МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
**«Дальневосточный федеральный университет»**
(ДВФУ)

**ШКОЛА ЕСТЕСТВЕННЫХ НАУК**

«СОГЛАСОВАНО»
Руководитель ОП

_____ Добржинский Ю.В
(подпись) (Ф.И.О.)

«УТВЕРЖДАЮ»
И.о. заведующего кафедрой
информационной безопасности

_____ Добржинский Ю.В
(подпись) (Ф.И.О.)

« 15 » июня 2019 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**
Методы алгебраической геометрии в криптографии
**Специальность 10.05.01 Компьютерная безопасность**
(Математические методы защиты информации)
**Форма подготовки очная**

курс 5 семестр 9
лекции 36 час.
практические занятия 54 час.
лабораторные работы 18 час.
в том числе с использованием МАО лек. 9 / пр. 00 / лаб. 00 час.
в том числе в электронной форме лек. 00 / пр. 00 / лаб. 00 час.
всего часов аудиторной нагрузки 108 час.
в том числе с использованием МАО 9 час.
в том числе в электронной форме 00 час.
самостоятельная работа 72 час.
в том числе на подготовку к экзамену 27 час.
курсовая работа / курсовой проект не предусмотрены
зачет не предусмотрен
экзамен 9 семестр

Рабочая программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования, утвержденного приказом Министерства образования и науки РФ от 01.12.2016 № 1512

Рабочая программа обсуждена на заседании кафедры информационной безопасности
протокол № 10 от « 15 » июня 2019 г.

И.о. заведующего кафедрой: Добржинский Ю.В., к.т.н., с.н.с.
Составитель (ли): Корнюшин П.Н. д.ф.-м.н., профессор

**Оборотная сторона титульного листа РПД**

**I. Рабочая программа пересмотрена на заседании кафедры**:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

**II. Рабочая программа пересмотрена на заседании кафедры**:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

**III. Рабочая программа пересмотрена на заседании кафедры**:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

**IV. Рабочая программа пересмотрена на заседании кафедры**:

Протокол от «_____» _____ 20___ г. № _____

Заведующий кафедрой _____ _____
(подпись) (И.О. Фамилия)

# ABSTRACT

**Specialist's degree in 10.05.01 Computer Security**

**Specialization "Mathematical Methods for Information Security"**

**Course title:** *Methods of algebraic geometry in cryptography*

**Basic part of Block 1, _5_credits**

**Instructor:** *Kornyushin P.N.*

**At the beginning of the course a student should be able to:**

• *ability to correctly apply the apparatus of mathematical analysis, geometry, algebra, discrete mathematics, mathematical logic, theory of algorithms, probability theory, mathematical statistics, information theory, number-theoretic methods (OPK-2) when solving professional problems;*

• *the ability to understand the importance of information in the development of modern society, to apply the achievements of information technology to search and process information on the profile of activities in global computer networks, library collections and other sources of information (OPK-3).*

**Learning outcomes:**

*PSK-2.2, based on the analysis of the applied mathematical methods and algorithms, to evaluate the effectiveness of information protection means and methods in computer systems*

*PSK-2.3 ability to develop computational algorithms that implement modern mathematical methods for protecting information*

*CPM-2.5 with the ability to conduct a comparative analysis and make a reasonable choice of software and hardware tools for protecting information, taking into account modern and advanced mathematical methods for protecting information.*

**Course description:**

*The course "Methods of Algebraic Geometry in Cryptography" is one of the fundamental parts of modern theoretical cryptography, without the knowledge of which further professional training in the field of modern information protection is impossible. During the development of this course, students form the skills of*

*competently applying the theoretical foundations of cryptography in the formulation of practical problems, in solving problems using the modern theoretical apparatus, in systematizing the knowledge gained.*

**Main course literature:**

*1. Беломойцев, Д.Е. Основные методы криптографической обработки данных [Электронный ресурс]: Учеб. пособие / Д. Е. Беломойцев, Т. М. Волосатова, С. В. Родионов. - М.: Издательство МГТУ им. Н. Э. Баумана, 2014. – 76 с. – Режим доступа: http://www.studentlibrary.ru/book/ISBN9785703838334.html*

