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

УТВЕРЖДАЮ

Заведующий кафедрой
цифровых технологий

Кургалин С. Д.

28.02.2022 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.В.ДВ.04.01 Теоретико-числовые методы в криптографии

1. Код и наименование направления подготовки:
02.04.01 Математика и компьютерные науки

2. Профиль подготовки:
Компьютерное моделирование и искусственный интеллект

3. Квалификация выпускника:
Магистр

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины:
кафедра цифровых технологий

6. Составители программы:
Кургалин Сергей Дмитриевич, д.ф.-м.н., профессор

Залыгаева Марина Евгеньевна, ст. преподаватель

7. Рекомендована:
НМС ФКН (протокол № 3 от 25.02.2022)

8. Учебный год: 2022-2023 **Семестр:** 1

9. **Цели и задачи учебной дисциплины**

Целями освоения учебной дисциплины являются: формирование систематизированных знаний в области теории сравнений и усвоение студентами теоретико-числовых методов в криптографии.

Задачи учебной дисциплины:

– изучить базовые теоретико-числовые методы криптографии;

– овладеть умением применять изученные методы для решения практических задач;

– развить навыки разработки и реализации криптографических алгоритмов на базе языков и пакетов прикладных программ моделирования.

10. Место учебной дисциплины в структуре ООП:

Часть, формируемая участниками образовательных отношений, блок Б1. Для успешного освоения дисциплины необходимо предварительное изучение следующих разделов математики: алгебра.

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

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ПК-1	Способен демонстрировать фундаментальные знания математических и естественных наук, программирования и информационных технологий.	ПК-1.1	Обладает фундаментальными знаниями, полученными в области математических и (или) естественных наук, программирования и информационных технологий	Знает основные понятия и факты в области теоретико-числовых методов в криптографии
		ПК-1.2	Умеет находить, формулировать и решать стандартные задачи в собственной научно- исследовательской деятельности в области программирования и информационных технологий	Умеет формулировать и доказывать теоремы, самостоятельно решать задачи теоретико-числовых методов в криптографии
		ПК-1.3	Имеет практический опыт научно-исследовательской деятельности в области программирования и информационных технологий	Владеет навыками практического использования теоретико-числовых методов в криптографии при решении различных задач
ПК-8	Способен создавать и исследовать новые математические модели в естественных науках, промышленности и	ПК-8.1	Знает основные методы проектирования и производства программного продукта, принципы построения, структуры и приемы работы с инструментальными средствами, поддерживающими	Знает методы проектирования криптографических систем

	бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники		создание программных продуктов и программных комплексов, их сопровождения, администрирования и развития (эволюции)	
		ПК-8.2	Умеет использовать методы проектирования и производства программного продукта, принципы построения, структуры и приемы работы с инструментальными средствами, поддерживающими создание программного продукта	Умеет выбирать подходящие методы криптографии для проектирования программных продуктов
		ПК-8.3	Имеет практический опыт применения указанных выше методов и технологий	Владеет навыками применения методов криптографической защиты для решения задач профессиональной деятельности
ПК-9	Способен использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования	ПК-9.1	Владеет современными методами разработки и реализации алгоритмов математических моделей на базе языков и пакетов прикладных программ моделирования	Знает основные криптографические алгоритмы
		ПК-9.2	Умеет разрабатывать и реализовывать алгоритмы математических моделей на базе языков и пакетов прикладных программ моделирования	Умеет адаптировать существующие и разрабатывать новые алгоритмы для решения задач криптографии
		ПК-9.3	Имеет практический опыт разработки и реализации алгоритмов на базе языков и пакетов прикладных программ моделирования	Владеет навыками реализации криптографических алгоритмов на базе языков и пакетов прикладных программ моделирования

12. Объем дисциплины в зачетных единицах/час — 3/108.

Форма промежуточной аттестации: зачет с оценкой

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость	
		Всего	По семестрам
			1 семестр
Аудиторные занятия		54	54
в том числе:	лекции	18	18
	практические		

лабораторные	36	36
Самостоятельная работа	54	54
в том числе: курсовая работа (проект)		
Форма промежуточной аттестации (зачет с оценкой)		
Итого:	108	108

