [Электронный ресурс] : монография / Б.Я. Рябко, А.Н. Фионов. — Электрон. дан. — Москва : Горячая линия-Телеком, 2011. — 232 с. — Режим доступа: https://e.lanbook.com/book/5192#book_name

3. Червяков, Н.И. Применение искусственных нейронных сетей и системы остаточных классов в криптографии [Электронный ресурс] : монография / Н.И. Червяков, А.А. Евдокимов, А.И. Галушкин, И.Н. Лавриненко. — Электрон. дан. — Москва : Физматлит, 2012. — 280 с. — Режим доступа: https://e.lanbook.com/book/5300#book_name

Дополнительная литература

1. Торстейнсон, П. Криптография и безопасность в технологии. NET [Электронный ресурс] / П. Торстейнсон, Г.А. Ганеш ; под ред. С. М. Молявко ; пер. с англ. В. Д. Хорева. — Электрон. дан. — Москва : Издательство "Лаборатория знаний", 2015. — 428 с. — Режим доступа: https://e.lanbook.com/book/70724#book_name

2. Глухов, М.М. Элементы теории обыкновенных представлений и характеров конечных групп с приложениями в криптографии [Электронный ресурс] : учебное пособие / М.М. Глухов, И.А. Круглов. — Электрон. дан. — Санкт-Петербург : Лань, 2015. — 176 с. — Режим доступа: https://e.lanbook.com/book/65044#book_name

3. Петров, А.А. Компьютерная безопасность. Криптографические методы защиты [Электронный ресурс] / А.А. Петров. — Электрон. дан. — Москва : ДМК Пресс, 2008. — 448 с. — Режим доступа: https://e.lanbook.com/reader/book/3027/#1

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Лекции Криптография [Электронный ресурс] режим доступа: https://habr.com/company/yandex/blog/324866/
2. Лекции теоретико-числовые методы [Электронный ресурс] Режим доступа: http://docplayer.ru/69224460-Teoretiko-chislovye-metody-v-kriptografii.html
3. Лекции теоретико-числовые методы в криптографии [Электронный ресурс] Режим доступа: http://window.edu.ru/resource/316/78316

Перечень информационных технологий

и программного обеспечения

Приморский край, г. Владивосток,	1) IBM SPSS Statistics Premium Campus

Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус L, ауд. L 607, Учебная аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от 18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно. 4) MathCad Education Universety Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно. 5) Corel Academic Site. Поставщик Софт Лайн Трейд. Договор ЭА-442-15 от 18.01.16 лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019. 6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18 лот 4. Срок действия договора 20.09.2018. Лицензия до 30.06.2020.

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Теория функции комплексной переменной», составляет 72 академических часов. На самостоятельную работу – 72 часов. При этом аудиторная нагрузка состоит из 36 лекционных часов и 36 часов практических занятий.

Обучающийся получает теоретические знания на лекционных занятиях, необходимые для последующего выполнения практических заданий. В ходе подготовки к лекциям должны использоваться источники из списка учебной литературы.

Студенту рекомендуется предварительно готовиться к лекции, используя ресурсы из списка, приведённого в разделе V, для более качественного освоения теоретического материала, а также возможности задать вопросы преподавателю.

При подготовке к практическим занятиям также необходимо повторить теоретический материал.

Промежуточная форма аттестации по данной дисциплине – экзамен. Вопросы к экзамену соответствуют темам, изучаемым на лекционных занятиях. Таким образом, при самостоятельной подготовке к экзамену студенту необходимо воспользоваться конспектами лекций, а также иными источниками из списка литературы для более глубокого понимания материала.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус L, ауд. L 607, Учебная аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 30) Оборудование: Доска аудиторная, переносной компьютер (ноутбук Lenovo) с сумкой – 1 шт

Приложение 1

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

по дисциплине «Теоретико-числовые методы в криптографии»
Специальность 10.05.01 Компьютерная безопасность
специализация «Математические методы защиты информации»
Форма подготовки очная

Владивосток
2019

План-график выполнения самостоятельной работы по дисциплине

№ п/п	Дата/сроки выполнения	Вид самостоятельной работы	Примерные нормы времени на выполнение	Форма контроля
1	1-17 недели обучения	Подготовка практических заданий (выполнение отчета по практическим заданиям 1-3)	9	Самостоятельные работы
2	18 неделя обучение	Подготовка к экзамену	27	Экзамен

Подготовка отчета к практическому заданию предполагает повторение лекционного материала и выполнение лабораторных работ по темам из Раздела II РПУД. В результате студент должен предоставить отчет о проделанной работе.