*2. Рябко, Б.Я., Фионов, А.Н. Криптографические методы защиты информации [Электронный ресурс] : Учебное пособие для вузов / Б.Я. Рябко, А.Н. Фионов. - 2-е издание, стереотип. - М.: Горячая линия - Телеком, 2012. – 229 с. – Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991202862.html*

*3. Рябко, Б.Я., Фионов, А.Н. Основы современной криптографии и стеганографии [Электронный ресурс] / Б.Я. Рябко, А.Н. Фионов. - М.: Горячая линия - Телеком, 2010. – 232 с. – Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991201506.html*

**Form of final control:** *exam.*

## Аннотация к рабочей программе дисциплины «Методы алгебраической геометрии в криптографии»

Курс учебной дисциплины «Методы алгебраической геометрии в криптографии» предназначен для обучения студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин базовой части учебного плана Б1.Б.40.3.

Общая трудоемкость освоения дисциплины составляет 180 академических часов (5 з.е.). Учебным планом предусмотрены лекции (36 часов), лабораторные работы (18 часов), практические занятия (54 часа), самостоятельные работы (45 часов), подготовку к экзамену (27 часов). Дисциплина реализуется на 5 курсе в 9 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина логически и содержательно связана с такими курсами, как «Алгебра», «Геометрия», «Дискретная математика», «Теория вероятностей и математическая статистика», «Теория информации», «Математическая логика и теория алгоритмов», «Основы информационной безопасности», «Методы программирования» и «Теоретико-числовые методы в криптографии».

Курс «Методы алгебраической геометрии в криптографии» составляет одну из фундаментальных частей современной теоретической криптографии, без знания которых невозможна дальнейшая профессиональная подготовка в области современной защиты информации. При освоении данного курса у студентов формируются навыки грамотного применения теоретических основ криптографии в постановке практических задач, в решении задач с применением современного теоретического аппарата, в систематизации полученных знаний.

**Цели** изучения дисциплины «Методы алгебраической геометрии в криптографии».

**Задачи:**

- последовательное изложение теоретического материала на лекциях, при котором все основные результаты снабжаются строгими доказательствами;
- сформировать представление о комплексе идей и методов классической геометрии плоскости и пространства;
- выработать у студентов умения применять основные приёмы геометрических методов при исследовании математических моделей, возникающих в естествознании и прикладных науках, развить математическую культуру студента и подготовить его к усвоению других основных математических курсов;
- отработка приемов решения задач на практических занятиях.

Для успешного изучения дисциплины «Методы алгебраической геометрии в криптографии» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способность корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов (ОПК-2);
- способность понимать значение информации в развитии современного общества, применять достижения информационных технологий для поиска и обработки информации по профилю деятельности в глобальных компьютерных сетях, библиотечных фондах и иных источниках информации (ОПК-3).

В результате изучения данной дисциплины у обучающихся формируются следующие профильно-специализированные компетенции (элементы компетенций):

| **Код и формулировка компетенции** | **Этапы формирования компетенции** |
|---|---|
| ПСК-2.2 способностью на основе анализа применяемых | Знает основные понятия алгебраической геометрии: аффинные и проективные пространства, алгебраические многообразия, дивизоры, и т.д.. |

| | | |
|---|---|---|
| математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах | Умеет | оценивать качество криптографической защиты. |
| | Владеет | навыками криптоанализа асимметричных систем шифрования. |
| ПСК-2.3 способностью разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации | Знает | принципы применения эллиптических и гиперэллиптических кривых в криптографии. |
| | Умеет | разрабатывать быстрые вычислительные алгоритмы для криптографических приложений. |
| | Владеет | навыками программирования алгебраических операций в конечных алгебраических структурах, в том числе в группе точек эллиптических и гиперэллиптических кривых. |
| ПСК-2.5 способностью проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации | Знает | принципы и методы построения быстрых алгоритмов для реализации систем защиты информации. |
| | Умеет | проводить предварительное оценивание временной сложности разрабатываемых алгоритмов. |
| | Владеет | методами алгебраической геометрии в криптографии. |

Для формирования вышеуказанных компетенций в рамках дисциплины «Методы алгебраической геометрии в криптографии» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, лекции-диалоги, работа в малых группах, метод обучения в парах. Используемые оценочные средства: конспекты (ПР-7), лабораторные работы (ПР-6), собеседование (ОУ-1), коллоквиум (ОУ-2).

