МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
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.
всего часов аудиторной нагрузки 108 час.
в том числе с использованием МАО 9 час.
самостоятельная работа 72 час.
в том числе на подготовку к экзамену 27 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 : Боршевников А.Е., ассистент штатный

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. 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: *Borshevnikov A.E.*

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

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

Learning outcomes:

- (CPM-2.2) the ability, 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) the ability to build mathematical models to assess the security of computer systems and analyze the components of the security system using modern mathematical methods
- (CPM-2.5) 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: This discipline is one of the fundamental parts of modern theoretical cryptography, without the knowledge of which no further training is possible in the field of modern information security. 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 c. — 978-5-7782-2409-4. — Режим доступа: http://www.iprbookshop.ru/45380.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

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 направления 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав базовых дисциплин базовой части учебного плана Б1.Б.7.3.

Общая трудоемкость дисциплины составляет 180 часов (5 з.е.). Учебным планом предусмотрены лекционные занятия (36 часов, в том числе 9 часов в интерактивной форме), лабораторные занятия – (18 часов), практическая работа – (54 часа), самостоятельная работа – (72 часа, в том числе 27 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 «Дискретная математика», «Математическая логика и теория алгоритмов» и «Теоретико-числовые методы в криптографии».

Данная дисциплина 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.

Цель изучения дисциплины «Методы алгебраической геометрии в криптографии» заключается в формировании представления 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).

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

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	методы анализа и обоснования адекватности математических процессов, возникающих при работе программно-аппаратных средств защиты информации.
	Умеет	разрабатывать, анализировать и обосновывать адекватность математических моделей процессов.

	Владеет	способностью разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации.
(ПСК-2.3) способностью строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов	Знает	основные алгоритмы эллиптической криптографии.
	Умеет	моделировать алгоритмы в системах компьютерной математики, оценивать эффективность.
	Владеет	способностью моделировать алгоритмы , владеть методами оценивания их работоспособности и эффективности.

(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	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.

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), лабораторные работы (ПР-6), собеседование (ОУ-1), коллоквиум (ОУ-2).

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Раздел I. Геометрия на плоскости (18 час.)

Тема 1. Определители и системы (1 час.)
Тема 2. Координаты (1 час.)
Тема 3. Введение в линейную алгебру (6 час.)
Тема 4. Линейная зависимость. Базис (6 час.)
Тема 5. Прямая на плоскости (2 час.)
Тема 6. Кривые второго порядка (2 час.)

Раздел II. Геометрия в пространстве (18 час.)

Тема 1. Плоскость (6 час.)
Тема 2. Прямая в пространстве (6 час.)
Тема 3. Поверхности (6 час.)

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практические занятия (54 час.)

Занятие 1. Определители и системы малых порядков (3 час.)

Занятие 2. Метод Гаусса (3 час.)

Занятие 3. Декартовы координаты (3 час.)

Занятие 4. Координаты (3 час.)

Занятие 5. Матричная алгебра. Обращение матриц (3 час.)

Занятие 6. Векторные пространства (3 час.)

Занятие 7. Базис векторного пространства (3час.)

Занятие 8. Преобразование координат (3 час.)

Занятие 9. Векторная алгебра (3 час.)

Занятие 10. Уравнения прямой (3 час.)

Занятие 11. Кривые второго порядка (3 час.)

Занятие 12. Уравнения плоскости (3 час.)

Занятие 13. Взаимное расположение плоскостей (3 час.)

Занятие 14. Прямая в пространстве (3 час.)

Занятие 15. Взаимное расположение прямой и плоскости (3 час.)

Занятие 16. Поверхности второго порядка (3 час.)

Занятие 17. Канонические уравнения поверхностей второго порядка

(3 час.)

Занятие 18. Подпространства линейного пространства (3 час.)

Лабораторные работы (18 час.)

Лабораторная работа № 1. Методы векторов. (10 час.)