Самостоятельная работа при подготовке к экзамену и включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников и материалов по практическим занятиям.

Приложение 2

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Теоретико-числовые методы в криптографии»
Специальность 10.05.01 Компьютерная безопасность
специализация «Математические методы защиты информации»
Форма подготовки очная

Владивосток
2019

Паспорт ФОС

Код и формулировка компетенции	Этапы формирования компетенции	
(ОПК-2) способностью 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	Знает	разделы курса «Математический анализ» необходимые для дальнейшего изучения курсов, функционального анализа, дифференциальных уравнений, дифференциальной геометрии, методов оптимизации, численных методов, теоретической механики, и других разделов математики, а также других дисциплин естественно-научного цикла
	Умеет	применять изученные математические методы при решении профессиональных задач и задач с практическим содержанием
	Владеет	математическим аппаратом, изученным в данном курсе и необходимым для дальнейшего совершенствования профессиональной деятельности

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Оценка сложности арифметических операций	ОПК-2	знает	собеседование (ОУ-1)	
			умеет	коллоквиум (ОУ-2)	
			владеет	конспект (ПР-7)	
2	Элементы теории чисел	ОПК-2	знает	собеседование (ОУ-1)	
			умеет	коллоквиум (ОУ-2)	
			владеет	конспект (ПР-7)	
3	Факторизация целых чисел	ОПК-2	знает	собеседование (ОУ-1)	
			умеет	коллоквиум (ОУ-2)	

			владеет	конспект (ПР-7)	
4	Алгоритмы дискретного логарифмирования	ОПК-2	знает	собеседование (ОУ-1)	
			умеет	коллоквиум (ОУ-2)	
			владеет	конспект (ПР-7)	
5	Тестирование чисел на простоту	ОПК-2	знает	собеседование (ОУ-1)	
			умеет	коллоквиум (ОУ-2)	
			владеет	конспект (ПР-7)	

Шкала оценивания уровня сформированности компетенций

Код и формулировка компетенции	**Этапы формирования компетенции**		**критерии**	**показатели**
(ОПК-2) способностью осваивать методики использования программных средств для решения практических задач	знает (пороговый уровень)	методики организации исследовательских и проектных работ. Основные методы разработки программных моделей процессов и систем и применять их к исследованию вычислительных компонент и комплексов.	полнота и системность знаний	изложение полученных знаний полное, в соответствии с требованиями учебной программы; ошибки отсутствуют или несущественны, обучающийся способен самостоятельно исправить.
	умеет (продвинутый)	организовать исследовательские и проектные работы. Применять основные методы разработки программных моделей процессов и систем к	степень самостоятельности выполнения действия (умения); осознанность действия (умения).	обучающийся способен свободно строить модели простых неформализуемых задач самостоятельно; свободно отвечает на вопросы, касающиеся выполняемых действий.

		исследованию вычислительных компонент и комплексов.		
	владеет (высокий)	базовыми навыками организации исследовательских и проектных работ. Навыком разработки программных моделей процессов и систем.	степень умения отбирать и интегрировать имеющиеся знания и навыки исходя из поставленной цели, проводить самоанализ и самооценку.	обучающийся способен самостоятельно создать программную модель процессов и систем.

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

Промежуточная форма аттестации по данной дисциплине – экзамен.

Для допуска к экзамену в необходимо сдать все практические задания. В случае, если к дню проведения зачёта обучающийся не сдал какие-либо из практических заданий, он получает возможность сдать их на зачёте.

Экзамен проводится в форме собеседования (УО-1), вопросы соответствуют темам, изучаемым на лекционных занятия, и представлены далее в Приложении. Для подготовки к ответу на экзамене обучающийся получает 40 минут. В ходе подготовки обучающийся может составлять любые записи, однако оценивается прежде всего устный, а не письменный ответ.

При определении оценки ответа обучающегося как на экзамене, так и на практическом занятии учитываются:

- соблюдение норм литературной речи;

- полнота и содержательность ответа;

- умение привести примеры;

- умение пользоваться дополнительной литературой при подготовке к занятиям;

- соответствие представленной в ответах информации материалам лекций и учебной литературы, актуальным сведениям из информационных ресурсов Интернет.

