Минобрнауки России

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Оренбургский государственный университет»

Кафедра математики и цифровых технологий

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б1.Д.В.Э.4.1 Методы алгебраической геометрии в криптографии»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

02.03.01 Математика и компьютерные науки

(код и наименование направления подготовки)

Цифровые технологии

(наименование направленности (профиля) образовательной программы)

Квалификация

Бакалавр

Форма обучения

Очная

Год набора 2024

Рабочая программа дисциплины «*Б1.Д.В.Э.4.1 Методы алгебраической геометрии в криптографии*» рассмотрена и утверждена на заседании кафедры

Кафедра математики и цифровых технологий
наименование кафедры

протокол № 6 от "19" февраля 2024 г.

Заведующий кафедрой
Кафедра математики и цифровых технологий _____ А.Е. Шухман
наименование кафедры *подпись* *расшифровка подписи*

Исполнители:
Старший преподаватель _____ А.Н. Благовисная
должность *подпись* *расшифровка подписи*

_____ _____ _____
должность *подпись* *расшифровка подписи*

СОГЛАСОВАНО:
Председатель методической комиссии по направлению подготовки
02.03.01 Математика и компьютерные науки _____ А.Е. Шухман
код наименование *личная подпись* *расшифровка подписи*

Заведующий отделом формирования фонда и научной обработки документов
_____ Н.Н. Бигалиева / С.А. Биктимирова
личная подпись *расшифровка подписи*

Уполномоченный по качеству института
_____ И.В. Крючкова
личная подпись *расшифровка подписи*

№ регистрации _____

1 Цели и задачи освоения дисциплины

Цель (цели) освоения дисциплины:

– формирование системы знаний об объектах и методах алгебраической геометрии, коммутативной и некоммутативной алгебры, применяемых при исследовании и построении современных алгоритмов, методов и моделей защиты информации.

Задачи:

– изучение базовых конструкций алгебраической геометрии, коммутативной и некоммутативной алгебры, используемых при исследовании и построении современных криптоалгоритмов;

– овладение алгоритмами теории эллиптических кривых, используемыми в криптографических конструкциях;

– приобретение навыков решения теоретических и практических задач защиты информации на основе теории эллиптических кривых.

2 Место дисциплины в структуре образовательной программы

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

Пререквизиты дисциплины: *Б1.Д.Б.34 Дополнительные разделы алгебры, Б1.Д.В.3 Теоретико-числовые методы в криптографии, Б1.Д.В.8 Системы аналитических вычислений*

Постреквизиты дисциплины: *Отсутствуют*

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
ПК*-1 Способен демонстрировать базовые знания математических и естественных наук, основ программирования и информационных технологий	ПК*-1-В-1 Обладает базовыми знаниями, полученными в области математических и (или)естественных наук, программирования и информационных технологий ПК*-1-В-2 Умеет находить, формулировать и решать стандартные задачи в собственной научно- исследовательской деятельности, в математике и информатике ПК*-1-В-3 Имеет практический опыт научно-исследовательской деятельности в математике и информатике	**Знать:** *- основные понятия теории групп, колец, полей, используемые в криптографических методах алгебраической геометрии;* *- формулировки классических задач теории эллиптических кривых, используемых в криптографических приложениях;* **Уметь:** *- решать задачи теории эллиптических кривых, возникающие при создании и исследовании криптографических конструкций;* **Владеть:** *- навыками постановки задач криптографии на основе аппарата теории эллиптических кривых.*
ПК*-2 Способен использовать современные методы разработки и реализации конкретных алгоритмов	ПК*-2-В-1 Знает современные методы разработки и реализации алгоритмов математических моделей на базе языков и пакетов прикладных программ	**Знать:** *- основные алгоритмы на эллиптических кривых, используемые в задачах защиты информации;* **Уметь:**

Код и наименование формируемых компетенций	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций
на основе математических моделей на базе языков программирования и пакетов прикладных программ моделирования	моделирования ПК*-2-В-2 Умеет разрабатывать и реализовывать алгоритмы математических моделей на базе языков и пакетов прикладных программ моделирования ПК*-2-В-3 Имеет практический опыт разработки и реализации алгоритмов на базе языков и пакетов прикладных программ моделирования	- *адаптировать алгоритмы на эллиптических кривых, используемые в криптографии, для программной реализации;* **Владеть:** - *навыками реализации программных средств на основе аппарата теории эллиптических кривых.*

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетные единицы (108 академических часов).