Лабораторная работа № 2. Подпространства (8 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
	Раздел I. Геометрия на плоскости	ПСК-2.2 ПСК-2.3 ПСК-2.5	Умеет	собеседование (ОУ-1) коллоквиум (ОУ-2)	1-35
			Знает	лабораторные	1-35

			работы (ПР-6),	
		Владеет	конспект (ПР-7)	1-35
Раздел II. Геометрия в пространстве	ПСК-2.2 ПСК-2.3 ПСК-2.5	Умеет	собеседование (ОУ-1) коллоквиум (ОУ-2)	36-71
		Знает	лабораторные работы (ПР-6),	36-71
		Владеет	конспект (ПР-7)	36-71

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 c. — 978-5-7782-2409-4. — Режим доступа: http://www.iprbookshop.ru/45380.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

Дополнительная литература

1. Щербакова Ю.В. Аналитическая геометрия [Электронный ресурс] : учебное пособие / Ю.В. Щербакова. — Электрон. текстовые данные. —

Саратов: Научная книга, 2012. — 159 c. — 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 c. — 978-5-7264-0826-2. — Режим доступа: http://www.iprbookshop.ru/26850.html

Перечень информационных технологий и программного обеспечения

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 732, 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. Срок действия договора 20.09.2018. Лицензия до 30.06.2020.

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Методы алгебраической геометрии в криптографии», составляет 90 часа. При этом аудиторная нагрузка состоит из 54 лекционных часов и 36 часов практических занятий.

Обучающийся получает теоретические знания на лекциях. В ходе подготовки к лекциям должны использоваться источники из списка учебной литературы.

Подготовка к практическим занятиям предполагает повторение лекционного материала. В результате студент должен быть готов к выполнению заданий на практическом занятии. Основной практической составляющей является выполнение одного практического задания с последующим предоставлением отчета о выполнении.

В рамках указанной дисциплины итоговой формы аттестации является экзамен. Самостоятельная работа при подготовке к экзамену включает изучение теоретического материала с использованием лекционных материалов, рекомендуемых источников и материалов по практическим занятиям.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 732, 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 – 48) Оборудование: Экран проекционный Projecta Elpro Large Electron, 500x316 см, размер рабочей области 490x306 Документ-камера Avervision CP 355 AF Мультимедийный проектор Panasonic PT-DZ11OXE, 10 600 ANSI Lumen, 1920x1200 Сетевая видеокамера Multipix MP-HD718 ЖК-панель 47"", Full HD, LG M4716 CCBA ЖК-панель 42"", Full HD, LG M4214 CCBA ЖК-панель 42"", Full HD, LG M4214 CCBA", 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»
Специальность 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	1-8 неделя обучения	Контрольная работа № 1. Векторная алгебра	22	Оценка работы
2	9-18 неделя обучения	Контрольная работа № 2. Геометрия в пространстве	23	Оценка работы
3	Сессия	Подготовка к экзамену	27	Экзамен

Подготовка к практическим занятиям предполагает повторение лекционного материала. В результате студент должен быть готов на практическом занятии представить решение обозначенных задач.

Для выполнения индивидуального задания преподаватель выдает обучающемуся задачу. В результате студент должен на практическом занятии представить решение задачи.

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
специализация «Математические методы защиты информации»
Форма подготовки очная

Владивосток
2019

Паспорт фонда оценочных средств

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	методы анализа и обоснования адекватности математических процессов, возникающих при работе программно-аппаратных средств защиты информации.
	Умеет	разрабатывать, анализировать и обосновывать адекватность математических моделей процессов.
	Владеет	способностью разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации.
(ПСК-2.3) способностью строить математические модели для оценки безопасности компьютерных систем и анализировать компоненты системы безопасности с использованием современных математических методов	Знает	основные алгоритмы эллиптической криптографии.
	Умеет	моделировать алгоритмы в системах компьютерной математики, оценивать эффективность.

	Владеет	способностью моделировать алгоритмы , владеть методами оценивания их работоспособности и эффективности.
(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	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.

