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

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

«СОГЛАСОВАНО»
Руководитель ОП

Доржинский Ю.В
(подпись) (Ф.И.О.)

«УТВЕРЖДАЮ»
И.о. заведующего кафедрой
информационной безопасности

Доржинский Ю.В
(подпись) (Ф.И.О.)

« 15 » июня 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Основы алгебры в криптологии
Специальность 10.05.01 Компьютерная безопасность
(Математические методы защиты информации)
Форма подготовки очная

курс 1,2 семестр 1,2,3
лекции 90 час.
практические занятия 90 час.
лабораторные работы 00 час.
в том числе с использованием МАО лек 00 /пр. 90 /лаб. 00 час.
в том числе в электронной форме лек 00 /пр. 00 /лаб. 00 час.
всего часов аудиторной нагрузки 180 час.
в том числе с использованием МАО 90 час.
в том числе в электронной форме 00 час.
самостоятельная работа 180 час.
в том числе на подготовку к экзамену 108 час.
курсовая работа / курсовой проект не предусмотрены
зачет не предусмотрен
экзамен 1,2,3 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: Доржинский Ю.В., к.т.н., с.н.с.
Составитель (ли): Закасовская Е.В. Д.ф.-м.н., профессор

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: *Fundamentals of algebra in cryptology*

Basic part of Block 1, 10 credits

Instructor: *Zakasovskaya E.V.*

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, 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 (GPC-3)

Learning outcomes:

the 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 (GPC-2).

Course description:

The study of algebra allows the future specialist to scientifically analyze the problems of his professional field (including those associated with the creation of new equipment and technologies) to successfully solve various scientific and technical problems in theoretical and applied aspects, independently — using modern educational and information technologies — to master that new information , with which he will have to face in the production and scientific activities. The study of the theoretical and algorithmic apparatus contributes to the development of future specialists' inclinations and abilities for creative thinking, the development of a systematic approach to the phenomena under study, the ability to independently build and analyze mathematical models of various systems.

Main course literature:

1. *Глухов, М.М. Алгебра [Электронный ресурс] : учебник / М.М. Глухов, В.П. Елизаров, А.А. Нечаев. — Электрон. дан. — Санкт-Петербург : Лань, 2015. — 608 с. — Режим доступа: https://e.lanbook.com/book/67458#book_name*

2. *Кадомцев, С.Б. Аналитическая геометрия и линейная алгебра [Электронный ресурс] : учебное пособие / С.Б. Кадомцев. — Электрон. дан. — Москва.: Физматлит, 2011. — 168 с. — Режим доступа: https://e.lanbook.com/book/2187#book_name*

3. *Шилин, И.А. Введение в алгебру. Группы [Электронный ресурс]: учебное пособие / И.А. Шилин. — Электрон. дан. — Санкт-Петербург: Лань, 2012. — 208 с. — Режим доступа: https://e.lanbook.com/book/4120#book_name*

Form of final knowledge control: *exam.*

Аннотация к рабочей программе дисциплины
«Основы алгебры в криптологии»

Рабочая программа учебной дисциплины «Основы алгебры в криптологии» разработана для студентов специальности 10.05.01 «Компьютерная безопасность», специализация «Математические методы защиты информации» и входит в состав дисциплин базовой части учебного плана Б1.Б.14.2.

Общая трудоемкость дисциплины составляет 10 зачетных единиц, 360 часов. Учебным планом предусмотрены лекционные занятия (90 часов), практические занятия (90 часов), самостоятельная работа студента (180 часов, в том числе 108 часов на подготовку к экзамену). Дисциплина реализуется на 1 и 2 курсе в 1, 2 и 3 семестре. Форма контроля по дисциплине в 1-3 семестрах – экзамен.

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

Изучение алгебры позволяет будущему специалисту научно анализировать проблемы его профессиональной области (в том числе связанные с созданием новой техники и технологий), успешно решать разнообразные научно-технические задачи в теоретических и прикладных аспектах, самостоятельно – используя современные образовательные и информационные технологии – овладевать той новой информацией, с которой ему придётся столкнуться в производственной и научной деятельности. Изучение теоретического и алгоритмического аппарата способствует развитию у будущих специалистов склонности и способности к творческому мышлению, выработке системного подхода к исследуемым явлениям, умения самостоятельно строить и анализировать математические модели различных систем.