# I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

**Раздел I. Элементы алгебраической геометрии (8 час.)**

**Тема 1. Аффинные и проективные пространства (4 час.)**

1.1. Аффинные и проективные пространства.

1.2. Алгебраические многообразия.

1.3. Алгебраические кривые.

**Тема 2. Дивизоры (4 час.)**

2.1. Дивизоры.

2.2. Группы классов дивизоров на алгебраических кривых.

**Раздел II. Эллиптические кривые (28 час.)**

**Тема 1. Эллиптические кривые (6 час.)**

1.1. Определение группового закона. Формулы для операций сложения и удвоения точек эллиптической кривой.

1.2. Эндоморфизмы эллиптических кривых. Теорема о кольце эндоморфизмов. Эндоморфизм Фробениуса.

1.3. Многочлены деления. Алгоритм Шуфа вычисления порядка группы точек эллиптической кривой.

**Тема 2. Эллиптические кривые над конечными полями и кольцами (16 час.)**

2.1. Эллиптические кривые над полем комплексных чисел. Дифференциальное уравнение для функции Вейерштрасса. Теорема сложения. Модулярные формы. Квадратичные формы отрицательного дискриминанта (алгоритм приведения Гаусса).

2.2. Эллиптические кривые с комплексным умножением. Связь комплексного умножения и порядка группы точек. Алгоритм построения кривых с комплексным умножением и алгоритм Аткина и Морейна проверки простоты целых чисел.

2.3. Эллиптические кривые над кольцами

2.4. Алгоритм Ленстры разложения целых чисел на множители.

**Тема 3. Криптографические приложения эллиптических кривых (6 час.)**

3.1. Стандарт на электронную цифровую подпись.

3.2. Протоколы Диффи--Хеллмана в группе точек эллиптических кривых.

## II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

**Практические занятия (54 час.)**

**Занятие 1. Аффинные и проективные пространства (6 час.)**

1. Аффинные и проективные алгебраические многообразия.
2. Алгебраические кривые.

**Занятие 2. Дивизоры (6 час.)**

1. Группы классов дивизоров на алгебраических кривых.

**Занятие 3. Эллиптические кривые (6 час.)**

1. Определение группового закона.
2. Формулы для операций сложения и удвоения точек эллиптической кривой.

**Занятие 4. Эндоморфизмы эллиптических кривых (6 час.)**

1. Теорема о кольце эндоморфизмов.
2. Эндоморфизм Фробениуса.

**Занятие 5. Многочлены деления (6 час.)**

1. Многочлены деления
2. Алгоритм Шуфа вычисления порядка группы точек эллиптической кривой.

**Занятие 6. Эллиптические кривые над полем комплексных чисел (6 час.)**

1. Дифференциальное уравнение для функции Вейерштрасса.
2. Теорема сложения.
3. Модулярные формы.
4. Квадратичные формы отрицательного дискриминанта (алгоритм приведения Гаусса).

**Занятие 7. Эллиптические кривые с комплексным умножением (6 час.)**

1. Связь комплексного умножения и порядка группы точек.
2. Алгоритм построения кривых с комплексным умножением и алгоритм Аткина и Морейна проверки простоты целых чисел.

**Занятие 8. Эллиптические кривые над кольцами (6 час.)**

1. Эллиптические кривые над кольцами.
2. Алгоритм Ленстры разложения целых чисел на множители.

**Занятие 9. Криптографические приложения эллиптических кривых (6 час.)**

1. Стандарт на электронную цифровую подпись
2. Протоколы Диффи-Хеллмана в группе точек эллиптических кривых.

