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
Геометрические аспекты криптологии
Специальность 10.05.01 Компьютерная безопасность
(Математические методы защиты информации)
Форма подготовки очная

курс 1, 2 семестр 2
лекции 18 час.
практические занятия 36 час.
лабораторные работы 00 час.
в том числе с использованием МАО лек. 00 / пр. 36 / лаб. 00 час.
в том числе в электронной форме лек. 00 / пр. 00 / лаб. 00 час.
всего часов аудиторной нагрузки 54 час.
в том числе с использованием МАО 36 час.
в том числе в электронной форме 00 час.
самостоятельная работа 54 час.
в том числе на подготовку к экзамену 27 час.
курсовая работа / курсовой проект не предусмотрены
зачет не предусмотрен
экзамен 2 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): Зотов С.С. Ассистент.

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: *Geometric aspects of cryptology*

Basic part of Block 1, _3_credits

Instructor: *Zotov S.S.*

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

• 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:

(OPK-2) the ability to correctly apply when 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

Course description:

Discipline is prior to the courses of mathematical analysis, differential equations, mechanics, discrete mathematics, physics.

Main course literature:

1. Шепелева Р.П. Курс высшей математики : учебное пособие. ладивосток : Изд-во Дальневосточного федерального университета, 2011. – 337 с. - http://lib.dvfu.ru:8080/lib/item?id=chamo:418094&theme=FEFU

2. Кадомцев, С. Б.. Аналитическая геометрия и линейная алгебра. [Электронный ресурс] / Кадомцев С. Б. - 2-е изд., испр. и доп. - М. : ФИЗМАТЛИТ, 2011. - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785922112901.html

3. Грешилов, А.А. Аналитическая геометрия. Векторная алгебра. Кривые второго порядка [Электронный ресурс]: Учеб. пособие. / Под ред. А.А. Грешилова - М. : Логос, 2017. - Режим доступа: http://www.studentlibrary.ru/book/ISBN5940102042.html

4. Шерстов, С.В. Аналитическая геометрия и линейная алгебра : матрицы и системы уравнений [Электронный ресурс] / Шерстов С.В. - М. : МИСиС, 2015. - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785876239709.html

Form of final control: *exam*

Аннотация к рабочей программе дисциплины
«Геометрические аспекты криптологии»

Рабочая программа учебной дисциплины «Геометрические аспекты криптологии» разработана для студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав базовых дисциплин учебного плана с кодом Б1.Б.12.2.

Общая трудоемкость дисциплины составляет 3 зачетных единицы, 108 часов. Учебным планом предусмотрены лекционные занятия (18 часов), практические занятия (36 часов), самостоятельная работа студента (54 часа, в том числе 27 часов на подготовку к экзамену). Дисциплина реализуется на 1 курсе в 2 семестре. Форма контроля по дисциплине – экзамен.

Дисциплина логически и содержательно связана с такими курсами, как «Математический анализ», «Введение в алгебру», «Основы геометрии».

Дисциплина является предшествующей к курсам математического анализа, дифференциальных уравнений, механики, дискретной математики, физики.

Цель дисциплины – 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 дисциплины - реализация указанных целей включает последовательное изложение теоретического материала на лекциях, при котором все основные результаты снабжаются строгими доказательствами; отработку приемов решения задач на практических занятиях; промежуточный и итоговый контроль выявляют степень усвоения навыков.

Для успешного изучения дисциплины «Геометрические аспекты криптологии» у обучающихся должны быть сформированы следующие предварительные компетенции:

- 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 общепрофессиональные компетенции (элементы компетенций).

