Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет имени В.А. Бондаренко»

Кафедра вычислительной техники и защиты информации

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.В.3 Математические основы криптологии»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки
10.03.01 Информационная безопасность
(код и наименование направления подготовки)

Безопасность автоматизированных систем (информационные технологии и электронная промышленность)
(наименование направленности (профиля) образовательной программы)

Квалификация
Бакалавр

Форма обучения
Очная

Год набора 2026

2240898

Рабочая программа дисциплины *«Б1.Д.В.3 Математические основы криптологии»* рассмотрена и утверждена на заседании кафедры

Кафедра вычислительной техники и защиты информации
наименование кафедры

протокол № 10 от "06" 03 2026 г.

Заведующий кафедрой
Кафедра вычислительной техники и защиты информации — В.В. Тугов
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
Доцент кафедры вычислительной техники и защиты информации — А.А. Рычкова
должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
10.03.01 Информационная безопасность — В.В. Тугов
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом формирования фонда и научной обработки документов
личная подпись *расшифровка подписи*

Уполномоченный по качеству института
С.Н. Морозова
личная подпись *расшифровка подписи*

№ регистрации _____

© Рычкова А.А., 2026
© ОГУ, 2026

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

формирование теоретических знаний прикладной алгебры и практических умений их применения для исследования основных криптографических алгоритмов защиты информации.

Задачи:

1. Освоение основных понятий и алгоритмов теории чисел: поиска наибольшего общего делителя чисел, факторизации составного числа; построения подходящих дробей.
2. Освоение методов решения линейных сравнений и систем сравнений.
3. Освоение методов построения примитивных и неприводимых многочленов над конечным полем.
4. Освоение простейших систем шифрования.
5. Приобретение навыков нахождения показателей, индексов; извлечения квадратного корня из квадратичного вычета.
6. Приобретение навыков построения псевдослучайных последовательностей.
7. Приобретение навыков разработки собственного программного обеспечения для решения задач модульной арифметики.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательным дисциплинам (модулям) вариативной части блока Д «Дисциплины (модули)»

Пререквизиты дисциплины: *Б1.Д.Б.15.1 Алгебра и геометрия, Б1.Д.В.1 Прикладная теория алгоритмов и математической логики в вычислительной технике*

Постреквизиты дисциплины: *Б1.Д.Б.19 Методы и средства криптографической защиты информации*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2-В-1 Понимает классическую структуру проекта с учетом оптимизации ресурсного обеспечения, способы представления проекта УК-2-В-2 Формулирует цели и задачи проекта, структурирует этапы процесса организации проектной деятельности УК-2-В-3 Применяет элементы анализа, планирования и оценки рисков для выбора оптимальной стратегии развития и обоснования устойчивости проекта УК-2-В-4 В рамках цели проекта опирается на правовые нормы основных отраслей российского законодательства при постановке целей и выборе	**Знать:** математические основы криптографических методов защиты информации **Уметь:** применять знания математических основ криптографических методов защиты информации при проектировании, разработке, оптимизации ресурсного обеспечения, планирования и оценки рисков проекта,

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
	оптимальных способов их достижения; обладает навыками использования нормативно-правовых ресурсов в разработке и реализации проектов	связанного со средствами защиты информации с учетом правовых норм основных отраслей российского законодательства **Владеть:** навыками применения знаний математических основ криптографических методов защиты информации при проектировании, разработке, оптимизации ресурсного обеспечения, планирования и оценки рисков проекта связанного со средствами защиты информации с учетом правовых норм основных отраслей российского законодательства
ПК*-6 Способен устанавливать и настраивать средства защиты информации в автоматизированных системах	ПК*-6-В-1 Планирует порядок и осуществляет необходимые работы по установке и настройке аппаратно-программных средств защиты	**Знать:** математические методы, применяемые в программных, программно-аппаратных, криптографических средствах защиты **Уметь:** осуществлять работы по установке и настройке аппаратно-программных средств защиты использующих математический аппарат криптографических средств защиты данных **Владеть:** навыками осуществления работ по установке и настройке аппаратно-программных средств защиты использующих математический аппарат криптографических средств защиты данных

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 академических часа).