Цель дисциплины – формирование и развитие личности студентов, их способностей к алгоритмическому и логическому мышлению, а также

обучение основным математическим понятиям и методам «Основ алгебры в криптологии». Изучение дисциплины способствует расширению научного кругозора и повышению общей культуры будущего специалиста, развитию его мышления и становлению его мировоззрения.

Задачи дисциплины:

- формирование устойчивых навыков по компетентностному применению фундаментальных положений алгебры при изучении дисциплин профессионального цикла и научном анализе ситуаций, с которыми выпускнику приходится сталкиваться в профессиональной и общекультурной деятельности;
- освоение студентами методов матричного исчисления, векторной алгебры, теории чисел; теории многочленов; теории групп; линейной алгебры; теории Галуа;
- обучение применению методов алгебры, терминологией, моделями и методами решения задач, применяемыми в практике инженерных и научно-технических расчетов.

Для успешного изучения дисциплины «Основы алгебры в криптологии» у обучающихся должны быть сформированы следующие предварительные компетенции:

- способностью 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 компетенция	**Этапы формирования компетенций**

(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	основные понятия и методы матричного исчисления; теорию определителе; методы решения различных систем уравнений; элементы векторной алгебры; основные методы аналитической геометрии на плоскости и в пространстве
	Умеет	применять методы линейной алгебры при решении инженерных задач
	Владеет	инструментом для решения математических задач в своей предметной области

Для формирования вышеуказанных компетенций в рамках дисциплины «Основы алгебры в криптологии» применяются следующие методы активного/ интерактивного обучения: интерактивные и проблемные лекции, работа в малых группах. Используемые оценочные средства: собеседование (ОУ-1), коллоквиум (ОУ-2), конспект (ПР-7).

I. СТРУКТУРА И СОДЕРЖАНИЕ ТЕОРЕТИЧЕСКОЙ ЧАСТИ КУРСА

Раздел I. Введение в алгебру (8 ч.)

Тема 1. Множества и отображения (2 ч.)

1.1. Предмет алгебры. Множества.

1.2. Композиция отображений. Теорема об ассоциативности композиции. Некоммутативность композиции отображений.

1.3. Обратные отображения. Теорема о существовании обратного отображения и ее следствия.

1.4. Теорема об инъективном преобразовании конечного множества.

Тема 2. Принцип математической индукции. (2 ч.)

2.1. Индукция полная и неполная.

2.2. Метод математической индукции.

Тема 3. Подстановки и перестановки. (4 ч.)

3.1. Перестановки. Транспозиция. Теорема о числе всех перестановок из n элементов.

3.2. Теорема о переходе от одной перестановке к другой с помощью транспозиций.

3.3. Инверсии. Четные и нечетные перестановки. Теорема о транспозиции в перестановке.

3.4. Теорема о перестановке элементов перестановки и ее следствия Теорема о числе четных и нечетных перестановок. Группа подстановок.

Раздел II. Системы линейных уравнений (10 ч.)

Тема 1. Теория определителей. (6 ч.)

1.1. Определители малых порядков. Определение определителя n-го порядка. Простейшие свойства определителей.

1.2. Методы вычисления определителей. Определитель Вандермонда.

1.3. Миноры и алгебраические дополнения. Теорема Крамера и ее следствия.

1.4. Определитель ступенчатой матрицы. Определение минора к-го порядка. Теорема Лапласа.

Тема 2. Общая теория решения линейных систем. (4 ч.)

2.1. Ранг матрицы. Теорема о ранге матрицы. Способы вычисления ранга матрицы: метод окаймления, метод элементарных преобразований Гаусса. Лемма о ранге эквивалентных систем.

2.2. Теорема Кронекера-Капелли. Теорема о числе решений произвольной совместной системы линейных алгебраических уравнений. Однородные системы.

Раздел III. Основные алгебраические структуры (6 ч.)

Тема 1. Группы. (4 ч.)

1.1. Понятие о бинарной алгебраической операции. Примеры групп: числовые, группы подстановок, классические линейные группы.

1.2. Подгруппы. Критерий подгруппы.

1.3. Гомоморфизмы и изоморфизмы. Теорема Кели.

1.4. Циклические группы. Разбиение на классы смежности и теорема Лагранжа и ее следствия.

Тема 2. Кольца. Поля. (2 ч.)

2.1. Понятие кольца, подкольца. Примеры колец.

2.2. Понятие поля, подполя. Примеры полей.

Раздел IV. Комплексные числа (12 ч.)

Тема 1. Действия над комплексными числами. (4 ч.)

