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 18 час.
лабораторные работы 36 час.
в том числе с использованием МАО лек. 9 / пр. 0 / лаб. 0 час.
всего часов аудиторной нагрузки 90 час.
в том числе с использованием МАО 00 час.
самостоятельная работа 90 час.
в том числе на подготовку к экзамену 36 час.
контрольные работы (количество) не предусмотрены
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: Власов А.А.

Владивосток
2019

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. Фамили

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;
- ability to use programming languages and systems, tools for solving professional, research and applied tasks (OPK-8).

Learning outcomes:

- (OPK-10) the ability to build an algorithm independently, to conduct its analysis and implementation in modern software systems
- PSK-2.2 ability based on the analysis of the applied mathematical methods and algorithms to evaluate the effectiveness of means and methods of protecting information in computer systems
- CPM-2.3 ability to develop computational algorithms that implement modern mathematical methods for protecting information
- PSK-2.5 the ability to conduct a comparative analysis and make an informed 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. Начертательная геометрия [Электронный ресурс] : методические указания / . — Электрон. текстовые данные. — Иваново: Ивановский государственный архитектурно-строительный университет, ЭБС АСВ, 2011. — 32 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/17738.html

2. Ивлева А.М. Линейная алгебра. Аналитическая геометрия [Электронный ресурс] : учебное пособие / А.М. Ивлева, П.И. Прилуцкая, И.Д. Черных. — Электрон. текстовые данные. — Новосибирск: Новосибирский государственный технический университет, 2014. — 180 с. — 978-5-7782-2409-4. — Режим доступа: http://www.iprbookshop.ru/45380.html

Form of final control: exam.

Аннотация к учебной программе дисциплины

«Методы алгебраической геометрии в криптографии»

Рабочая программа 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 базовых дисциплин учебного плана с кодом Б1.Б.13.03.

Общая трудоемкость освоения дисциплины составляет 180 часов (5 з.е.). Учебным планом предусмотрены лекционные занятия (36 час.), практические занятия (18 часов), лабораторные работы (36 часов), самостоятельная работа (90 час., в том числе 36 часов на подготовку к экзамену). Дисциплина реализуется на 5 курсе в 9 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина логически и содержательно связана с такими курсами, как «Геометрия», «Дискретная математика», «Теория вероятностей и математическая статистика», «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:

- 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.

Задачи:

- последовательное изложение теоретического материала на лекциях, при котором все основные результаты снабжаются строгими доказательствами;
- 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 использовать языки и системы программирования, инструментальные средства для решения профессиональных, исследовательских и прикладных задач (ОПК-8).

В результате изучения данной дисциплины у обучающихся формируются следующие общепрофессиональные, профессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	**Этапы формирования компетенции**	
(ОПК-10) способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах	Знает	базовые структуры данных; современные технологии программирования
	Умеет	планировать разработку сложного программного обеспечения; проводить оценку сложности алгоритмов; разрабатывать эффективные алгоритмы и программы
	Владеет	навыками документирования программного обеспечения; навыками разработки алгоритмов решения типовых профессиональных задач
ПСК-2.2 способность на основе анализа	Знает	основные понятия алгебраической геометрии: аффинные и проективные пространства,

применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах		алгебраические многообразия, дивизоры, и т.д
	Умеет	оценивать качество криптографической защиты
	Владеет	навыками криптоанализа асимметричных систем шифрования
ПСК-2.3 способность 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 способность 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: конспект (ПР-7), собеседование (ОУ-1), коллоквиум (ОУ-2), лабораторные работы (ПР-6).

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 (18 час.)

Занятие 1. Аффинные и проективные пространства (2 час.)

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

Занятие 2. Дивизоры (2 час.)

1. Группы классов дивизоров на алгебраических кривых.

Занятие 3. Эллиптические кривые (2 час.)

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

Занятие 4. Эндоморфизмы эллиптических кривых (2 час.)

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

Занятие 5. Многочлены деления (2 час.)

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

Занятие 6. Эллиптические кривые над полем комплексных чисел (2 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 (2 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 (2 час.)