**Лабораторные работы (18 час.)**

**Лабораторная работа №1. Элементы алгебраической геометрии (6 час.)**

**Лабораторная работа №2. Эллиптические кривые в криптографии (6 час.)**

**Лабораторная работа №3. Дискретное логарифмирование на эллиптической кривой (6 час.)**

## III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Методы алгебраической геометрии в криптографии» представлено в Приложении 1 и включает в себя:

план-график выполнения самостоятельной работы по дисциплине, в том числе примерные нормы времени на выполнение по каждому заданию;

характеристика заданий для самостоятельной работы обучающихся и методические рекомендации по их выполнению;

требования к представлению и оформлению результатов самостоятельной работы;

критерии оценки выполнения самостоятельной работы.

## IV. КОНТРОЛЬ ДОСТИЖЕНИЯ ЦЕЛЕЙ КУРСА

| № п/п | Контролируемые разделы / темы дисциплины | Коды и этапы формирования компетенций | | Оценочные средства - наименование | |
|---|---|---|---|---|---|
| | | | | текущий контроль | промежуточная аттестация |
| 1 | Раздел I. Элементы алгебраической геометрии | ПСК-2.2<br>ПСК-2.3<br>ПСК-2.5 | Умеет | ПР-7 | 1-4 |
| | | | Знает | ПР-7 | 1-4 |
| | | | Владеет | ПР-6 | 1-4 |
| 2 | Раздел II. Эллиптические кривые | ПСК-2.2<br>ПСК-2.3<br>ПСК-2.5 | Умеет | ПР-7 | 5-18 |
| | | | Знает | ПР-7 | 5-18 |
| | | | Владеет | ПР-6 | 5-18 |

Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков и (или) опыта деятельности, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 2.

## V. СПИСОК УЧЕБНОЙ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### Основная литература

*(электронные и печатные издания)*


1. Беломойцев, Д.Е. Основные методы криптографической обработки данных [Электронный ресурс]: Учеб. пособие / Д. Е. Беломойцев, Т. М. Волосатова, С. В. Родионов. - М.: Издательство МГТУ им. Н. Э. Баумана, 2014. – 76 с. – Режим доступа: http://www.studentlibrary.ru/book/ISBN9785703838334.html
2. Рябко, Б.Я., Фионов, А.Н. Криптографические методы защиты информации [Электронный ресурс] : Учебное пособие для вузов / Б.Я. Рябко, А.Н. Фионов. - 2-е издание, стереотип. - М.: Горячая линия - Телеком, 2012. – 229 с. – Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991202862.html
3. Рябко, Б.Я., Фионов, А.Н. Основы современной криптографии и стеганографии [Электронный ресурс] / Б.Я. Рябко, А.Н. Фионов. - М.: Горячая линия - Телеком, 2010. – 232 с. – Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991201506.html


### Дополнительная литература


1. Аграновский, А.В. Практическая криптография: алгоритмы и их программирование [Электронный ресурс] : справочник / А.В. Аграновский, Р.А. Хади. — Электрон. дан. — Москва : СОЛОН-Пресс, 2009. — 256 с. — Режим доступа: https://e.lanbook.com/book/13653
2. Музыкантский, А.И. Лекции по криптографии [Электронный ресурс]: учебное пособие / А.И. Музыкантский, В.В. Фурин. — Электрон. дан. — М.: МЦНМО, 2013. — 68 с. — Режим доступа: https://e.lanbook.com/book/56408
3. Романьков, В.А. Алгебраическая криптография [Электронный ресурс]: монография / В.А. Романьков. — Электрон. дан. — Омск: ОмГУ, 2013. — 136 с. — Режим доступа: https://e.lanbook.com/book/75405
4. Ю. Л. Сагалович Введение в алгебраические коды : учебное пособие / Москва : Изд-во Института проблем передачи информации РАН, 2014. 310 с.

Режим доступа: http://lib.dvfu.ru:8080/lib/item?id=chamo:756734&theme=FEFU

## VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Методы алгебраической геометрии в криптографии», составляет 108 часов. На самостоятельную работу отведено 72 часа, из них 27 часов на подготовку к экзамену.