Контроль достижения целей курса

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства - наименование	
				текущий контроль	промежуточная аттестация
	Раздел I. Геометрия на плоскости	ПСК-2.2 ПСК-2.3 ПСК-2.5	Умеет	собеседование (ОУ-1) коллоквиум (ОУ-2)	1-35
			Знает	лабораторные работы (ПР-6),	1-35
			Владеет	конспект (ПР-7)	1-35
	Раздел II. Геометрия в пространстве	ПСК-2.2 ПСК-2.3 ПСК-2.5	Умеет	собеседование (ОУ-1) коллоквиум (ОУ-2)	36-71
			Знает	лабораторные работы (ПР-6),	36-71
			Владеет	конспект (ПР-7)	36-71

Шкала оценивания уровня сформированности компетенций

Код и формулировка компетенции	**Этапы формирования компетенции**		**критерии**	**показатели**
(ПСК-2.1) способностью разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации	Знает (пороговый уровень)		Полнота с системность знаний.	стандартные алгоритмы применяемых методов.
	Умеет (продвинутый)		Степень самостоятельности.	проводить научные эксперименты, обрабатывать результаты эксперимента.
	Владеет (высокий)		Степень владения.	владеть компьютерными

				пакетами для проведения исследовательских экспериментов.
(ПСК-2.3) способностью разрабатывать вычислительные алгоритмы, реализующие современные математические методы защиты информации	Знает(пороговый уровень)		Полнота с системность знаний.	методы анализа и обоснования адекватности математических процессов
	Умеет(продвинутый)		Степень самостоятельности.	разрабатывать, анализировать и обосновывать адекватность математических моделей процессов.
	Владеет (высокий)		Степень владения.	способностью разрабатывать, анализировать и обосновывать адекватность математических моделей процессов.
(ПСК-2.4) способностью моделировать алгоритмы в системах компьютерной математики, оценивать их	Знает(пороговый уровень)		Полнота с системность знаний.	основные алгоритмы эллиптической криптографии
	Умеет(продвинутый)		Степень самостоятельности.	моделировать алгоритмы в системах компьютерной математики,

работоспособность и эффективность				оценивать эффективность
	Владеет (высокий)		Степень владения.	способностью моделировать алгоритмы.

(ПСК-2.6) способностью разрабатывать, анализировать и обосновывать адекватность математических моделей процессов, возникающих при работе программно-аппаратных средств защиты информации	Знает(пороговый уровень)		Полнота с системность знаний.	методы анализа и обоснования адекватности математических процессов
	Умеет(продвинутый)		Степень самостоятельности.	разрабатывать, анализировать и обосновывать адекватность математических моделей процессов.
	Владеет (высокий)		Степень владения.	способностью разрабатывать, анализировать и обосновывать адекватность математических моделей процессов.
(ПСК-2.7) способностью проводить сравнительный анализ и осуществлять обоснованный	Знает(пороговый уровень)		Полнота с системность знаний.	основные алгоритмы эллиптической криптографии
	Умеет(продвинутый)		Степень самостоятельности.	моделировать алгоритмы в системах

выбор программно-аппаратных средств защиты информации				компьютерной математики, оценивать эффективность

Методические рекомендации, определяющие процедуры оценивания результатов освоения дисциплины

Заполняется в соответствии с Положением о фондах оценочных средств образовательных программ высшего образования – программ бакалавриата, специалитета, магитратуры ДВФУ, утвержденным приказом ректора от 12.05.2015 №12-13-850.

Оценочные средства для промежуточной аттестации

Вопросы к экзамену

1. Определители второго порядка.
2. Система двух уравнений с двумя неизвестными. Правило Крамера.
3. Система двух уравнений с двумя неизвестными с определителем равным нулю
4. Геометрическая интерпретация решения системы двух уравнений с двумя неизвестными
5. Свойства определителей третьего порядка. Система трех уравнений с тремя неизвестными
6. Метод Гаусса
7. Однородные системы *n* уравнений с *n* неизвестными
8. Декартовы координаты на прямой
9. Декартовы координаты на плоскости и в пространстве

