


МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой
функционального анализа и операторных уравнений
наименование кафедры, отвечающей за реализацию дисциплины


Каменский М.И.
подпись, расшифровка подписи
26.06.2018г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.05 Теоретико-числовые алгоритмы в криптологии
Код и наименование дисциплины в соответствии с учебным планом

1. Код и наименование направления подготовки/специальности:

02.04.01 Математика и компьютерные науки

2. Профиль подготовки/специализация: Математические основы компьютерных наук

3. Квалификация (степень) выпускника: магистр

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины: функционального анализа и операторных уравнений

6. Составители программы: Завгородний Михаил Григорьевич
(ФИО, ученая степень, ученое звание)
Канд. физ-мат. наук, доцент

7. Рекомендована: НМС математического факультета, протокол №0500-07 от 03.07.2018

8. Учебный год: 2018-2019 Семестр(ы): 1

9. Цели и задачи учебной дисциплины: Цель курса - дать студентам математический аппарат для разработки и анализа криптографических алгоритмов. А также оценки их сложности.

Основными задачами изучения дисциплины являются:

- изучение алгоритмов арифметических операций с большими целыми числами в позиционной системе счисления и в кольце вычетов
- изучение алгоритмов возведения в степень и нахождения целой части корня;
- изучение алгоритмов нахождения НОД и обратного элемента в кольце вычетов;
- изучение алгоритмов факторизации числа.

10. Место учебной дисциплины в структуре ООП: (блок Б1, базовая или вариативная часть, к которой относится дисциплина; требования к входным знаниям, умениям и навыкам; дисциплины, для которых данная дисциплина является предшествующей))

Дисциплина входит в вариативную часть цикла естественно-научных дисциплин. Для изучения и освоения дисциплины нужны знания из курсов алгебры и теории чисел, технология программирования и работа на ЭВМ. Знания и умения, приобретенные студентами в результате изучения дисциплины, будут использоваться в курсах «Программирование криптографических алгоритмов», «Математические основы криптологии», при выполнении дипломных работ, связанных с математическим моделированием в области защиты информации.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):

Компетенция		Планируемые результаты обучения
Код	Название	
ОК-3	готовность к саморазвитию, самореализации, использованию творческого потенциала	<p>знать: алгоритмы арифметических операций с большими целыми числами и в кольце вычетов; алгоритмы быстрого умножения и возведения в степень; алгоритмы нахождения НОД и его линейного представления; алгоритмы нахождения обратного элемента; алгоритмы проверки числа на простоту и разложения составного числа на простые сомножители.</p> <p>уметь: реализовать алгоритмы в виде блок-схем;</p> <p>владеть (иметь навык(и)): разработки алгоритмов для решения задач модулярной арифметики больших чисел.</p>
ОПК-3	готовность самостоятельно создавать прикладные программные средства на основе современных информационных технологий и сетевых ресурсов	<p>знать: алгоритмы арифметических операций с большими целыми числами и в кольце вычетов; алгоритмы быстрого умножения и возведения в степень; алгоритмы нахождения НОД и его линейного представления; алгоритмы нахождения обратного элемента; алгоритмы проверки числа на простоту и разложения составного числа на простые сомножители.</p> <p>уметь: реализовать алгоритмы в виде блок-схем;</p> <p>владеть (иметь навык(и)): разработки алгоритмов для решения задач модулярной арифметики больших чисел.</p>

12. Объем дисциплины в зачетных единицах/час.(в соответствии с учебным планом) — 2/72.

Форма промежуточной аттестации(зачет/экзамен) зачет.

