Минобрнауки России

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

Кафедра алгебры и дискретной математики

РАБОЧАЯ ПРОГРАММА

ДИСЦИПЛИНЫ

«Б.1.В.ОД.12 Методы алгебраической геометрии в криптографии»

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки
02.03.01 Математика и компьютерные науки
(код и наименование направления подготовки)

Алгоритмы и приложения компьютерной математики
(наименование направленности (профиля) образовательной программы)

Тип образовательной программы
Программа академического бакалавриата

Квалификация
Бакалавр

Форма обучения
Очная

Год набора 2017

Рабочая программа рассмотрена и утверждена на заседании кафедры

Кафедра алгебры и дискретной математики
наименование кафедры

протокол № 7 от "21" февраля 2017 г.

Заведующий кафедрой
Кафедра алгебры и дискретной математики _____ О.А. Пихтилькова
наименование кафедры *подпись* *расшифровка подписи*

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

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

Заведующий отделом комплектования научной библиотеки
_____ Н.Н. Грицай
личная подпись *расшифровка подписи*

Уполномоченный по качеству факультета
_____ 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 обязательным дисциплинам (модулям) вариативной части блока 1 «Дисциплины (модули)»

Пререквизиты дисциплины: *Б.1.Б.14 Фундаментальная и компьютерная алгебра, Б.1.Б.16 Дискретная математика, математическая логика и их приложения в информатике и компьютерных науках*

Постреквизиты дисциплины: *Б.2.В.П.1 Преддипломная практика*

3 Требования к результатам обучения по дисциплине

Процесс изучения дисциплины направлен на формирование следующих результатов обучения

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
Знать: *- основные понятия теории групп, колец, полей, используемые в криптографических методах алгебраической геометрии;* **Уметь:** *- решать задачи теории эллиптических кривых, возникающие при создании и исследовании криптографических конструкций;* **Владеть:** *- алгоритмами на эллиптических кривых, используемыми в задачах защиты информации.*	ПК-1 способностью к определению общих форм и закономерностей отдельной предметной области
Знать: *- формулировки классических задач теории эллиптических кривых, используемых в криптографических приложениях;* **Уметь:** *- адаптировать постановки классических задач теории эллиптических кривых для криптографических целей;* **Владеть:** *- навыками постановки задач криптографии на основе аппарата теории эллиптических кривых.*	ПК-2 способностью математически корректно ставить естественнонаучные задачи, знание постановок классических задач математики
Знать: *- формулировки утверждений и теорем теории эллиптических кривых, связанных с задачами защиты информации;* **Уметь:**	ПК-3 способностью строго доказать утверждение, сформулировать результат, увидеть следствия

Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций	Формируемые компетенции
- *доказывать утверждения и теоремы теории эллиптических кривых, связанных с задачами защиты информации;* **Владеть:** - *различными методами вывода основных результатов теории эллиптических кривых.*	полученного результата

4 Структура и содержание дисциплины

4.1 Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных единиц (108 академических часов).

Вид работы	Трудоемкость, академических часов	
	7 семестр	всего
Общая трудоёмкость	**108**	**108**
Контактная работа:	**51,25**	**51,25**
Лабораторные работы (ЛР)	50	50
Консультации	1	1
Промежуточная аттестация (зачет, экзамен)	0,25	0,25
Самостоятельная работа: *- самоподготовка (проработка и повторение материала учебников и учебных пособий;* *- подготовка к лабораторным занятиям;* *- подготовка к устным и письменным опросам;* *- подготовка к рубежному контролю)*	**56,75**	**56,75**
Вид итогового контроля (зачет, экзамен, дифференцированный зачет)	**экзамен**	

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	32			16	16
2	Эллиптические кривые	28			12	16
3	Криптографические приложения эллиптических кривых	48			22	26
	Итого:	108			50	58
	Всего:	108			50	58

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 34.10-2012.