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

Занятие 9. Криптографические приложения эллиптических кривых

(2 час.)

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

Лабораторные работы (36 час.)

Лабораторная работа №1. Элементы алгебраической геометрии (12 час.)

Лабораторная работа №2. Эллиптические кривые в криптографии (12 час.)

Лабораторная работа №3. Дискретное логарифмирование на эллиптической кривой (12 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	ОПК-10 ПСК-2.2 ПСК-2.3 ПСК-2.6	Умеет	собеседование (ОУ-1), коллоквиум (ОУ-2).	1-4
			Знает	лабораторные	1-4

				работы (ПР-6)	
			Владеет	конспект (ПР-7),	1-4
			Умеет	собеседование (ОУ-1), коллоквиум (ОУ-2).	5-18
2	Раздел II. Эллиптические кривые	ОПК-10 ПСК-2.2 ПСК-2.3 ПСК-2.6	Знает	лабораторные работы (ПР-6)	5-18
			Владеет	конспект (ПР-7),	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. Начертательная геометрия [Электронный ресурс] : методические указания / . — Электрон. текстовые данные. — Иваново: Ивановский государственный архитектурно-строительный университет, ЭБС АСВ, 2011. — 32 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/17738.html

2. Ивлева А.М. Линейная алгебра. Аналитическая геометрия [Электронный ресурс] : учебное пособие / А.М. Ивлева, П.И. Прилуцкая, И.Д. Черных. — Электрон. текстовые данные. — Новосибирск: Новосибирский государственный технический университет, 2014. — 180 с. — 978-5-7782-2409-4. — Режим доступа: http://www.iprbookshop.ru/45380.html

Дополнительная литература

1. Щербакова Ю.В. Аналитическая геометрия [Электронный ресурс] : учебное пособие / Ю.В. Щербакова. — Электрон. текстовые данные. — Саратов: Научная книга, 2012. — 159 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/6259.html

2. Аналитическая геометрия [Электронный ресурс] : практикум. Учебное

пособие / Е.Б. Малышева [и др.]. — Электрон. текстовые данные. — М. : Московский государственный строительный университет, ЭБС АСВ, 2014. — 99 с. — 978-5-7264-0826-2. — Режим доступа: http://www.iprbookshop.ru/26850.html

3. 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

Перечень информационных технологий и программного обеспечения

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 314, Специализированная лаборатория кафедры ИБ. Учебная аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от 18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно. 4) MathCad Education Universety Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно. 5) Corel Academic Site. Поставщик Софт Лайн Трейд. Договор ЭА-442-15 от 18.01.16 лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019. 6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18 лот 4. Срок действия договора 20.09.2018. Лицензия до 30.06.2020
Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 546а, Компьютерный класс, аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от 18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно. 4) MathCad Education Universety Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно. 5) Corel Academic Site. Поставщик Софт Лайн Трейд. Договор ЭА-442-15 от 18.01.16 лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019.

	6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18 лот 4. Срок действия договора 20.09.2018. Лицензия до 30.06.2020.
Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус L, ауд. L 574, специализированная лаборатория кафедры ОиГ: Лаборатория океанологических измерений. Учебная аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	1) IBM SPSS Statistics Premium Campus Edition. Поставщик ЗАО Прогностические решения. Договор ЭА-442-15 от 18.01.16 лот 5. Срок действия договора 30.06.2016. Лицензия бессрочно. 2) SolidWorks Campus 500. Поставщик Солид Воркс Р. Договор 15-04-101 от 23.12.2015. Срок действия договора 15.03.2016. Лицензия бессрочно. 3) АСКОН Компас 3D v17. Поставщик Навиком. Договор 15-03-53 от 20.12.2015. Срок действия договора 31.12.2015. Лицензия бессрочно. 4) MathCad Education Universety Edition. Поставщик Софт Лайн Трейд. Договор 15-03-49 от 02.12.2015. Срок действия договора 30.11.2015. Лицензия бессрочно. 5) Corel Academic Site. Поставщик Софт Лайн Трейд. Договор ЭА-442-15 от 18.01.16 лот 4. Срок действия договора 30.06.2016. Лицензия закончилась 28.01.2019. 6) Microsoft Office, Microsoft Visual Studio. Поставщик Софт Лайн Трейд. Договор ЭА-261-18 от 02.08.18 лот 4. Срок действия договора 20.09.2018. Лицензия до 30.06.2020.