Для получения «экзамена» ответ студента должен соответствовать следующим минимальным требованиям: полный ответ на 1 вопрос или частичный ответ на 2 вопроса; допускаются нарушения в последовательности изложения; демонстрируются поверхностные знания вопроса; имеются затруднения с выводами; допускаются нарушения норм литературной речи.

Оценка «не удовлетворительно» выставляется в случае если: обучающийся не ответил полно ни на один вопрос; материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний по дисциплине; имеются заметные нарушения норм литературной речи

Оценочные средства для промежуточной аттестации

1. Сложность алгоритма
2. Модели вычислений. Оценки функции сложности
3. Сложность операций сложения и вычитания целых чисел
4. Сложность операций умножения и деления целых чисел
5. Сложность операции возведения в степень целого числа
6. Сложность алгоритма Евклида
7. Расширенный алгоритм Евклида
8. Сложность операций сложения и вычитания в кольце вычетов
9. Сложность операции умножения в кольце вычетов
10. Сложность операций обращения и деления в кольце вычетов
11. Непрерывные дроби и их свойства. Теорема о фундаментальном соответствии
12. Представление действительных чисел непрерывными дробями
13. Квадратичные вычеты
14. Квадратичный закон взаимности Гаусса. Теорема Чебышева о распределении простых чисел
15. Модульная арифметика
16. Вычисления с многочленами. Алгоритм Руффини-Горнера
17. Дискретное преобразование Фурье
18. Определение факторизации целых чисел и метод пробных делений
19. Факторизация Ферма

20. Алгоритм факторизации Диксона
21. Алгоритм факторизации Брилхарта-Моррисона
22. Метод факторизации квадратичным решетом
23. Методы факторизации Полларда
24. Алгоритм факторизации Полларда-Штрассена
25. $(p-1)$-метод факторизации Полларда
26. Определение дискретного логарифмирования и метод Полига-Хеллмана
27. Дискретное логарифмирование. Шаги младенца и шаги гиганта
28. Дискретное логарифмирование. ρ-метод Полларда
29. Дискретное логарифмирование. λ-метод Полларда
30. Параллельный ρ-метод дискретного логарифмирования
31. Решето Эратосфена и критерий Вильсона
32. Тест простоты на основе малой теоремы Ферма
33. Тест простоты Соловея-Штрассена
34. Тест простоты Рабина-Миллера

Полиномиальный тест распознавания простоты

Оценочные средства для текущей аттестации

В качестве оценочных средств для текущей аттестации применяются конспект (ПР-7).

Конспект является показателем сформированности компетенции на пороговом уровне. Темы конспектов соответствуют темам теоретической части курса из Раздела II РПУД. Критерии оценки по данному виду оценочных средств представлены в таблице:

Оценка	Содержание конспекта
Отлично	Конспект содержит все понятия, термины, положения, изученные на лекции и/или с использованием основных источников литературы, а также содержит сведения из дополнительных источников.
Хорошо	Конспект содержит все понятия, термины, положения, изученные на лекции и/или с использованием основных источников литературы.
Удовлетворительно	Конспект содержит базовые понятия, термины, положения, изученные на лекции.
Неудовлетворительно	Конспект не содержит основных понятий, терминов, положений по данной теме.

Приложение 3

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«Дальневосточный федеральный университет»
(ДВФУ)

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по дисциплине «Теоретико-числовые методы в криптографии»
Специальность 10.05.01 Компьютерная безопасность
Специализация «Математические методы защиты информации»
Форма подготовки очная

Владивосток
2017

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Теоретико-числовые методы в криптографии», составляет 72 академических часов. На самостоятельную работу – 9 часов. При этом аудиторная нагрузка состоит из 36 лекционных часов и 36 часов практических занятий.

Обучающийся получает теоретические знания на лекционных занятиях, необходимые для последующего выполнения практических заданий. В ходе

подготовки к лекциям должны использоваться источники из списка учебной литературы.

Студенту рекомендуется предварительно готовиться к лекции, используя ресурсы из списка, приведённого в разделе V, для более качественного освоения теоретического материала, а также возможности задать вопросы преподавателю.

При подготовке к практическим занятиям также необходимо повторить теоретический материал.

Промежуточная форма аттестации по данной дисциплине – экзамен. Вопросы к зачету соответствуют темам, изучаемым на лекционных занятиях. Таким образом, при самостоятельной подготовке к зачету студенту необходимо воспользоваться конспектами лекций, а также иными источниками из списка литературы для более глубокого понимания материала.