1.1. Определение комплексных чисел. Свойства действий. Поле комплексных чисел.

1.2. Тригонометрическая форма комплексного числа.

1.3. Возведение комплексного числа в степень с целым показателем. Формула Муавра.

1.4. Извлечение корня из комплексного числа, теорема о количестве различных значений корня.

Тема 2. Первообразные корни из единицы (4 ч.)

2.1. Теорема о первообразных корнях из единицы и следствие.

2.2. Группа корней из единицы, порождение ее первообразным корнем.

Тема 3. Решение уравнений 3-й и 4-й степени (4 ч.)

3.1. Решение уравнений 3-й степени по формулам Кардано.

3.2. Решение уравнений 4-й степени методом Феррари.

Раздел V. Введение в теорию чисел (22 ч.)

Тема 1. Теория делимости. (4 ч.)

1.1. Понятие делимости. Делители. Множители и кратные. Собственные делители. Простые числа.

1.2. Основная теорема арифметики (о существовании и единственности разложения).

1.3. Теорема Евклида (о бесконечности множества всех простых чисел) Общий делитель. Взаимно простые числа.

1.4. Деление с остатком. Теорема о существовании и единственности деления с остатком.

1.5. Теорема о линейном представлении НОД.

1.6. Алгоритм Евклида.

Тема 2. Простейшие свойства делимости (4 ч.)

2.1. Делимость произведения и делимость сомножителей. Сокращение (умножение) на общий множитель.

2.2. Вынесение общего множителя (делителя) из НОД. Связь НОД с НОК.

3.3. Элементарные свойства делимости простых чисел. Теорема Дирихле.

Тема 3. Непрерывные дроби (4 ч.)

3.1. Разложение действительного числа в непрерывную дробь. Неполные частные и подходящие дроби. Схема вычислений, таблица.

3.2. Периодическая дробь. Период. Разложение квадратичной иррациональности в непрерывную дробь. Теорема об иррациональности периодической непрерывной дроби и ее обращение. Лемма о связи Pi и Qi.

3.3. Применение непрерывных дробей к решению в целых числах неопределенного уравнения первой степени с двумя неизвестными.

Тема 4. Арифметические функции (4 ч.)

4.1. Важнейшие функции в теории чисел. Показатель степени, с которым входит простое число в факториал. Мультипликативные функции и их свойства. Сумма всех делителей и число всех делителей данного числа.

4.2. Функция Мёбиуса, ее мультипликативность. Сумма произведений функции Мёбиуса на мультипликативную функцию по всем делителям: $\sum_{d|a} \mu(d)\theta(d)$.

4.3. Функция Эйлера. Теорема о вычислении функции Эйлера через каноническое разложение числа. Функция Эйлера от простого числа и степени простого числа.

Тема 5. Сравнения первой степени (6 ч.)

5.1. Определение сравнения по модулю, простейшие свойства. Сравнения и арифметические действия над ними. Умножение и сокращение сравнений на число.

5.2. Полная и приведенная система вычетов.

5.3. Малая теорема Ферма. Теорема Эйлера.

5.4. Решение сравнения первой степени $ax \equiv b \pmod m$ в случае, когда $(a,m) = 1$. Решение сравнения первой степени $ax \equiv b \pmod m$ в случае, когда $(a,m) \neq 1$. Вопросы существования и количества решений.

5.5. Практическое решение сравнений первой степени методом подходящих дробей. Практическое решение сравнений первой степени методом Эйлера.

Раздел VI. Многочлены и их корни (8 ч.)

Тема 1. Расширения колец, целостные кольца. (2 ч.)

1.1. Присоединение множества к телу. Простое расширение.

1.2. Делители нуля. Теорема о конечных целостных кольцах. Теорема о кольце классов вычетов по простому модулю.

Тема 2. Строение кольца многочленов. (2 ч.)

2.1. Алгебраические и трансцендентные элементы. Теорема о кольце многочленов над произвольным кольцом.

2.2. Теорема о кольце многочленов над целостным кольцом. Степень суммы и произведения.

Тема 3. Делимость в кольце многочленов (2 ч.)

3.1. Деление с остатком. Свойства делимости.

3.2. Алгоритм Евклида. Теорема о выражении НОД в виде линейной комбинации данных многочленов.

Тема 4. Корни многочленов, неприводимые многочлены (2 ч.)

4.1. Неприводимые многочлены. Свойства. Теорема об однозначном разложении.