13. Виды учебной работы

Вид учебной работы	Трудоемкость (часы)	
	Всего	По семестрам
		сем. № 1 (9)
Аудиторные занятия	32	32
в том числе: лекции	0	0
практические	0	0
лабораторные	32	32
Самостоятельная работа	40	40
Итого:	72	72

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1	Предмет и задачи курса.	Структура курса. Терминология. Оценка сложности алгоритмов обработки числовых данных.
2	Алгоритмы арифметических операций с большими целыми числами и оценка их сложности	Классические алгоритмы сложения, вычитания и умножения больших целых чисел в позиционной системе счисления. Классический алгоритм деления больших целых чисел с остатком. О способах выбора очередной цифры частного алгоритма деления с остатком.
3	Быстрые алгоритмы умножения целых чисел, возведения в степень и их сложность. Алгоритмы нахождения целой части корня.	Алгоритм Карацубы-Офмана умножения целых чисел и его сложность. Сложность других быстрых алгоритмов умножения. Сложность алгоритма возведения в степень. Целочисленные алгоритмы извлечения квадратного корня и корня n -ой степени.
4	Алгоритмы нахождения НОД двух чисел и его сложность.	Алгоритм Евклида и бинарный алгоритм нахождения НОД целых чисел. Оценка их сложности. Расширенный алгоритм Евклида и расширенный бинарный алгоритм. Алгоритм нахождения линейного представления НОД.
5	Алгоритмы умножения и нахождения обратного элемента в кольце вычетов.	Алгоритм Монтгомери. Алгоритмы нахождения обратного элемента на основе расширенного алгоритма Евклида, расширенного бинарного алгоритма и малой теоремы Ферма.
6	Проблемы простоты числа.	Вероятностные алгоритмы проверки простоты числа.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)			
		Лекции	Лабораторные	Самостоятельная работа	Всего

1	Предмет и задачи курса.	-	2	2	4
2	Алгоритмы арифметических операций с большими целыми числами и оценка их сложности	-	6	8	14
3	Быстрые алгоритмы умножения целых чисел, возведения в степень и их сложность. Алгоритмы нахождения целой части корня.	-	6	6	12
4	Алгоритмы нахождения НОД двух чисел и его сложность.	-	6	10	16
5	Алгоритмы умножения и нахождения обратного элемента в кольце вычетов.	-	6	10	16
6	Проблемы простоты числа.	-	6	4	10
	Итого	0	32	40	72

14. Методические указания для обучающихся по освоению дисциплины

(рекомендации обучающимся по освоению дисциплины: работа с конспектами лекций, презентационным материалом, выполнение практических заданий, тестов, заданий текущей аттестации и т.д.)

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины (список литературы оформляется в соответствии с требованиями ГОСТ и используется общая сквозная нумерация для всех видов источников)

№ п/п	Источник
1	Кнут, Дональд Эрвин. Искусство программирования : Учебное пособие / Дональд Эрвин Кнут ; Под общ. ред. Ю.В. Козаченко ; Пер. с англ. и ред.: Л.Ф. Козаченко, В.Т. Тертышного, И.В. Красикова. — М. : Вильямс, 2000-. Т. 2: Получисленные алгоритмы. — 3-е изд. — 2000. — 828 с. : ил.
2	Василенко, Олег Николаевич. Теоретико-числовые алгоритмы в криптографии / О.Н. Василенко ; Ин-т проблем информационной безопасности МГУ. — М. : МЦНМО, 2003. — 325 с.
3	Майорова С.П. Алгебра : учебное пособие / С.П. Майорова, М.Г. Завгородний. – Воронеж : ГОУВПО «Воронеж. гос. техн. ун-т», 2007. – Ч. 2 – 130 с.
4	Майорова С.П. Алгебра : учебное пособие / С.П. Майорова, М.Г. Завгородний. – Воронеж : ГОУВПО «Воронеж. гос. техн. ун-т», 2008. – Ч. 3 – 102 с.

* Вначале указываются ЭБС, с которыми имеются договора у ВГУ, затем открытые электронно-образовательные ресурсы

16. Перечень учебно-методического обеспечения для самостоятельной работы (учебно-методические рекомендации, пособия, задачки, методические указания по выполнению практических (контрольных) работ и др.)