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК*
1. Лекции			
1.1	Основные понятия криптографии	Шифр, зашифровывание, расшифровывание, дешифрование. Исторические примеры шифров. Криптосистемы без передачи ключей. Криптосистемы с открытым ключом	https://edu.vsu.ru/course/view.php?id=10097
1.2	Теория сравнений	Простые числа и факторизация. Алгоритм Евклида. Сравнения по модулю. Теорема Эйлера. Сравнения с одной переменной. Сравнения по простому модулю	https://edu.vsu.ru/course/view.php?id=10097
1.3	Развитие методов решета	Решето Эратосфена. Методы решета Бруна, Бухштаба, Сельберга. Метод весового решета	https://edu.vsu.ru/course/view.php?id=10097
2. Практические занятия			
2.1	Основные понятия криптографии	Шифр, зашифровывание, расшифровывание, дешифрование. Исторические примеры шифров. Криптосистемы без передачи ключей. Криптосистемы с открытым ключом	https://edu.vsu.ru/course/view.php?id=10097
2.2	Теория сравнений	Простые числа и факторизация. Алгоритм Евклида. Сравнения по модулю. Теорема Эйлера. Сравнения с одной переменной. Сравнения по простому модулю	https://edu.vsu.ru/course/view.php?id=10097
2.3	Развитие методов решета	Решето Эратосфена. Методы решета Бруна, Бухштаба, Сельберга. Метод весового решета	https://edu.vsu.ru/course/view.php?id=10097

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (количество часов)			
		Лекции	Практические /Лабораторные	Самостоятельная работа	Всего
1	Основные понятия криптографии	4	8	12	24
2	Теория сравнений	6	12	18	36
3	Развитие методов решета	8	16	24	48
	Итого:	18	36	54	108

14. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины складывается из аудиторной работы (учебной деятельности, выполняемой под руководством преподавателя) и внеаудиторной работы (учебной деятельности, реализуемой обучающимся самостоятельно).

Аудиторная работа состоит из работы на лекциях и выполнения практических заданий в объёме, предусмотренном учебным планом. Лекция представляет собой последовательное и систематическое изложение учебного материала, направленное на знакомство обучающихся с основными понятиями и теоретическими положениями изучаемой дисциплины.

Лекционные занятия формируют базу для практических занятий, на которых полученные теоретические знания применяются для решения конкретных практических задач. Обучающимся для успешного освоения дисциплины рекомендуется вести конспект лекций и практических занятий.

Самостоятельная работа предполагает углублённое изучение отдельных разделов дисциплины с использованием литературы, рекомендованной преподавателем, а также конспектов лекций, конспектов практических занятий. В качестве плана для самостоятельной работы может быть использован раздел 13.1 настоящей рабочей программы, в котором зафиксированы разделы дисциплины и их содержание. В разделе 13.2 рабочей программы определяется количество часов, отводимое на самостоятельную работу по каждому разделу дисциплины. Большее количество часов на самостоятельную работу отводится на наиболее трудные разделы дисциплины. Для самостоятельного изучения отдельных разделов дисциплины используется перечень литературы и других ресурсов, перечисленных в пунктах 15 и 16 настоящей рабочей программы. Обязательным элементом самостоятельной работы является выполнение домашнего задания.

Успешность освоения дисциплины определяется систематичностью и глубиной аудиторной и внеаудиторной работы обучающегося.

При использовании дистанционных образовательных технологий и электронного обучения требуется выполнять все указания преподавателей, вовремя подключаться к онлайн-занятиям, ответственно подходить к заданиям для самостоятельной работы.

В рамках дисциплины предусмотрено проведение трёх текущих аттестаций за семестр. Результаты текущей успеваемости учитываются при выставлении оценки по

промежуточной аттестации в соответствии с положением П ВГУ 2.1.04.16–2019 «Положение о текущей и промежуточной аттестации знаний, умений и навыков обучающихся на факультете компьютерных наук Воронежского государственного университета с использованием балльно-рейтинговой системы».