10. Проекция вектора на ось. Расстояние между двумя точками
11. Деление отрезка в заданном отношении
12. Аффинная система координат. Понятие проекции
13. Полярные координаты на плоскости. Связь с ДПСК
14. Полярные координаты в пространстве: сферические и цилиндрические
15. Понятие векторного пространства
16. Следствие аксиом векторного пространства
17. Примеры векторных пространств: геом. векторы, нулевое, координатное
18. Действия сложения и умножения на число над матрицами
19. Ассоциативность умножения матриц.
20. Обзор действий над матрицами
21. Определитель произведения матриц
22. Обращение матриц.
23. Матричные группы. Классические линейные группы *GL, SL*
24. Матричная форма теоремы Крамера
25. Линейная комбинация. Линейная зависимость и независимость
26. Лемма о линейной зависимости s векторов в n-мерном пространстве при $s > n$.
27. Основная теорема о двух системах векторов и ее следствия
28. Эквивалентные системы векторов и максимальные линейно независимые системы. Ранг системы векторов
29. Базис векторного пространства. Порождающая совокупность
30. Три эквивалентных определения базиса
31. Теорема о координатах вектора в базисе и ее следствия
32. Изоморфизм векторных пространств
33. Единственность разложения по базису
34. Координаты вектора в разных базисах
35. Перенос начала, переход к системе координат с тем же началом, переход к системе координат с изменением начала
36. Преобразование декартовой системы координат

37. Скалярное произведение

38. Векторное произведение

39. Смешанное произведение

40. Уравнения прямой на плоскости: общее, с угловым коэффициентом, через заданную точку в заданном направлении, через две точки, уравнение прямой в отрезках, параметрическое уравнение прямой

41. Уравнение прямой нормального вида. Расстояние от точки до прямой

42. Вывод уравнения эллипса. Свойства эллипса

43. Вывод уравнения гиперболы. Свойства гиперболы

44. Вывод уравнения параболы. Свойства параболы

45. Диаметры и директрисы КВП

46. Уравнения КВП в полярных координатах

47. Лемма о преобразовании уравнения КВП к виду без слагаемого, содержащего xy

48. Лемма о преобразовании уравнения КВП к виду без слагаемого, содержащего x (y)

49. Основная классификационная теорема о КВП.

50. Уравнение плоскости, проходящей через точку с нормальным вектором

51. Теорема о параллельности вектора и плоскости. Исследование общего уравнения плоскости

52. Параметрическое уравнение плоскости

53. Уравнение плоскости, проходящей через три точки

54. Уравнение плоскости в отрезках

55. Взаимное расположение двух плоскостей

56. Взаимное расположение трех плоскостей

57. Нормальное уравнение плоскости. Расстояние от точки до плоскости

58. Параметрические и канонические уравнения прямой в пространстве

59. Уравнение прямой, проходящей через две точки

60. Прямая как пересечение двух плоскостей. Взаимное расположение двух прямых в пространстве

61. Угол между двумя прямыми, параллельность и перпендикулярность

62. Расстояние от точки до прямой

63. Взаимное расположение прямой и плоскости

64. Угол между прямой и плоскостью, параллельность и перпендикулярность

65. Уравнение перпендикуляра, опущенного из точки на прямую

66. Теорема об уравнении цилиндрической поверхности

67. Цилиндры второго порядка: эллиптический, гиперболический и параболический

68. Поверхности вращения: эллипсоид, гиперболоиды однополостный и двуполостный, параболоид, конус

69. Сжатие и растяжение поверхностей. Канонические уравнения поверхностей второго порядка

70. Гиперболический параболоид

71. Метод сечений при исследовании формы поверхностей: эллипсоид, гиперболоиды однополостный и двуполостный, эллиптический параболоид, конус

Оценочные средства для текущей аттестации

Приводятся типовые оценочные средства для текущей аттестации и критерии оценки к ним (по каждому виду оценочных средств) в соответствии с Положением о фондах оценочных средств образовательных программ высшего образования – программ бакалавриата, специалитета, магитратуры ДВФУ, утвержденным приказом ректора от 12.05.2015 №12-13-850.