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.08 Математические основы 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 №0500-06 от 03.07.2018

8. Учебный год: *2018-2019* **Семестр(ы):** 3

9.Цели и задачи учебной дисциплины: Цель курса - дать студентам математический аппарат анализа и синтеза криптографических алгоритмов. А также математические методы, необходимые для описания математических моделей программно-реализуемых шифров и расчета их криптографических характеристик.

Основными задачами изучения дисциплины являются:

- изучение свойств абстрактных алгебраических структур: групп, колец, полей, используемых при построении криптосистем
- изучение алгебраической структуры конечных групп и полей над целыми числами и многочленами, используемых при построении криптосистем
- изучение разделов теории чисел, необходимых для построения криптосистем
- ознакомление с математическими моделями симметричных и асимметричных криптосистем,
- ознакомление с математическими методами криптоанализа.

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 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-1	способность к абстрактному мышлению, анализу, синтезу	**знать:** общие принципы построения систем криптографической защиты информации; основные математические методы, лежащие в основе построения криптосистем и криптоанализа (свойства абстрактных алгебраических структур над целыми числами и многочленами, разделы теории чисел, математические модели симметричных и асимметричных криптосистем); криптоалгориты, составляющие основу криптографической защиты информации в современных компьютерных сетях и их криптографические свойства. **уметь:** шифровать и расшифровать тексты, зашифрованные методами с симметричным ключом и с асимметричным ключом; проводить криптоанализ шифртекстов; осуществлять выбор параметров криптосистем, обеспечивающих необходимую криптостойкость; осуществлять выбор алгоритмов криптосистем построения и тестирования; **владеть** (иметь навык(и))**:** разработки криптосистем с симметричным и асимметричным ключами; проведения криптоанализа ряда криптосистем с симметричным ключом и асимметричным

		ключом.
ОК-3	готовность к саморазвитию, самореализации, использованию творческого потенциала	**знать:** общие принципы построения систем криптографической защиты информации; основные математические методы, лежащие в основе построения криптосистем и криптоанализа (свойства абстрактных алгебраических структур над целыми числами и многочленами, разделы теории чисел, математические модели симметричных и асимметричных криптосистем); криптоалгориты, составляющие основу криптографической защиты информации в современных компьютерных сетях и их криптографические свойства. **уметь:** шифровать и расшифровать тексты, зашифрованные методами с симметричным ключом и с асимметричным ключом; проводить криптоанализ шифртекстов; осуществлять выбор параметров криптосистем, обеспечивающих необходимую криптостойкость; осуществлять выбор алгоритмов криптосистем построения и тестирования; **владеть** (иметь навык(и))**:** разработки криптосистем с симметричным и асимметричным ключами; проведения криптоанализа ряда криптосистем с симметричным ключом и асимметричным ключом.
ОПК-3	готовность самостоятельно создавать прикладные программные средства на основе современных информационных технологий и сетевых ресурсов	**знать:** общие принципы построения систем криптографической защиты информации; основные математические методы, лежащие в основе построения криптосистем и криптоанализа (свойства абстрактных алгебраических структур над целыми числами и многочленами, разделы теории чисел, математические модели симметричных и асимметричных криптосистем); криптоалгориты, составляющие основу криптографической защиты информации в современных компьютерных сетях и их криптографические свойства. **уметь:** шифровать и расшифровать тексты, зашифрованные методами с симметричным ключом и с асимметричным ключом; проводить криптоанализ шифртекстов; осуществлять выбор параметров криптосистем, обеспечивающих необходимую криптостойкость; осуществлять выбор алгоритмов криптосистем построения и тестирования; **владеть** (иметь навык(и))**:** разработки криптосистем с симметричным и асимметричным ключами; проведения криптоанализа ряда криптосистем с

		симметричным ключом и асимметричным ключом.
ПК-1	способность к интенсивной научно-исследовательской работе	**знать:** общие принципы построения систем криптографической защиты информации; основные математические методы, лежащие в основе построения криптосистем и криптоанализа (свойства абстрактных алгебраических структур над целыми числами и многочленами, разделы теории чисел, математические модели симметричных и асимметричных криптосистем); криптоалгориты, составляющие основу криптографической защиты информации в современных компьютерных сетях и их криптографические свойства. **уметь:** шифровать и расшифровать тексты, зашифрованные методами с симметричным ключом и с асимметричным ключом; проводить криптоанализ шифртекстов; осуществлять выбор параметров криптосистем, обеспечивающих необходимую криптостойкость; осуществлять выбор алгоритмов криптосистем построения и тестирования; **владеть** (иметь навык(и))**:** разработки криптосистем с симметричным и асимметричным ключами; проведения криптоанализа ряда криптосистем с симметричным ключом и асимметричным ключом.