Вид работы	Трудоемкость, академических часов	
	6 семестр	всего
Общая трудоёмкость	**144**	**144**
Контактная работа:	**84,25**	**84,25**
Лекции (Л)	34	34
Практические занятия (ПЗ)	16	16
Лабораторные работы (ЛР)	34	34
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- выполнение индивидуального творческого задания (ИТЗ);* *- самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий;* *- изучение разделов курса в системе электронного обучения;* *- подготовка к лабораторным занятиям;* *- подготовка к практическим занятиям;* *- подготовка к рубежному контролю)*	**59,75**	**59,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**диф. зач.**	

Разделы дисциплины, изучаемые в 6 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Введение. Информационные ресурсы, подлежащие защите с помощью математических преобразований, используемых в криптографических средствах.	9	4			5
2	Математический аппарат для решения задач в области криптографии: элементы теории чисел и применение языков программирования для их реализации	34	4	4	16	10
3	Математический аппарат для решения задач в области криптографии: Сравнения и вычеты и применение языков программирования для их реализации	32	6	8	8	10
4	Математический аппарат для решения задач в области криптографии: Алгебраические структуры	22	6	2	4	10
5	Математический аппарат для решения задач в области криптографии: показатели и индексы. Кодовые последовательности	12	2			10
1	Математический аппарат симметричной криптографии.	13	4		4	5
2	Математические аппарат асимметричной криптографии	11	4	2	-	5
	Итого:	144	34	16	34	60
	Всего:	144	34	16	34	60

4.2 Содержание разделов дисциплины

1. **Введение. Информационные ресурсы, подлежащие защите с помощью математических преобразований, используемых в криптографических средствах.** История криптографии, основные понятия и определения, требования к криптографическим системам.

2. **Математический аппарат для решения задач в области криптографии: элементы теории чисел и применение языков программирования для их реализации**. Наибольший общий делитель и его свойства. Простые числа. Каноническое разложение составного числа. Непрерывные дроби, подходящие дроби и их вычисление. Мультипликативные функции и их свойства. Функции Эйлера.

3. **Математический аппарат для решения задач в области криптографии: Сравнения и вычеты и применение языков программирования для их реализации**. Сравнения и их свойства. Классы сравнимых по модулю чисел. Вычеты, системы вычетов. Теорема Эйлера. Примитивный корень. Решение линейных и нелинейных сравнений. Решение систем сравнений. Китайская теорема об остатках. Квадратичные вычеты. Символы Лежандра, Якоби. Извлечение квадратного корня из квадратичного вычета.

4. **Математический аппарат для решения задач в области криптографии: Алгебраические структуры**. Бинарная алгебра (БА). Моноид, конечный моноид. Ноль БА, 1 БА. Группа, циклическая группа, Абелева группа. Кольцо. Поле. Поля Галуа.

5. **Математический аппарат для решения задач в области криптографии: показатели и индексы**. Первообразный корень. Показатели и их свойства. Индексы. Приложения индексов к решению сравнений. Характеристические многочлены. Характеристическая функция. Неприводимые многочлены.

6. **Математический аппарат симметричной криптографии**. Сеть Фейстеля. SP-сети

7. **Математические аппарат асимметричной криптографии**. Факторизация чисел. Дискретное логарифмирование

8. **Математический аппарат хэш-функций.** Понятие хэш-функций, требования к современным хэш-функциям. Математические преобразования в хэш-функциях

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	2	Нахождения наибольшего общего делителя двух чисел на основе алгоритма Евклида	2
2	2	Нахождения наибольшего общего делителя системы чисел на основе канонического разложения числа;	2
3	2	Нахождения последовательности простых чисел, не превосходящих данного N, на основе алгоритма Эратосфена	4
4	2	Отыскания функции Эйлера для положительного целого числа	4
5	2	Реализация алгоритма вычисления подходящих дробей	4
6	3	Решение линейных сравнений с одним неизвестным;	4
7	3	Решение системы линейных сравнений с помощью Китайской теоремы об остатках	4
8	4	Операции в полях Галуа	4
		Итого:	34

4.4 Практические занятия (семинары)

№ занятия	№ раздела	Тема	Кол-во часов
1	2	Нахождение наибольшего общего делителя чисел с помощью алгоритма Евклида, построение последовательности простых чисел алгоритмом Эратосфена.	2