Аудиторная нагрузка состоит из 36 лекционных часов, 54 часов практических работ и 18 часов лабораторных работ. На лекционных занятиях обучающийся получает теоретические знания, усвоение которых необходимо для дальнейшего выполнения лабораторных работ и практических заданий. Студенту рекомендуется предварительно готовиться к лекции, используя ресурсы из списка, приведённого в разделе V, для более качественного освоения теоретического материала, а также возможности задать вопросы преподавателю.

Подготовка к лабораторным и практическим работам предполагает повторение лекционного материала. В результате выполнения работы студент предоставляет преподавателю отчёт о проделанной работе, содержащий следующие пункты: цель работы, краткий теоретический материал, задание, ход работы, результаты и выводы о проделанной работе.

В рамках указанной дисциплины промежуточной формой аттестации является экзамен. Для допуска к экзамену обучающийся должен получить оценку «зачтено» по всем практическим и лабораторным работам курса.

Вопросы к экзамену соответствуют темам, изучаемым на лекционных занятиях. Самостоятельная работа при подготовке к экзамену включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников из списка литературы и материалов по лабораторным и практическим работам.

## VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

| | |
|---|---|
| Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус L, ауд. L 609, Учебная аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. | Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 28)<br>Оборудование:<br>Доска аудиторная, переносной компьютер (ноутбук Lenovo) с сумкой – 1 шт. |

Приложение 1

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
**«Дальневосточный федеральный университет»**
(ДВФУ)

**ШКОЛА ЕСТЕСТВЕННЫХ НАУК**

# УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

**по дисциплине «Методы алгебраической геометрии в криптографии»**
**Направление подготовки 10.05.01 Компьютерная безопасность**
специализация «Математические методы защиты информации»
**Форма подготовки очная**

**Владивосток**
**2019**

## План-график выполнения самостоятельной работы по дисциплине

| № п/п | Дата/сроки выполнения | Вид самостоятельной работы | Примерные нормы времени на выполнение | Форма контроля |
|---|---|---|---|---|
| **1** | 1-18 неделя обучения | Подготовка практического задания (выполнение отчета к занятию) | 45 | Отчет о выполнении практического задания |
| **2** | Сессия | Подготовка и сдача экзамена | 27 | Экзамен |

### Рекомендации по самостоятельной работе студентов

При подготовке отчета о выполнении практического задания должны использоваться источники из списка учебной литературы, а также примеры, рассмотренные на лекционных и практических занятиях. Отчет должен содержать:

- титульный лист;
- содержание;
- описание задания;
- решение;
- выводы.

### Методические указания к выполнению отчета по занятию

Для получения **«зачтено»** отчет должен содержать основные пункты: титульный лист, содержание, описание задания, решение, выводы. При представлении отчета к сдаче обучающийся последовательно излагает принцип выполненной работы.

Оценка **«незачтено»** выставляется в случае, если отчет не содержит решения или выводов; обучающийся не может объяснить решение, излагает материал непоследовательно, сбивчиво.

Приложение 2

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
**«Дальневосточный федеральный университет»**
(ДВФУ)

**ШКОЛА ЕСТЕСТВЕННЫХ НАУК**

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
**по дисциплине «Методы алгебраической геометрии в криптографии»**
**Направление подготовки 10.05.01 Компьютерная безопасность**
специализация «Математические методы защиты информации»
**Форма подготовки очная**