Код и формулировка компетенции	**Этапы формирования компетенции**	
(ОПК-2) 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	Знает	понятия линейного, аффинного, евклидова пространств, базиса, системы координат, прямой, плоскости, угла, объема (длины, площади), алгебраической поверхности (кривой) второго порядка, преобразования.
	Умеет	переходить от одной системы координат к другой в аффинном, и евклидовом пространствах, исследовать взаимное расположение прямых, плоскостей, кривых и поверхностей второго порядка в пространстве, решать метрические задачи с участием плоскостей (прямых) и алгебраических поверхностей (кривых) второго порядка, приводить алгебраические кривые и поверхности второго порядка к каноническому виду согласно аффинной и метрической классификациям.
	Владеет	аппаратом векторной алгебры в трехмерном евклидовом пространстве, навыками работы в различных системах координат, аналитическими и алгебраическими методами классификации поверхностей (кривых) второго порядка, выполнения преобразований пространства.

Для формирования вышеуказанных компетенций в рамках дисциплины «Геометрические аспекты криптологии» 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).

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Раздел I. Определители и системы (2 час.)

Тема 1. Системы линейных уравнений (2 час.)

Понятие о видах СЛАУ и методах их решений

Раздел II. Координаты (2 час.)

Тема 2. Декартовы координаты (1 час.)

Расположение точки *P* на плоскости определяется декартовыми координатами с помощью пары чисел (x,y)

Тема 3. Полярные координаты (1 час.)

В полярной системе координат, применяемой на плоскости, положение точки *P* определяется её расстоянием до начала координат $r = |OP|$ и углом φ её радиус-вектора к оси *Ox*.

Раздел III. Введение в линейную алгебру (2 час.)

Тема 1. Векторные пространства. Определение и примеры векторных пространств (1 час.)

Математическая структура, которая представляет собой набор элементов, называемых векторами, для которых определены операции сложения друг с другом и умножения на число — скаляр.

Тема 2. Алгебра матриц (1 час.)

Введение в понятие о матрицах.

Раздел IV. Линейная зависимость. Базис (2 час.)

Тема 1. Линейная зависимость векторов (1 час.)

Понятие о линейно-зависимых и линейно-независимых векторах.

Тема 2. Ранг системы векторов (1 час.)

Понятие о ранге системы векторов.

Раздел V. Прямая на плоскости (2 час.)

Тема 1. Уравнения прямой на плоскости (2 час.)

Вывод уравнения прямой на плоскости

Раздел VI. Кривые второго порядка (2 час.)

Тема1. Эллипс (1 час.)

Уравнение эллипса. Виды эллипсоидов.

Тема2. Гипербола (1 час.)

Уравнение гиперболы. Виды гиперболоидов.

Раздел VI. Плоскость (2 час.)

Тема 1. Общее уравнение плоскости (1 час.)

Уравнение плоскости. Значение его коэффициентов.

Тема 2. Различные уравнения плоскости (1 час.)

Виды уравнений плоскости. Применение уравнений в различных условиях.

Раздел VII. Прямая в пространстве (4 час.)

Тема 1. Уравнения прямой (2 час.)

Уравнение прямой. Значение его коэффициентов.

Тема 2. Взаимное расположение прямой и плоскости (1 час.)

Виды взаимного расположения прямой и плоскости

Тема 3. Цилиндрические поверхности (1 час.)

Виды цилиндрических поверхностей и их уравнения.

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практические занятия (36 час.)

Занятие 1. Определители и системы малых порядков (2 час.)

1. Системы линейных алгебраических уравнений (СЛАУ) 2-го и 3-го порядков.
2. Определение определителя 2-го порядка.
3. Решение СЛАУ 2-го порядка по правилу Крамера.
4. Вычисление определителей 3-го порядка и решение СЛАУ

Занятие 2. Метод Гаусса (2 час.)

1. Системы линейных алгебраических уравнений произвольного вида. Совместные и несовместные системы.
2. Приведение матрицы системы к ступенчатому виду.
3. Определение числа главных и свободных переменных.
4. Нахождение общего и частного решения СЛАУ.

Занятие 3. Декартовы координаты (2 час.)

1. Понятие вектора. Определение. Величина вектора. Нулевой вектор.
2. Равенство векторов. Операции над направленными отрезками – сумма и умножение на число.
3. Декартовы координаты на прямой, плоскости и в пространстве.
4. Деление отрезка в заданном отношении. Формулы для плоскости и пространства.