№ занятия	№ раздела	Тема	Кол-во часов
2	2	Построение канонического разложения составного числа. Нахождение функции Эйлера. Построение непрерывных и подходящих дробей.	2
3	3	Решение линейных сравнений.	2
4	3	Решение систем сравнений. Китайская теорема об остатках.	2
5	3	Вычисление символа Якоби и Лежандра.	2
6	3	Извлечение квадратного корня из квадратичного вычета. Решение квадратичных сравнений.	2
7	4	Алгебраические структуры	2
		Итого:	16

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Виноградов, И. М. Основы теории чисел [Текст] / И. М. Виноградов.- 10-е изд., стер. - СПб. : Лань, 2004. - 176 с - ISBN 5-8114-0535-9.

2. Смарт, Н. Криптография [Текст] / Н. Смарт; пер. с англ. С. А. Кулешова; под ред. С. К. Ландо. - Москва : Техносфера, 2006. - 528 с. : табл. - (Мир программирования). - Предм. указ.: с. 524-525. - ISBN 15-94836-043-1. - ISBN 0077099877. - ISBN 15-94836-043-1

5.2 Дополнительная литература

1.Хорев, П.Б., Методы и средства защиты информации в компьютерных системах [Текст] : учеб. пособие / П. Б. Хорев .- 4-е изд., стер. – М. : Академия, 2008. - 256 с.

2. Биркгоф, Г. Современная прикладная алгебра = Modern Applied Algebra [Текст] : пер. с англ. / Г. Биркгоф, Т.К. Барти.- 2-е изд., стер. - СПб. : Лань, 2005. - 400 с.

3. Программирование алгоритмов защиты информации: учебное пособие/ А.В. Домашев, В.О. Попов, Д.И. Правиков и др. – М.: Нолидж, 2000.

4. Судоплатов С.В., Овчинникова Е.В. Элементы дискретной математики: учеб. для вузов / С.В. Судоплатов. – Новосибирск: НГТУ, 2002.

5. Рычкова, А. А. Математические основы криптологии [Электронный ресурс] : методические указания для обучающихся по образовательной программе высшего образования по направлению подготовки 10.03.01 Информационная безопасность / А. А. Рычкова, Е. И. Ряполова; М-во науки и высш. образования Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. образования "Оренбург. гос. ун-т", Каф. вычисл. техники и защиты информ. - Электрон. текстовые дан. (1 файл: 0.95 Мб). - Оренбург : ОГУ, 2019. - 56 с. - Режим доступа: Режим доступа: http://artlib.osu.ru/web/books/metod_all/89717_20190215.pdf

5.3 Периодические издания

Защита информации. Инсайд [Электронный ресурс] – ИВИС. – Режим доступа: https://eivis.ru/browse/publication/122426/udb/12/защита-информации-инсайд

5.4 Интернет-ресурсы

1. Национальный Открытый Университет «ИНТУИТ». – Электрон. дан. - НОУ «ИНТУИТ», ИДО «ИНТУИТ», ООО «ИНТУИТ», Режим доступа: www.intuit.ru. – Загл. с экрана.

2. http://www.securitylab.ru/ информационный портал по ИТ безопасности

3. http://www.citforum.ru/ форум по информационным технологиям, методам защиты информации

4. https://www.lektorium.tv/mooc - «Лекториум», МООК: «Дискретная математика»

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1. Операционная система РЕД ОС.

2. Пакет офисных приложений «МойОфис Образование»

3. Для работы с ресурсами Интернет - веб-браузер Яндекс https://yandex.ru/..

4. ГАРАНТ Платформа F1 [Электронный ресурс]: справочно-правовая система. / Разработчик ООО НПП «ГАРАНТ-Сервис», 119992, Москва, Воробьевы горы, МГУ, [1990–2026]. – Режим доступа в сети ОГУ http://garant.net.osu.ru

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий лекционного типа, для проведения групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Аудитории оснащены комплектами ученической мебели, техническими средствами обучения, служащими для представления учебной информации большой аудитории.

Для проведения лабораторных занятий используется компьютерный класс, оснащенный плакатами.

Помещение для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к сети "Интернет", и обеспечением доступа в электронную информационно-образовательную среду ОГУ.