**Владивосток**
**2019**

# Паспорт ФОС

| Код и формулировка компетенции | Этапы формирования компетенции | |
|---|---|---|
| ПСК-2.2 способностью на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах | Знает | основные понятия алгебраической геометрии: аффинные и проективные пространства, алгебраические многообразия, дивизоры, и т.д.. |
| | Умеет | оценивать качество криптографической защиты. |
| | Владеет | навыками криптоанализа асимметричных систем шифрования. |
| ПСК-2.3 способностью разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации | Знает | принципы применения эллиптических и гиперэллиптических кривых в криптографии. |
| | Умеет | разрабатывать быстрые вычислительные алгоритмы для криптографических приложений. |
| | Владеет | навыками программирования алгебраических операций в конечных алгебраических структурах, в том числе в группе точек эллиптических и гиперэллиптических кривых. |
| ПСК-2.5 способностью проводить сравнительный анализ и осуществлять обоснованный выбор программно-аппаратных средств защиты информации с учетом современных и перспективных математических методов защиты информации | Знает | принципы и методы построения быстрых алгоритмов для реализации систем защиты информации. |
| | Умеет | проводить предварительное оценивание временной сложности разрабатываемых алгоритмов. |
| | Владеет | методами алгебраической геометрии в криптографии. |

| № п/п | Контролируемые разделы / темы дисциплины | Коды и этапы формирования компетенций | | Оценочные средства - наименование | |
|---|---|---|---|---|---|
| | | | | текущий контроль | промежуточная аттестация |
| 1 | Раздел I. Элементы алгебраической геометрии | ПСК-2.2<br>ПСК-2.3<br>ПСК-2.5 | Умеет | ПР-7 | 1-4 |
| | | | Знает | ПР-7 | 1-4 |
| | | | Владеет | ПР-6 | 1-4 |
| 2 | Раздел II. Эллиптические кривые | ПСК-2.2<br>ПСК-2.3<br>ПСК-2.5 | Умеет | ПР-7 | 5-18 |
| | | | Знает | ПР-7 | 5-18 |
| | | | Владеет | ПР-6 | 5-18 |

## Оценочные средства для промежуточной аттестации

### Вопросы к экзамену:

1. Аффинные и проективные пространства.
2. Алгебраические многообразия.
3. Алгебраические кривые.
4. Дивизоры. Группы классов дивизоров на алгебраических кривых.
5. Определение группового закона.
6. Формулы для операций сложения и удвоения точек эллиптической кривой.
7. Эндоморфизмы эллиптических кривых. Теорема о кольце эндоморфизмов. Эндоморфизм Фробениуса.
8. Многочлены деления. Алгоритм Шуфа вычисления порядка группы точек эллиптической кривой.
9. Эллиптические кривые над полем комплексных чисел.
10. Дифференциальное уравнение для функции Вейерштрасса.
11. Теорема сложения.
12. Модулярные формы. Квадратичные формы отрицательного дискриминанта (алгоритм приведения Гаусса).
13. Эллиптические кривые с комплексным умножением. Связь комплексного умножения и порядка группы точек.
14. Алгоритм построения кривых с комплексным умножением и алгоритм Аткина и Морейна проверки простоты целых чисел.
15. Эллиптические кривые над кольцами
16. Алгоритм Ленстры разложения целых чисел на множители.
17. Стандарт на электронную цифровую подпись.
18. Протоколы Диффи-Хеллмана в группе точек эллиптических кривых.

### Критерии выставления оценки на экзамене

| Оценка | Требования к сформированным компетенциям |
|---|---|
| *«отлично»* | Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении |

| | |
|---|---|
| | заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач по методологии научных исследований. |
| *«хорошо»* | Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения. |
| *«удовлетворительно»* | Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ |
| *«неудовлетворительно»* | Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по соответствующей дисциплине. |

## Оценочные средства для текущей аттестации

| № п/п | Код ОС | Наименование оценочного средства | Кроткая характеристика оценочного средства | Представление оценочного средства в фонде |
|---|---|---|---|---|
| 1 | ОУ-1 | Собеседование | Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определённому разделу, теме, проблеме и т.п. | Вопросы по темам/разделам дисциплины |

| | | | | |
|---|---|---|---|---|
| 2 | ОУ-2 | Коллоквиум | Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования преподавателя с обучающимися. | Вопросы по темам/разделам дисциплины |
| 3 | ПР-6 | Лабораторная работа | Средство для закрепления и практического освоения материала по определенному разделу | Комплект лабораторных заданий |
| 4 | ПР-7 | Конспект | Продукт самостоятельной работы обучающегося, отражающий основные идеи заслушанной лекции, сообщения и т.д. | Темы/разделы дисциплины |