Количество аудиторных часов, отведенных на изучение дисциплины «Методы алгебраической геометрии в криптографии», составляет 90 часов. На самостоятельную работу отведено 90 часа, из них 36 часов на подготовку к экзамену.

Аудиторная нагрузка состоит из 36 лекционных часов, 18 часов практических работ и 36 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 D, ауд. D 314, Специализированная лаборатория кафедры ИБ. 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 – 15) Оборудование: "Компьютер DNS Office (автоматизированное рабочее место), Рабочее место сотрудников в составе: системный блок, клавиатура, мышь, монитор 17"" Aser-173 Мультимедийное оборудование: Экран проекционный ScreenLine Trim White Ice 50 см черная кайма сверху, размер рабочей области 236x147 см Документ-камера Avervision CP355AF ЖК-панель 47"", Full HD, LG M4716 CCBA Мультимедийный проектор Mitsubishi EW33OU, 3000 ANSI Lumen, 1280x800 Сетевая видеокамера Multipix MP-HD718 Доска аудиторная

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 546а, Компьютерный класс, 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 – 15) Оборудование: Компьютер (твердотельный диск - объемом 128 ГБ; жесткий диск - объем 1000 ГБ; форм-фактор - Tower; комплектуется клавиатурой, мышью, монитором AOC i2757Fm; комплектом шнуров эл. питания) модель - M93p 1 Доска аудиторная
Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус L, ауд. L 574, специализированная лаборатория кафедры ОиГ: Лаборатория океанологических измерений. 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 – 24) Оборудование: Доска аудиторная, переносной компьютер (ноутбук Lenovo) с сумкой – 1 шт. T,S - анализатор, батометр металлический (2 шт), вертушки, вольтметр универсальный В7-26, гальванометр, гальванометр зеркальный постоянного тока, генератор сигналов низкочастотный ГЗ-109, генератор сигналов низкочастотный прецезионный, зонд STD Mark-3, зонд STD-1000 (2 шт), зонд АЦИТ, измеритель напряженности магнитного поля, кондуктометр переменного тока, микровольтметр В3-57, осциллограф, осциллограф универсальный запоминающий, плоттер, селективный нановольтметр, универсальный измерительный мост TESLA, усилитель высокочастотный широкополосный УЗ-29, электросолемеры

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»
Специальность 10.05.01 Компьютерная безопасность
(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 недели обучения	Подготовка к лабораторным и практическим занятиям	54	Отчёт по лабораторной работе
2	Сессия	Подготовка к экзамену	36	Экзамен

Подготовка отчета по лабораторным работам и практическим занятиям предполагает повторение лекционного материала и выполнение задания для лабораторных и практических работ по темам из Раздела II РПУД.

В ходе самостоятельной работы обучающийся должен подготовить для сдачи отчёт по проделанной работе. Необходимо указать в отчёте следующую информацию: название и цель работы, краткий теоретический материал, задание на лабораторную или практическую работу, ход работы, полученные результаты и выводы. По результатам защиты отчёта студенту выставляется «зачтено» или «не зачтено». Студент получает «зачтено», если отчёт содержит все перечисленные ранее пункты и оформлен в соответствии с правилами оформления письменных работ.

Для допуска к экзамену обучающийся должен получить оценку «зачтено» по всем практическим и лабораторным работам курса. На основании сдачи работ выставляется зачёт.

Самостоятельная работа при подготовке к экзамену включает изучение теоретического материала с использованием лекционных материалов, а также основной и дополнительной литературы из списка рекомендуемых источников. Список вопросов для подготовки к экзамену, а также методические рекомендации по оцениванию представлены в Приложении 2 РПУД.