Вид работы	Трудоемкость, академических часов	
	7 семестр	всего
Общая трудоёмкость	**108**	**108**
Контактная работа:	**34,25**	**34,25**
Лекции (Л)	18	18
Лабораторные работы (ЛР)	16	16
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: - *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 рубежному контролю и т.п.)*	**73,75**	**73,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**зачет**	

Разделы дисциплины, изучаемые в 7 семестре

№ раздела	Наименование разделов	Количество часов				
		всего	аудиторная работа			внеауд. работа
			Л	ПЗ	ЛР	
1	Основы и алгоритмы теории групп, колец и полей, необходимые для реализации методов алгебраической геометрии в криптографии	24	4		2	18
2	Эллиптические кривые и алгоритмы на эллиптических кривых	38	8		4	26
3	Криптографические приложения эллиптических кривых	46	6		10	30
	Итого:	108	18		16	74
	Всего:	108	18		16	74

4.2 Содержание разделов дисциплины

№ 1 Основы и алгоритмы теории групп, колец и полей, необходимые для реализации методов алгебраической геометрии в криптографии

Группы. Основные определения и свойства. Циклическая группа. Подгруппы. Смежные классы группы по подгруппе. Алгоритмы определения порядка группы, поиска образующего элемента циклической группы, поиска элемента высокого порядка циклической группы.

Кольца. Основные определения и свойства. Кольцо классов вычетов по модулю m. Кольцо многочленов от одной переменной.

Поля. Определение. Подполе. Простое поле. Поле Галуа. Порядок поля Галуа. Мультипликативная группа поля Галуа. Простые конечные поля. Многочлены над конечным полем. Порядок мультипликативной группы конечного поля: определение и основные свойства. Понятие примитивного элемента поля. Характеристика конечного поля. Конечное расширение поля. Поле разложения многочлена. Число элементов конечного поля. Минимальные многочлены. Примитивные многочлены. Неприводимые многочлены. Алгоритмическое представление поля Галуа $GF(2^n)$. Поле Галуа как векторное пространство. Реализация конечных полей.

№ 2 Эллиптические кривые и алгоритмы на эллиптических кривых

Алгебраические кривые порядка n над полем. Кривые второго порядка. Неособые точки кривой и неособые кривые. Эллиптические кривые над полем. Форма Вейерштрасса. Проективная замена координат. Бесконечно удаленная точка. Дискриминант и инвариант эллиптической кривой. Критерий гладкости кривой. Изоморфные кривые над полем и алгебраическим замыканием поля. Суперсингулярные кривые. Группа точек эллиптической кривой. Эллиптические кривые над конечными полями. Точки конечного порядка. Порядок эллиптической кривой. Неравенство Хассе и его применение. Эллиптические кривые над $GF(2^n)$. Реализация эллиптических кривых над конечными полями.

Алгоритмы на эллиптических кривых над конечными полями. Алгоритмы сложения и скалярного умножения и умножения точек эллиптических кривых. Вычисление порядка точки эллиптической кривой.

№ 3 Криптографические приложения эллиптических кривых

Криптографически надежные параметры эллиптических кривых. Эллиптические алгоритмы генерации псевдослучайных последовательностей.

Схема симметричного шифрования на эллиптических кривых. Схема асимметричного шифрования на эллиптических кривых. Протоколы цифровой подписи, основанные на эллиптической криптографии. Протоколы распределения ключей на основе эллиптических кривых. Схемы гибридного шифрования на эллиптических кривых. Российский стандарт на ЭЦП ГОСТ Р 34.10-2018.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	1	Построение полей Галуа.	2
2	2	Эллиптические кривые над конечными полями. Алгоритмы сложения и скалярного умножения точек эллиптических кривых. Алгоритм определения порядка точки на эллиптической кривой.	4
3	3	Генерация псевдослучайных последовательностей.	2
4	3	Схемы симметричного и асимметричного шифрования на эллиптических кривых.	2
5	3	Протоколы цифровой подписи, основанные на эллиптической криптографии.	2
6	3	Протоколы распределения ключей на основе эллиптических кривых.	2
7	3	Схемы гибридного шифрования на эллиптических кривых.	2

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
		Итого:	16

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Курош, А. Г. Курс высшей алгебры: учеб. для вузов / А. Г. Курош. – 17-е изд., стер. – СПб.: Лань, 2008. – 432 с.

2. Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: учеб. пособие для вузов / О. Р. Лапонина. – М.: Интернет-Ун-т Информ. Технологий, 2005. – 608 с.

3. Пихтильков, С. А. Фундаментальная и компьютерная алгебра [Электронный ресурс]: учебное пособие для студентов, обучающихся по программе высшего образования по направлению подготовки 02.03.01 Математика и компьютерные науки / С. А. Пихтильков, О. А. Пихтилькова, Л. Б. Усова; М-во образования и науки Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. образования «Оренбург. гос. ун-т». – Электрон. текстовые дан. (1 файл: 0.58 Мб). – Оренбург: ОГУ, 2016. – 116 с. – Загл. с тит. экрана. – Adobe Acrobat Reader 6.0. – Режим доступа: http://artlib.osu.ru/web/books/metod_all/31506_20160919.pdf

4. Смарт, Н. Криптография [Текст] / Н. Смарт; пер. с англ. С. А. Кулешова; под ред. С. К. Ландо. – Москва: Техносфера, 2006. – 528 с.

5.2 Дополнительная литература

1. Пихтилькова, О. А. Лабораторные работы по дисциплине «Методы алгебраической геометрии в криптографии» [Электронный ресурс]: методические указания для обучающихся по образовательной программе высшего образования по направлению подготовки 02.03.01 Математика и компьютерные науки / О. А. Пихтилькова, А. Н. Благовисная; М-во науки и высш. образования Рос. Федерации, Федер. гос. бюджет. образоват. учреждение высш. образования «Оренбург. гос. ун-т», Каф. алгебры и дискрет. математики. – Электрон. текстовые дан. (1 файл: 1.01 Мб). – Оренбург: ОГУ, 2019. – 77 с. – Загл. с тит. экрана. – Adobe Acrobat Reader 6.0. – Режим доступа: http://artlib.osu.ru/web/books/metod_all/92829_20190327.pdf

5.3 Периодические издания

1. Вестник компьютерных и информационных технологий: журнал. – М.: Агентство «Роспечать», 2017-2022.

2. Информационные технологии: журнал. – М.: Агентство «Роспечать», 2017-2022.

5.4 Интернет-ресурсы

1. http://eqworld.ipmnet.ru/indexr.htm – международный научно-образовательный сайт «Мир математических уравнений», который содержит обширную учебную физико-математическую библиотеку и предназначен для широкого круга ученых, преподавателей вузов, инженеров, аспирантов и студентов в различных областях математики и других наук; все ресурсы сайта являются бесплатными для его пользователей).

2. https://www.gost.ru/portal/gost/ – портал Федерального агентства по техническому регулированию и метрологии.

5.5 Программное обеспечение, профессиональные базы данных и информационные справочные системы

1. Операционная система РЕД ОС.
2. «МойОфис Образование» – набор приложений для работы с текстом, таблицами и презентациями в образовательных организациях.
3. Программная система для организации видео-конференц-связи MTS Link
4. Программа для просмотра сайтов Яндекс.Браузер, свободно распространяемая, входит в реестр отечественного ПО.
5. Elibrary [Электронный ресурс]: реферативная база данных, с ограниченным доступом к полным текстам статей – Режим доступа: https://www.elibrary.ru/, в локальной сети ОГУ.
6. Math-Net.ru [Электронный ресурс]: общероссийский математический портал, включающий информационно-справочную систему по публикациям в отечественных математических журналах. – Режим доступа http://www.mathnet.ru/.
7. Система программирования Python, свободно распространяемая по лицензии PSFL.

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 компьютерной техникой.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой подключенной к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду ОГУ.