Обучение лиц с ограниченными возможностями здоровья осуществляется с учетом их индивидуальных психофизических особенностей и в соответствии с индивидуальной программой реабилитации. Для лиц с нарушением слуха при необходимости допускается присутствие на лекциях и практических занятиях ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки на зачете может быть увеличено. Для лиц с нарушением зрения допускается аудиальное предоставление информации (например, с использованием программ-синтезаторов речи), а также использование на лекциях звукозаписывающих устройств (диктофонов и т.д.). На лекциях и практических занятиях при необходимости допускается присутствие ассистента. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам. При необходимости время подготовки на экзамене может быть увеличено. Для лиц с нарушениями опорно-двигательного аппарата при необходимости допускается присутствие ассистента на лекциях и практических занятиях. Промежуточная аттестация для лиц с нарушениями опорно-двигательного аппарата проводится на общих основаниях, при необходимости процедура экзамена может быть реализована дистанционно.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	Авдошин, С. М. Дискретная математика. Модулярная алгебра, криптография, кодирование [Электронный ресурс] / Авдошин С. М., Набебин А. А. — Москва : ДМК Пресс, 2017 .— 352 с. — Книга из коллекции ДМК Пресс - Информатика .— ISBN 978-5-97060-408-3 .— <URL:https://e.lanbook.com/book/93575>.
2	Теоретико-числовые методы в криптографии : практикум / ; авт.-сост. Ф. Б. Тебуева ; авт.-сост. В. О. Антонов ; Министерство образования и науки РФ ; Федеральное государственное автономное образовательное учреждение высшего образования «Северо-Кавказский федеральный университет». — Ставрополь : СКФУ, 2017. — 107 с. : ил. — Библиогр. в кн. — http://biblioclub.ru/. — <URL: http://biblioclub.ru/index.php?page=book&id=483838>.
3	Кнауб, Л. В. Теоретико-численные методы в криптографии : учебное пособие / Л.В. Кнауб, Е.А. Новиков, Ю.А. Шитов ; Министерство образования и науки Российской Федерации ; Сибирский Федеральный университет .— Красноярск : Сибирский федеральный университет, 2011 .— 160 с. — http://biblioclub.ru/ .— ISBN 978-5-7638-2113-7 .— <URL:http://biblioclub.ru/index.php?page=book&id=229582>.

б) дополнительная литература:

№ п/п	Источник
1	Романьков, В.А. Алгебраическая криптография / В.А. Романьков. - Омск : Омский государственный университет, 2013. - 136 с. - ISBN 978-5-7779-1600-6 ; То же [Электронный ресурс]. - <URL: http://biblioclub.ru/index.php?page=book&id=238045>
2	Ниссенбаум, О. В. Теоретико-числовые методы в криптографии. Сборник заданий: учебно-методическое пособие для студентов специальностей «Компьютерная безопасность» и «Информационная безопасность автоматизированных систем»,

	направления «Информационная безопасность» : учебно-методическое пособие. Часть 3 / О.В. Ниссенбаум ; Министерство образования и науки Российской Федерации ; ФГБОУ ВПО Тюменский государственный университет ; Институт математики и компьютерных наук ; Кафедра информационной безопасности .— Тюмень : Издательство Тюменского государственного университета, 2014 .— 40 с. : ил. — Библиогр. в кн .— http://biblioclub.ru/ .— <URL:http://biblioclub.ru/index.php?page=book&id=567498>.

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет):

№ п/п	Ресурс
1	ЗНБ ВГУ: https://lib.vsu.ru/
2	Электронно-библиотечная система "Университетская библиотека online": http://biblioclub.ru/
3	Электронно-библиотечная система "Лань": https://e.lanbook.com/
4	Электронно-библиотечная система "Консультант студента": http://www.studmedlib.ru
5	Электронный университет ВГУ: https://edu.vsu.ru/

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Авдошин, С. М. Дискретная математика. Модулярная алгебра, криптография, кодирование [Электронный ресурс] / Авдошин С. М., Набебин А. А. — Москва : ДМК Пресс, 2017 .— 352 с. — Книга из коллекции ДМК Пресс - Информатика .— ISBN 978-5-97060-408-3 .— <URL:https://e.lanbook.com/book/93575>.

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ, электронное обучение (ЭО), смешанное обучение)

При реализации дисциплины могут использоваться технологии электронного обучения и дистанционные образовательные технологии на базе портала edu.vsu.ru, а также другие доступные ресурсы сети Интернет.

18. Материально-техническое обеспечение дисциплины

Аудитория для лекционных занятий: мультимедиа-проектор, экран для проектора, компьютер с выходом в сеть «Интернет». Специализированная мебель (столы ученические, стулья, доска). Программное обеспечение: LibreOffice v.5-7, программа для просмотра файлов формата pdf, браузер.

Аудитория для лабораторных занятий: компьютеры с выходом в сеть «Интернет» и доступом к электронным библиотечным системам, специализированная мебель (столы ученические, стулья, доска). Программное обеспечение: LibreOffice v.5-7, программа для просмотра файлов формата pdf, браузер.

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция	Индикатор(ы) достижения компетенции	Оценочные средства
1	Разделы 1-3	ПК-1 ПК-8 ПК-9	ПК-1.1 ПК-1.2 ПК-1.3 ПК-8.1 ПК-8.2 ПК-8.3 ПК-9.1 ПК-9.2 ПК-9.3	Лабораторная работа
Промежуточная аттестация форма контроля – зачет				Вопросы к зачёту

20. Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1. Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств: лабораторная работа

Перечень лабораторных работ

1. Криптосистема без передачи ключей.
2. Сравнения первой степени с одной переменной.
3. Простые числа.