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»
Специальность 10.05.01 Компьютерная безопасность
(Математические методы защиты информации)
Форма подготовки очная

Владивосток
2019

Паспорт ФОС

Код и формулировка компетенции	Этапы формирования компетенции	
(ОПК-10) способность к самостоятельному построению алгоритма, проведению его анализа и реализации в современных программных комплексах	Знает	базовые структуры данных; современные технологии программирования
	Умеет	планировать разработку сложного программного обеспечения; проводить оценку сложности алгоритмов; разрабатывать эффективные алгоритмы и программы
	Владеет	навыками документирования программного обеспечения; навыками разработки алгоритмов решения типовых профессиональных задач
ПСК-2.2 способность 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 способность 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 способность 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	ОПК-10 ПСК-2.2 ПСК-2.3 ПСК-2.6	Умеет	собеседование (ОУ-1), коллоквиум (ОУ-2).	1-4
			Знает	лабораторные работы (ПР-6)	1-4
			Владеет	конспект (ПР-7),	1-4
2	Раздел II. Эллиптические кривые	ОПК-10 ПСК-2.2 ПСК-2.3 ПСК-2.6	Умеет	собеседование (ОУ-1), коллоквиум (ОУ-2).	5-18
			Знает	лабораторные работы (ПР-6)	5-18
			Владеет	конспект (ПР-7),	5-18

Шкала оценивания уровня сформированности компетенций

Код и формулировка компетенции	**Этапы формирования компетенции**		**критерии**	**показатели**
ПСК-2.2 способностью на основе анализа применяемых математических методов и алгоритмов оценивать эффективность средств и методов защиты информации в компьютерных системах	Знает (пороговый уровень)	Основные понятия алгебраической геометрии: аффинные и проективные пространства, алгебраические многообразия, дивизоры, и т.д.	полнота и системность знаний	знает основные термины и понятия алгебраической геометрии; способен анализировать математические явления и процессы при решении профессиональных задач
	Умеет (продвинутый)	Оценивать качество криптографической защиты;	степень самостоятельности и	Самостоятельно применяет основы алгебраической

			понимания своих действий	геометрии в профессиональной и иной деятельности. Свободно отвечает на вопросы, касающиеся своих действий.
	Владеет (высокий)	Навыками криптоанализа асимметричных систем шифрования.	степень владения инструментом для решения заданий	способен свободно решать профессиональные задачи с использованием математического аппарата, применять основы алгебраической геометрии в криптологии
ПСК-2.3 способностью разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации	Знает (пороговый уровень)	Принципы применения эллиптических и гиперэллиптических кривых в криптографии;	полнота и системность знаний	знает основные термины и понятия алгебраической геометрии; способен анализировать математические явления и процессы при решении профессиональных задач
	Умеет(продвинутый)	Разрабатывать быстрые вычислительные алгоритмы для криптографических приложений;	степень самостоятельности и понимания своих действий	Способен самостоятельно разработать вычислительный алгоритм, использующий

				методы алгебраической геометрии в крпитографии. Свободно отвечает на вопросы, касающиеся своих действий.
	Владеет (высокий)	Навыками программирования алгебраических операций в конечных алгебраических структурах, в том числе в группе точек эллиптических и гиперэллиптических кривых.	степень владения инструментом для решения заданий	способен свободно решать профессиональные задачи с использованием математического аппарата, применять основы алгебраической геометрии в криптологии
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 (пороговый уровень)	Принципы и методы построения быстрых алгоритмов для реализации систем защиты информации;	полнота и системность знаний	знает основные термины и понятия алгебраической геометрии; способен анализировать математические явления и процессы при решении профессиональных задач
	Умеет(продвинутый)	Проводить предварительное оценивание временной сложности разрабатываемых алгоритмов	степень самостоятельности и понимания своих действий	Самостоятельно применяет основы алгебраической геометрии в профессиональной и

				иной деятельности. Свободно отвечает на вопросы, касающиеся своих действий.
	Владеет (высокий)	Методами алгебраической геометрии в криптографии.	степень владения инструментом для решения заданий	способен свободно решать профессиональные задачи с использованием математического аппарата, применять основы алгебраической геометрии в криптологии

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

Промежуточная форма аттестации по данной дисциплине – зачёт и экзамен.