Занятие 4. Координаты (2 час.)

1. Аффинная система координат. Понятие проекции
2. Полярные координаты на плоскости. Связь с ДПСК
3. Полярные координаты в пространстве: сферические и цилиндрические

Занятие 5. Матричная алгебра. Обращение матриц (2 час.)

1. Действия над матрицами: сложение и умножение на число
2. Обращение матриц
3. Классические линейные группы $GL(n, K)$, $SL(n, K)$
4. Матричная форма теоремы Крамера

Занятие 6. Векторные пространства (2 час.)

1. Понятие векторного пространства, его свойства и примеры.
2. Линейная комбинация векторов.
3. Линейная зависимость и независимость.
4. Ранг системы векторов. Нахождение ранга двумя способами

Занятие 7. Базис векторного пространства (2 час.)

1. Три эквивалентных определения базиса. Примеры.
2. Координаты вектора в базисе.

3. Единственность разложения по базису.
4. Координаты вектора в разных базисах

Занятие 8. Преобразование координат (2 час.)

1. Перенос начала, переход к системе координат с тем же началом, переход к системе координат с изменением начала
2. Преобразование декартовой системы координат
3. Преобразование аффинной системы координат

Занятие 9. Векторная алгебра (2 час.)

1. Скалярное произведение
2. Векторное произведение
3. Смешанное произведение

Занятие 10. Уравнения прямой (2 час.)

1. Уравнение прямой, проходящей через две точки.
2. Уравнение прямой в отрезках.
3. Уравнение прямой нормального вида.
4. Расстояние от точки до прямой

Занятие 11. Кривые второго порядка (2 час.)

1. Кривые второго порядка: окружность, эллипс, гипербола, парабола, их канонические уравнения.
2. Приведение уравнения второго порядка с двумя переменными к каноническому виду.

Занятие 12. Уравнения плоскости (2 час.)

1. Общее уравнение плоскости
2. Различные уравнения плоскости

Занятие 13. Взаимное расположение плоскостей (2 час.)

1. Взаимное расположение двух плоскостей

2. Взаимное расположение трех плоскостей

Занятие 14. Прямая в пространстве (2 час.)

1. Параметрические и канонические уравнения прямой в пространстве
2. Уравнение прямой, проходящей через две точки
3. Прямая как пересечение двух плоскостей. Взаимное расположение двух прямых в пространстве
4. Угол между двумя прямыми, параллельность и перпендикулярность
5. Расстояние от точки до прямой
6. Взаимное расположение прямой и плоскости
7. Угол между прямой и плоскостью, параллельность и перпендикулярность
8. Уравнение перпендикуляра, опущенного из точки на прямую

Занятие 15. Взаимное расположение прямой и плоскости (2 час.)

1. Взаимное расположение прямой и плоскости
2. Угол между прямой и плоскостью, параллельность и перпендикулярность
3. Уравнение перпендикуляра, опущенного из точки на прямую

Занятие 16. Поверхности второго порядка (2 час.)

1. Цилиндры второго порядка.
2. Поверхности вращения

Занятие 17. Канонические уравнения поверхностей второго порядка (2 час.)

1. Гиперболический параболоид.
2. Метод сечений при исследовании формы поверхностей

Занятие 18. Подпространства линейного пространства (2 час.)