4.3 Лабораторные работы

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
1	1	Группы. Поиск порядка элемента группы, образующего элемента группы. Построение смежных классов.	4
2	1	Кольца. Арифметические операции в кольцах вычетов по модулю *m*.	4
3	1	Поля. Конечные поля. Многочлены над простыми конечными полями. Арифметические операции в кольце многочленов над простым конечным полем	4
4	1	Построение полей Галуа.	4
5	2	Эллиптические кривые над конечными полями.	4
6	2	Алгоритм сложения точек эллиптических кривых.	4
7	2	Алгоритм скалярного умножения точек эллиптических кривых.	2
8	2	Алгоритм определения порядка точки на эллиптической кривой.	2
9	3	Криптографически надежные параметры эллиптических кривых.	2
10	3	Генерация псевдослучайных последовательностей.	2
11	3	Схема симметричного шифрования на эллиптических кривых.	2
12	3	Схема асимметричного шифрования на эллиптических кривых.	4
13	3	Протоколы цифровой подписи, основанные на эллиптической криптографии.	4
14	3	Протоколы распределения ключей на основе эллиптических кривых.	4

№ ЛР	№ раздела	Наименование лабораторных работ	Кол-во часов
15	3	Схемы гибридного шифрования на эллиптических кривых.	2
16	3	Российский стандарт на ЭЦП ГОСТ Р 34.10-2012.	2
		Итого:	50

5 Учебно-методическое обеспечение дисциплины

5.1 Основная литература

1. Винберг, Э.Б. Алгебра [Электронный ресурс] / Э.Б. Винберг. – НЦНМО, 2011. – Режим доступа: http://biblioclub.ru/index.php?page=book_view&book_id=63299

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

3. 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.

4. 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.

5. 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. Василенко, О.Н. Теоретико-числовые алгоритмы в криптографии [Электронный ресурс] / О.Н. Василенко. – Москва: МЦНМО, 2006. – 336 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=61814

5.3 Периодические издания

1. Прикладная математика и механика: журнал. - М.: Агентство «Роспечать», 2016.
2. Вычислительные технологии: журнал. - М.: Агентство «Роспечать», 2016.
3. Вестник компьютерных и информационных технологий: журнал. – М.: Агентство «Роспечать», 2017.
4. Информационные технологии: журнал. – М.: Агентство «Роспечать», 2017.

5.4 Интернет-ресурсы

1. http://cryptography.ru – сайт посвящен вопросам математической криптографии, содержит календарь конференций, семинаров и т. п., которые полностью или частично посвящены вопросам защиты информации, а также актуальные ссылки на сайты данных научных мероприятий.
2. 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).
3. https://arxiv.org/ – крупнейший бесплатный архив электронных публикаций научных статей и их препринтов по физике, математике, астрономии, информатике и биологии.

4. 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 современных информационных технологий

1. Операционная система Microsoft Windows.
2. OpenOffice/LibreOffice - свободный офисный пакет программ, включающий в себя текстовый и табличный редакторы, редактор презентаций и другие офисные приложения.
3. Бесплатное средство просмотра файлов PDF Adobe Reader.
4. Microsoft Visual Studio (лицензии по программе Microsoft Dream Spark Premium).
5. SCOPUS [Электронный ресурс]: реферативная база данных / компания Elsevier. – Режим доступа: https://www.scopus.com/, в локальной сети ОГУ.
6. Springer [Электронный ресурс]: база данных научных книг, журналов, справочных материалов / компания Springer Customer Service Center GmbH. – Режим доступа: https://link.springer.com/, в локальной сети ОГУ.
7. Общероссийский математический портал Math-Net.Ru [Электронный ресурс]: профессиональная база данных для математиков – Режим доступа: http://www.mathnet.ru/index.phtml/?option_lang=rus

6 Материально-техническое обеспечение дисциплины

Учебные аудитории для проведения занятий семинарского 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.

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

К рабочей программе прилагаются:

- Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине;
- Методические указания для обучающихся по освоению дисциплины.