Для допуска к экзамену обучающийся должен получить оценку «зачтено» по всем практическим и лабораторным работам курса. Критерии оценивания практических работ представлены далее в данном Приложении. На основании сдачи работ выставляется зачёт.

Экзамен проводятся в форме собеседования (УО-1), вопросы к экзамену соответствуют темам, изучаемым на лекционных занятиях, и представлены далее в Приложении. Для подготовки к ответу на экзамене обучающийся получает 20 минут. В ходе подготовки обучающийся может составлять любые записи, однако оценивается прежде всего устный, а не письменный ответ.

При определении оценки учитываются:

- соблюдение норм литературной речи;
- полнота и содержательность ответа;
- умение привести примеры;

- умение пользоваться дополнительной литературой при подготовке к занятиям;

- соответствие представленной в ответах информации материалам лекций и учебной литературы, актуальным сведениям из информационных ресурсов Интернет.

- умение использовать фундаментальные понятия из базовых естественнонаучных и общепрофессиональных дисциплин при ответе.

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.

На экзамене каждый экзаменационный билет содержит два вопроса из списка выше. Результаты экзамена оцениваются по четырёх балльной системе

(«отлично», «хорошо», «удовлетворительно», «неудовлетворительно») и заносятся в экзаменационную ведомость и зачетную книжку. В зачетную книжку заносятся только положительные оценки.

При определении оценки учитываются:

- полнота и содержательность ответа;
- умение привести примеры;
- умение пользоваться дополнительной литературой при подготовке к занятиям;
- соответствие представленной в ответах информации материалам лекций и учебной литературы, сведениям из информационных ресурсов Интернет.

Оценка **«отлично».** Ответы на поставленные вопросы в билете излагаются логично, последовательно и не требуют дополнительных пояснений. Делаются обоснованные выводы. Демонстрируются глубокие знания дисциплины. Соблюдаются нормы литературной речи.

Оценка **«хорошо».** Ответы на поставленные вопросы излагаются систематизировано и последовательно. Материал излагается уверенно. Демонстрируется умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер. Соблюдаются нормы литературной речи.

Оценка **«удовлетворительно».** Допускаются нарушения в последовательности изложения. Демонстрируются поверхностные знания вопроса. Имеются затруднения с выводами. Допускаются нарушения норм литературной речи.

Оценка **«неудовлетворительно».** Материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний по дисциплине. Имеются заметные нарушения норм литературной речи.

В случае неявки студента на экзамен в экзаменационной ведомости делается отметка «не явился».

Оценочные средства для текущей аттестации

В качестве оценочных средств для текущей аттестации применяются лабораторные работы (ПР-6) и конспект (ПР-7).

Конспект является показателем сформированности компетенции на пороговом и продвинутом уровнях. Темы конспектов соответствуют темам теоретической части курса из Раздела I РПУД. Критерии оценки по данному виду оценочных средств представлены в таблице:

Оценка	Содержание конспекта
Отлично	Конспект содержит все понятия, термины, положения, изученные на лекции и/или с использованием основных источников литературы, а также содержит сведения из дополнительных источников.
Хорошо	Конспект содержит все понятия, термины, положения, изученные на лекции и/или с использованием основных источников литературы.
Удовлетворительно	Конспект содержит базовые понятия, термины, положения, изученные на лекции.
Неудовлетворительно	Конспект не содержит основных понятий, терминов, положений по данной теме.

Для оценки высокого уровня сформированности компетенции проводятся лабораторные работы. Темы лабораторных работ представлены в Разделе II РПУД. Критерии оценки по данному виду оценочных средств представлены в таблице:

Оценка	Критерий
Зачтено	Отчёт по лабораторной работе содержит все необходимые пункты (цель работы, краткий теоретический материал, задание на лабораторную работу, ход работы, полученные результаты, выводы). Оформление отчёта соответствует правилам оформления письменных работ.
Незачтено	Отчёт по лабораторной работе не содержит какого-либо необходимого пункта(ов) и/или оформление отчёта не соответствует правилам оформления письменных работ.