№ п/п	Источник
5	Кнут, Дональд Эрвин. Искусство программирования для ЭВМ : [в 3 т.] / Д. Кнут. — М. : Мир, 1976 - Т. 2: Получисленные алгоритмы / пер. с англ. Т.П. Бабенко, Э.Т. Белаги и Л.В. Майорова ; под ред. К.И. Бабенко. — 1977. — 723,[1] с. : ил., табл.
6	Ахо, Альфред В. Структуры данных и алгоритмы : [Учебное пособие] / Альфред В. Ахо, Джон Э. Хопкрофт, Джеффри Д. Ульман ; Пер. с англ. и ред. А.А. Минько. — М. и др. : Вильямс, 2001. — 382 с. : ил., табл.

17. Информационные технологии, используемые для реализации учебной дисциплины, включая программное обеспечение и информационно-справочные системы (при необходимости)

18. Материально-техническое обеспечение дисциплины:

(при использовании лабораторного оборудования указывать полный перечень, при большом количестве оборудования можно вынести данный раздел в приложение к рабочей программе)

Лекционная аудитория (доска, мел, маркеры), компьютерные классы для проведения лабораторных работ, мультимедийный проектор.

Компьютерный класс (14-15 компьютеров + программное обеспечение)

19. Фонд оценочных средств:

19.2 Описание критериев и шкалы оценивания компетенций (результатов обучения) при промежуточной аттестации

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в форме лабораторных работ и контрольной работы.

Промежуточная аттестация проводится в форме и включает в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и практическое задание, позволяющее оценить степень сформированности умений и навыков.

При оценивании используется следующая шкала:

5 баллов ставится, если обучающийся демонстрирует полное соответствие знаний, умений, навыков приведенным в таблицах показателям, свободно оперирует приобретенными знаниями, умениями, применяет их при решении практических задач;

4 балла ставится, если обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач;

3 балла ставится, если обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач;

2 балла ставится, если обучающийся демонстрирует явное несоответствие знаний, умений, навыков приведенным в таблицах показателям.

При сдаче зачета

оценка «зачтено» - 3-5 баллов

оценка «незачтено» - 0-2 балла

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
<i>Обучающийся в полной мере владеет понятийным аппаратом в области построения алгоритмов модулярной арифметики, способен иллюстрировать ответ примерами, фактами, применять теоретические знания для поставленных задач.</i>	<i>Повышенный уровень</i>	<i>Зачтено</i>
<i>У обучающегося сформированы знания, умения и навыки в области построения алгоритмов; он способен иллюстрировать ответ примерами, фактами, применять теоретические знания для решения практических задач; но допускает отдельные несущественные пробелы в своих знаниях, допускает ошибки при выполнении практических задач.</i>	<i>Базовый уровень</i>	<i>Зачтено</i>
<i>У обучающегося сформированы неполные знания, умения и</i>	<i>Пороговый</i>	<i>Зачтено</i>

навыки; он допускает отдельные существенные пробелы в своих знаниях, допускает существенные ошибки при выполнении практических задач.	уровень	
Сформированы лишь фрагментарные знания, умения и навыки или знания, умения и навыки отсутствуют	–	Не зачтено

19.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие этапы формирования компетенций в процессе освоения образовательной программы

Пример КИМ № 1

УТВЕРЖДАЮ
Заведующий кафедрой функционального
анализа и операторных уравнений

_____ Каменский М.И.
подпись, расшифровка подписи

Направление подготовки / специальность 02.04.01 Математика и компьютерные науки

Дисциплина Б1.В.ОД.5 Теоретико-числовые алгоритмы криптологии

Форма обучения _____ очная _____

очное, очно-заочное, заочное

Вид контроля _____ зачет _____

экзамен, зачет

Вид аттестации _____ промежуточная _____

текущая, промежуточная

Контрольно-измерительный материал № _____

1. Алгоритм Монтомгери умножения в кольцах вычетов. Оценка сложности алгоритма умножения в кольцах вычетов.

2. Алгоритмы вычисления НОД. Оценка сложности этих алгоритмов.

Преподаватель _____
подпись расшифровка подписи

Пример контрольного задания (вариант задания)

Контрольная работа

по дисциплине «Теоретико-числовые алгоритмы криптологии»

Вариант № ____

1. Составьте алгоритм возведения в квадрат числа, имеющего не более ста десятичных разрядов. Оцените его сложность.