Типовые задания для лабораторных работ
Лабораторная работа No 1
«Криптосистема без передачи ключей»

Цель работы: осуществить переписку между абонентами с секретным ключом при помощи системы компьютерной алгебры Maple.
Требования к выполнению работы: надо представить в системе компьютерной алгебры Maple
криптосистему с секретным ключом в виде переписки между абонентами A и B и проверить для
достаточно больших чисел.
Отчёт о работе проводится в виде собеседования и заключается в демонстрации работы программы, объяснении принципов работы алгоритма и ответов на дополнительные вопросы.
Критерии оценки: для получения оценки «зачтено» необходимо показать высокий уровень владения теоретическим материалом, уметь объяснить принцип работы написанной программы,
верно ответить на дополнительные вопросы.
Задание: написать программы для осуществления сообщения с секретным ключом между абонентами A и B с использованием команд модулярной арифметики системы Maple и проверить
для достаточно больших чисел.

Лабораторная работа No 2
«Сравнения первой степени с одной переменной»

Цель работы: составить программы для решения сравнений первой степени с одной переменной
при помощи системы компьютерной алгебры Maple.

Требования к выполнению работы: применить команды модулярной арифметики системы Maple
для решения сравнений первой степени различными методами и проверить для достаточно
больших чисел.
Отчёт о работе проводится в виде собеседования и заключается в демонстрации работы программы, объяснении принципов работы алгоритма и ответов на дополнительные вопросы.
Критерии оценки: для получения оценки «зачтено» необходимо показать высокий уровень

владения теоретическим материалом, уметь объяснить принцип работы написанной программы,
верно ответить на дополнительные вопросы.
Задание: написать программы с использованием команд модулярной арифметики системы Maple
для решения произвольных сравнений методом перебора и сравнений первой степени с одной
переменной при помощи теоремы Эйлера.

Лабораторная работа No 3
«Простые числа»

Цель работы: составить программы для решения задач на тестирование и нахождение достаточно больших простых чисел.
Требования к выполнению работы: применить команды модулярной арифметики системы Maple
для проверки простых чисел специальных видов и для решения задач с нахождением достаточно
больших простых чисел.
Отчёт о работе проводится в виде собеседования и заключается в демонстрации работы программы, объяснении принципов работы алгоритма и ответов на дополнительные вопросы.
Критерии оценки: для получения оценки «зачтено» необходимо показать высокий уровень владения теоретическим материалом, уметь объяснить принцип работы написанной программы,
верно ответить на дополнительные вопросы.

Задание: написать программы с использованием команд модулярной арифметики системы Maple
при решении задач с тестированием и нахождением достаточно больших простых чисел.

20.2. Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств: перечень вопросов к зачёту.

Перечень вопросов к зачету

1. Шифр, зашифровывание, расшифровывание, дешифрование.
2. Исторические примеры шифров.
3. Криптосистемы без передачи ключей.
4. Криптосистемы с открытым ключом.
5. Простые числа и факторизация.
6. Алгоритм Евклида.
7. Сравнения по модулю.
8. Теорема Эйлера.
9. Сравнения с одной переменной.
10. Сравнения по простому модулю.
11. Решето Эратосфена.
12. Метод решета Бруна.
13. Метод решета Бухштаба.
14. Метод решета Сельберга.
15. Метод весового решета.

Для оценивания результатов обучения на зачёте с оценкой используется 4-балльная шала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Полное соответствие ответа обучающегося всем перечисленным критериям. Обучающийся демонстрирует высокий уровень владения материалом, ориентируется в предметной области, верно отвечает на все дополнительные вопросы.	Повышенный уровень	Отлично
Ответ на контрольно-измерительный материал не соответствует одному или двум из перечисленных показателей, но обучающийся дает правильные ответы на дополнительные вопросы. Допускаются ошибки при воспроизведении части теоретических положений.	Базовый уровень	Хорошо
Ответ на контрольно-измерительный материал не соответствует любым трём из перечисленных показателей, обучающийся дает неполные ответы на дополнительные вопросы. Сформированные знания основных понятий, определений и теорем, изучаемых в курсе, не всегда полное их понимание с затруднениями при воспроизведении.	Пороговый уровень	Удовлетворительно
Ответ на контрольно-измерительный материал не соответствует любым четырём из перечисленных показателей. Обучающийся демонстрирует отрывочные знания (либо их отсутствие) основных понятий, определений и теорем, используемых в курсе.	–	Неудовлетворительно