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. № 3
Аудиторные занятия	*44*	*44*
в том числе: лекции	*18*	*18*
практические	*0*	*0*
лабораторные	*26*	*26*
Самостоятельная работа	*64*	*64*
Итого:	*108*	*108*

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1	Предмет криптологии и этапы ее развития	Основные задачи криптологии. Криптография и криптоанализ. Основные понятия и определения. Этапы развития криптологии. Роль математики в развитии методов

		защиты информации.
2	Арифметические и статистические основы простейших криптосистем	Математическая модель открытого текста. Простейшие методы шифрования с закрытым ключом. Математические модели простейших шифров.
3	Математические методы криптоанализа простейших симметричных систем	Индекс совпадения и взаимный индекс совпадения. Тест Казиски. Дешифрование шифров моно- и полиалфавитной замены. Дешифрование шифров перестановки.
4	Математические модели симметричных криптосистем. Стандартные криптосистемы с симметричным ключом	Шеноновские модели криптосистем. Основные типы шифров. Методы шифрования с закрытым ключом. Блочный и потоковый шифры. Группа шифрующих преобразований, их свойства и взаимосвязь со стойкостью. Математические модели криптосистем DES, IDEA, ГОСТ 28147-89.
5	Математические методы криптоанализа симметричных систем	Методы криптоанализа на основе теории статистических решений. Разностный и линейный криптоанализ. Теоретико-информационные оценки стойкости симметричных криптосистем
6	Арифметические и алгебраические основы криптосистем с ассимметричным ключом	Проблемы простоты числа и факторизации числа. Критерии простоты числа. Проблемы дискретного логарифмирования.
7	Математические модели ассимметричных криптосистем. Математические методы криптоанализа ассимметричных систем	Рюкзачный метод шифрования и его стойкость. L^3 -атака на рюкзачный метод шифрования. Криптосистема RSA и ее стойкость. Атаки на криптосистему RSA при неудачном выборе ее параметров (на основе теоремы Ферма, повторным шифрованием, на основе Китайской теоремы об остатках, безключевым чтением). Криптосистемы Эль-Гамаля, Рабина, и их стойкость.
8	Новые направления в криптологии	Мультибазисная криптография. Возможности квантовой криптографии. Математическое разделение секрета. Активный криптоанализ.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)			
		Лекции	Лабораторные	Самостоятельная работа	Всего
1	Предмет криптологии и этапы ее развития	2	–	2	4
2	Арифметические и статистические основы простейших криптосистем	2	4	6	12
3	Математические методы криптоанализа простейших симметричных систем	2	6	12	20
4	Математические модели симметричных криптосистем. Стандартные криптосистемы с симметричным ключом	4	–	6	10
5	Математические методы криптоанализа симметричных систем	2	2	8	12
6	Арифметические и алгебраические основы криптосистем с ассимметричным ключом	2	4	8	14
7	Математические модели ассимметричных криптосистем. Математические методы криптоанализа ассимметричных систем	3	10	20	33
8	Новые направления в криптологии	1	-	2	3
					0

	Итого	18	26	64	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	*Аграновский, Александр Владимирович. Практическая криптография : Алгоритмы и их программирование / А.В. Аграновский, Р.А. Хади .— М. : СОЛОН-Пресс, 2002 .— 254, [1] с. : ил.*
2	*Иванов, Михаил Александрович. Криптографические методы защиты информации в компьютерных системах и сетях / Иванов М. А. — М. : Кудиц-Образ, 2001 .— 363 с. : ил.*
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	*Коробейников А.Г. Математические основы криптологии : учебное пособие / А.Г. Коробейников, Ю.А. Гатчин. – СПб : СПб ГУ ИТМО, 2004. – 106 с.*
6	*Галуев Г.А. Математические основы криптологии : учебно-методическое пособие / Г.А. Галуев. – Таганрог : Изд-во ТРТУ, 2003. – 120с.*
7	*Жданов О. Н. Криптоанализ классических шифров : лабораторный практикум / Жданов О. Н., Куденкова И. А. – Красноярск, 2008. – 107 с.*

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
Обучающийся в полной мере владеет понятийным аппаратом в области построения алгоритмов модулярной арифметики, способен иллюстрировать ответ примерами, фактами, применять теоретические знания для поставленных задач.	*Повышенный уровень*	*Зачтено*
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.	*Базовый уровень*	*Зачтено*
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*	*Зачтено*
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.8 Математические основы криптологии_____

Форма обучения _____очная_____
очное, очно-заочное, заочное

Вид контроля _____зачет_____
экзамен, зачет

Вид аттестации _____промежуточная_____
текущая, промежуточная

Контрольно-измерительный материал № ___

1. Математическая модель открытого текста.

2. Атаки на RSA. Циклическая атака.

Преподаватель _____ _____.
подпись расшифровка подписи

Пример контрольного задания (вариант задания)

Контрольная работа
по дисциплине «Математические основы криптологии»
Вариант №___

В результате шифрования методом Вижинера был получен следующий шифртекст: «СПЦСЗЗЮУГИВЕБЬБТЖЩИОБ». Прочитайте этот шифртекст, если известно, что шифрующая последовательность содержит только символы А, Б и В.