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
26.06.2018 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.Б.4 Программирование криптографических алгоритмов
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: _____

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 №0500-06 от 03.07.2018
(наименование рекомендующей структуры, дата, номер протокола)

8. Учебный год: *2018-2019* **Семестр(ы):** 2

9.Цели и задачи учебной дисциплины:

Целью изучения предмета «Программирование криптографических алгоритмов» является приобретение основных знаний и умений по программированию алгоритмов криптографии и компьютерной алгебры, приобретение навыков по составлению эффективных алгоритмов для решения типовых задач модулярной арифметики и последующей их реализации в форме программы (программ).

Основными задачами изучения дисциплины являются:

- изучение быстрых алгоритмов сложения, умножения и возведения в степень больших целых чисел и реализация этих алгоритмов в виде программ;
- изучение эффективных алгоритмов и составление программ нахождения НОД и обратного элемента в кольце вычетов;
- составление программ проверки чисел на простоту и факторизации чисел.

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 курсе «Математические основы криптологии» и 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	
ОПК- 1	способность находить, формулировать и решать актуальные и значимые проблемы фундаментальной и прикладной математики	**знать:** основные алгоритмы криптографии и компьютерной алгебры, а также алгоритмы криптоанализа текстов, зашифрованных методами с симметричным и асимметричным ключами; **уметь:** реализовать алгоритмы криптографии и криптоанализа в виде эффективных программ; использовать полученные знания для организации секретной переписки; **владеть** (иметь навык(и))**:** разработки алгоритмов и программ для решения задач модулярной арифметики больших чисел.
ОПК- 2	способность создавать и исследовать новые математические модели в естественных науках	**знать:** основные алгоритмы криптографии и компьютерной алгебры, а также алгоритмы криптоанализа текстов, зашифрованных методами с симметричным и асимметричным ключами; **уметь:** реализовать алгоритмы криптографии и криптоанализа в виде эффективных программ; использовать полученные знания для организации секретной переписки; **владеть** (иметь навык(и))**:** разработки алгоритмов и программ для решения задач модулярной арифметики больших чисел.
ПК- 1	способность к интенсивной научно-исследовательской	**знать:** основные алгоритмы криптографии и компьютерной алгебры, а

	работе	также алгоритмы криптоанализа текстов, зашифрованных методами с симметричным и асимметричным ключами; **уметь:** реализовать алгоритмы криптографии и криптоанализа в виде эффективных программ; использовать полученные знания для организации секретной переписки; **владеть** (иметь навык(и))**:** разработки алгоритмов и программ для решения задач модулярной арифметики больших чисел.

12. Объем дисциплины в зачетных единицах/час.(*в соответствии с учебным планом)* **— 3/108.**

Форма промежуточной аттестации*(зачет/экзамен)* *зачет.*

13. Виды учебной работы

Вид учебной работы	Трудоемкость (часы)	
	Всего	По семестрам
		сем. № 2 (10)
Аудиторные занятия	*42*	*42*
в том числе: лекции	*16*	*16*
практические	*0*	*0*
лабораторные	*32*	*32*
Самостоятельная работа	*60*	*60*
Итого:	*108*	*108*

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1	Предмет и задачи курса. Программирование быстрых алгоритмов арифметических операций с большими целыми числами	Структура курса. Терминология. Программы, основанные на алгоритме Карацубы-Офмана и рекурсивном алгоритме возведения в степень. Улучшение схемы возведения в степень.
2	Программирование быстрых алгоритмов нахождения НОД.	Изучение бинарного алгоритма нахождения НОД и составление программы на его основе. Программа нахождения линейного представления НОД.
3	Быстрые алгоритмы умножения и возведения в степень целых чисел в кольце вычетов.	Теорема Монтгомери. Алгоритм Монтгомери умножения целых чисел в кольце вычетов. Программы умножения и возведения в степень, основанные на алгоритме Монтгомери
4	Алгоритмы нахождения обратного элемента в кольце вычетов.	Алгоритмы нахождения обратного элемента на основе бинарного алгоритма нахождения НОД и малой теоремы Ферма. Программы нахождения обратного элемента в кольце вычетов.
5	Методы распознавания простых и составных чисел	Метод пробных делителей, метод Ферма, метод Лемана. $(n \pm 1)$ -методы проверки простоты чисел и построения больших простых чисел. Программы, составленные на основе этих методов.

6	Вероятностные алгоритмы проверки простоты числа.	Теоремы Соловея-Штрассена и Миллера-Рабина. Программы, составленные на основании тестов Соловея-Штрассена и Миллера-Рабина.
7	Субэкспоненциальные методы проверки простоты числа.	Знакомство с алгоритмом Ленстры.

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. Программирование быстрых алгоритмов арифметических операций с большими целыми числами	4	2	4	10
2	Программирование быстрых алгоритмов нахождения НОД.	2	4	8	14
3	Быстрые алгоритмы умножения и возведения в степень целых чисел в кольце вычетов.	2	6	8	16
4	Алгоритмы нахождения обратного элемента в кольце вычетов.	2	6	10	18
5	Методы распознавания простых и составных чисел.	2	8	18	28
6	Вероятностные алгоритмы проверки простоты числа.	2	4	8	14
7	Субэкспоненциальные методы проверки простоты числа.	2	2	4	8
	Итого	16	32	60	108

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, задачники, 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)

№ п/п	Источник
1	*www.fstec.ru, www.securitylab.ru , www.cyberpol.ru , www.azi.ru , www.infotecs.ru , www.infosec.ru , www.infoforum.ru , www.cnews.ru , www.brighttalk.com , www.coresecurity.com .*

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), Компьютерный класс (14-15 компьютеров + программное обеспечение) мультимедийный проектор.

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 «отлично» - 5 баллов
оценка «хорошо» - 4 балла
оценка «удовлетворительно» - 3 балла
оценка «неудовлетворительно» - 2 балла.

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся в полной мере владеет понятийным аппаратом в области программирования и технологии работы на ЭВМ, способен иллюстрировать ответ примерами, фактами, применять теоретические знания для решения практических задач программирования, СУБД и сетевых технологий.	*Повышенный уровень*	*Отлично*
У обучающегося сформированы знания, умения и навыки программирования и технологии работы на ЭВМ; 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.	*Базовый уровень*	*Хорошо*
У обучающегося сформированы неполные знания, умения и навыки; он допускает отдельные существенные пробелы в своих знаниях, допускает существенные ошибки при выполнении практических задач.	*Пороговый уровень*	*Удовлетвори-тельно*
Сформированы лишь фрагментарные знания, умения и навыки или знания, умения и навыки отсутствуют	–	*Неудовлетвори-тельно*

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.Б.2.2 Дополнительные главы программирования

Форма обучения _____очная_____
очное, очно-заочное, заочное
Вид контроля _____зачет_____
экзамен, зачет
Вид аттестации _____промежуточная_____
текущая, промежуточная

Контрольно-измерительный материал № ___

1. Программирование умножения в кольцах вычетов. Алгоритм Монтгомери. Оценка сложности алгоритма умножения в кольцах вычетов.

2. Программирование алгоритмов вычисления дискретных логарифмов в конечном поле. Оценка сложности этих алгоритмов.

Преподаватель _____ _____.
подпись расшифровка подписи

Пример контрольного задания (вариант задания)

Контрольная работа
по дисциплине «Дополнительные главы программирования»
Вариант №___

1. Напишите программу возведения в квадрат числа, имеющего не более ста десятичных разрядов.
2. Оцените сложность алгоритма возведения в квадрат.