1. Сумма и пересечение подпространств.
2. Размерности и базисы суммы и пересечения подпространств

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Название дисциплины» 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	
				текущий контроль	промежуточная аттестация
1	Раздел I. Определители и системы	(ОПК-2)	знает	ПР-7	1-3
			умеет	ПР-7	3-5
			владеет	ОУ-2	*5-7*
2	Раздел II. Координаты	(ОПК-2)	знает	ПР-7	8-10
			умеет	ПР-7	10-12
			владеет	ОУ-2	12-14
3	Раздел III. Введение в линейную алгебру	(ОПК-2)	знает	ПР-7	15
			умеет	ПР-7	16
			владеет	ОУ-2	*17*
4	Раздел IV. Линейная зависимость. Базис	(ОПК-2)	знает	ПР-7	*25-29*
			умеет	ПР-7	*30-35*
			владеет	ОУ-2	*36-39*
5	Раздел V. Прямая на плоскости	(ОПК-2)	знает	ПР-7	*40-43*
			умеет	ПР-7	*44-48*
			владеет	ОУ-2	*49-52*
6	Раздел VI.	(ОПК-2)	знает	ПР-7	*53-56*

	Плоскость		умеет	ПР-7	*56-60*
			владеет	ПР-6	*61-64*
7	Раздел VII. Прямая в пространстве	(ОПК-2)	знает	ПР-7	*65-67*
			умеет	ПР-7	*68,69*
			владеет	ПР-6	*70,71*

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

1. Шепелева Р.П. Курс высшей математики : учебное пособие. ладивосток : Изд-во Дальневосточного федерального университета, 2011. – 337 с. - http://lib.dvfu.ru:8080/lib/item?id=chamo:418094&theme=FEFU

2. Кадомцев, С. Б.. Аналитическая геометрия и линейная алгебра. [Электронный ресурс] / Кадомцев С. Б. - 2-е изд., испр. и доп. - М. : ФИЗМАТЛИТ, 2011. - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785922112901.html

3. Грешилов, А.А. Аналитическая геометрия. Векторная алгебра. Кривые второго порядка [Электронный ресурс]: Учеб. пособие. / Под ред. А.А. Грешилова - М. : Логос, 2017. - Режим доступа: http://www.studentlibrary.ru/book/ISBN5940102042.html

4. Шерстов, С.В. Аналитическая геометрия и линейная алгебра : матрицы и системы уравнений [Электронный ресурс] / Шерстов С.В. - М. : МИСиС, 2015. - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785876239709.html

Дополнительная литература

1. Протасов, Ю.М. Линейная алгебра и аналитическая геометрия [Электронный ресурс] / Протасов Ю.М. - М. : ФЛИНТА, 2017. - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785976509566.html

2. Ивлев, А.М. Линейная алгебра. Аналитическая геометрия [Электронный ресурс]: учеб. пособие / Ивлева А.М. - Новосибирск : Изд-во НГТУ, 2014. - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785778224094.html

3. Чеголин, А.П. Линейная алгебра
и аналитическая геометрия [Электронный ресурс]: учебное пособие / Чеголин А.П. - Ростов н/Д : Изд-во ЮФУ, 2015. - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785927517282.html

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. https://www.youtube.com/watch?v=iiVyfwkojYg Голубев М.О.. 1 курс. Семинар по аналитической геометрии и линейной алгебре
2. https://biblio-online.ru/book/CF0DDA58-4A87-4F81-9F20-B8804427CC00/kriptograficheskie-metody-zaschity-informacii-v-2-ch-chast-2-sistemnye-i-prikladnye-aspekty Криптографические методы защиты информации
3. https://www.lektorium.tv/mooc2/26288 Линейная алгебра и аналитическая геометрия

Перечень информационных технологий и программного обеспечения

Для работы в литературой из списка необходимо наличие к студента аккаунтов в указанных электронно-библиотечных системах: ЭБС «Консультант студента (http://www.studentlibrary.ru).

VI. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

На изучение дисциплины отводится 108 часа аудиторных занятий. На лекциях преподаватель объясняет теоретический материал. Вводит основные понятия, определения, свойства. Формулирует и доказывает теоремы. Приводит примеры. Необходимо поддерживать непрерывный контакт с аудиторией, отвечать на возникающие у студентов вопросы. На практических занятиях преподаватель разбирает примеры по пройденной теме. Во второй части занятия студентам предлагается работать самостоятельно, выполняя задания по теме. Преподаватель контролирует работу студентов, отвечает на возникающие вопросы, подсказывает ход и метод решения. Если знаний, полученных в аудитории, оказалось недостаточно, студент может самостоятельно повторно прочитать лекцию. После выполнения задания, студент отправляет его на проверку преподавателю. Работа должна быть отослана в формате PDF одним документом. По данному курсу разработаны методические указания.

VII МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 412 / D 542, 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 – 90) Оборудование: "Мультимедийное 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 «Геометрические аспекты криптологии»

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)	27	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.

Материалы для самостоятельной работы студентов подготовлены в виде индивидуальных домашних заданий по каждой теме (образцы типовых ИДЗ представлены в разделе «Материалы для самостоятельной работы студентов»). Работа должна быть отправлена преподавателю на проверку в системе Bb dvfu по соответствующему «Назначению». Оформление в формате PDF. Критерии оценки: студент получает максимальный балл, если работа выполнена без ошибок и оформлена в соответствии с требованиями преподавателя.

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 «Геометрические аспекты криптологии»
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**	
(ОПК-2) способностью 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	Знает	Понятия линейного, аффинного, евклидова пространств, базиса, системы координат, прямой, плоскости, угла, объема (длины, площади), алгебраической поверхности (кривой) второго порядка, преобразования.
	Умеет	Переходить от одной системы координат к другой в аффинном, и евклидовом пространствах, исследовать взаимное расположение прямых, плоскостей, кривых и поверхностей второго порядка в пространстве, решать метрические задачи с участием плоскостей (прямых) и алгебраических поверхностей (кривых) второго порядка, приводить алгебраические кривые и поверхности второго порядка к каноническому виду согласно аффинной и метрической классификациям.
	Владеет	Аппаратом векторной алгебры в трехмерном евклидовом пространстве, навыками работы в различных системах координат, аналитическими и алгебраическими методами классификации поверхностей (кривых) второго порядка, выполнения преобразований пространства.

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Раздел I. Определители и системы	(ОПК-2)	знает	ПР-7	1-3
			умеет	ПР-7	3-5
			владеет	ОУ-2	*5-7*
2	Раздел II. Координаты	(ОПК-2)	знает	ПР-7	8-10
			умеет	ПР-7	10-12
			владеет	ОУ-2	12-14
3	Раздел III. Введение в линейную алгебру	(ОПК-2)	знает	ПР-7	15
			умеет	ПР-7	16
			владеет	ОУ-2	*17*
4	Раздел IV. Линейная зависимость.	(ОПК-2)	знает	ПР-7	*25-29*
			умеет	ПР-7	*30-35*

	Базис		владеет	ОУ-2	*36-39*
5	Раздел V. Прямая на плоскости	(ОПК-2)	знает	ПР-7	*40-43*
			умеет	ПР-7	*44-48*
			владеет	ОУ-2	*49-52*
6	Раздел VI. Плоскость	(ОПК-2)	знает	ПР-7	*53-56*
			умеет	ПР-7	*56-60*
			владеет	ПР-6	*61-64*
7	Раздел VII. Прямая в пространстве	(ОПК-2)	знает	ПР-7	*65-67*
			умеет	ПР-7	*68,69*
			владеет	ПР-6	*70,71*

Оценочные средства для промежуточной аттестации

Список вопросов на экзамен

Определители и системы малых порядков

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

Координаты

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

Векторное пространство

15. Понятие векторного пространства

16. Следствие аксиом векторного пространства

17. Примеры векторных пространств: геом. векторы, нулевое, координатное

Пространство матриц

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

Линейная зависимость. Базис векторного пространства

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

Геометрия на плоскости

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

Кривые второго порядка (КВП)

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.

Плоскость

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

Прямая в пространстве

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

Поверхности второго порядка

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

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	Вопросы по темам/разделам дисциплины

			обучающимися.	
3	ПР-7	Конспект	Продукт самостоятельной работы обучающегося, отражающий основные идеи заслушанной лекции, сообщения и т.д.	Темы/разделы дисциплины