4.2. Схема Горнера. Теорема о делении на линейный многочлен.

4.3. Теорема Безу. Кратные корни и производные. Основная теорема алгебры и ее следствия. Формулы Виета.

4.4. Целые корни многочлена с целыми коэффициентами. Рациональные корни многочлена с целыми коэффициентами.

Раздел VII. Теория групп (10 ч.)

Тема 1. Элементы теории групп. (2 ч.)

1.1. Определение группы. Левые, правые единицы и обратные. Группа подстановок n–й степени. Примеры групп. Классические линейные группы.

1.2. Подгруппы. Необходимое и достаточное условие подгруппы. Циклические подгруппы. Примеры подгрупп. Описание подгрупповой структуры группы S3.

1.3. Теорема Кэли. Конечные и бесконечные циклические группы Классические группы малых размерностей.

1.4. Теоремы о классах смежности. Теорема Лагранжа и ее следствия. Нормализатор и централизатор. Теорема о числе множеств, сопряженных данному. Нормальные подгруппы. Фактор-группа.

Тема 2. Гомоморфизмы и действия групп на множествах. (4 ч.)

2.1. Гомоморфизмы и изоморфизмы. Предложение о ядре гомоморфизма и полных прообразах.

2.2. Теоремы о гомоморфизмах. Центр и коммутант. Фактор-группа по коммутанту.

2.3. Действие групп на множествах. Отношение эквивалентности. Стационарные подгруппы. Длина орбиты. Сопряженность стационарных подгрупп. Примеры действия групп. Классы сопряженных элементов в симметрической группе. Центр конечной p-группы.

2.4. Ложность обращения теоремы Лагранжа. Теоремы Силова: существование, сопряженность, количество. (1 ч.)

Тема 3. Абелевы группы (4 ч.)

3.1. Внешнее прямое произведение. Внутреннее прямое произведение. Теорема о прямом произведении силовских подгрупп.

3.2. Конечно порожденная свободная группа. Теорема о существовании несократимых слов. Теорема о задании группы образующими и соотношениями. Конечно порожденная группа как гомоморфный образ свободной.

3.3. Конечные абелевы группы. Аннулятор элемента. Аннулятор группы. Теорема о строении конечной абелевой группы. Подгруппы циклической группы. Разложение примарной группы в прямую сумму циклических.

Раздел VIII. Линейная алгебра (10 ч.)

Тема 1. Общее решение СЛАУ. (6 ч.)

1.1. Теорема о множестве решений однородной системы. Фундаментальная система решений.

1.2. Теорема о задании произвольного подпространства с помощью однородной системы.

1.3. Теорема о представлении общего решения СЛАУ в виде суммы частного решения и общего решения соответствующей однородной системы.

1.4. Диагонализуемость матрицы линейного оператора в случае простых и кратных корней.

Тема 2. Евклидовы и унитарные пространства. (4 ч.)

2.1. Скалярное произведение. Неравенство Коши-Буняковсконго.

2.2. Ортогонализация совокупности векторов. Линейная независимость ортогональных векторов. Теорема об ортогонализации.

2.3. Классификация евклидовых и унитарных пространств. Следствия неравенства Коши-Буняковсконго. Определитель Грамма.

2.4. Ортогональное дополнение. Теорема об ортогональном разложении Евклидова или унитарного пространства. Геометрическая интерпретация однородной системы на языке ортогональных дополнений. Объем k-мерного параллелепипеда.

Раздел IX. Квадратичные формы (4 ч.)

Тема 1. Квадратичные формы. (4 ч.)

1.1. Определение квадратичной формы. Матрица квадратичной формы. Линейное преобразование переменных в квадратичной форме. Канонический вид. Теорема Лагранжа.

1.2. Вещественные квадратичные формы. Положительно определенные квадратичные формы. Критерий Сильвестра.

1.3. Закон инерции квадратичных форм. Теорема о приведении вещественной квадратичной формы к каноническому виду ортогональным преобразованием.

1.4. Приведение общего уравнения кривой второго порядка к главным осям.

II. СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКОЙ ЧАСТИ КУРСА

Практические занятия (90 час.)

Занятие 1. Метод математической индукции (2 час.)

1. Основные алгебраические структуры: группы, кольца, поля, векторные пространства.

Занятие 2. Перестановки. Транспозиция. Инверсии (2 час.)

1. Четные и нечетные перестановки
2. Действия над подстановками.
3. Группа подстановок.

Занятие 3. Определители малых порядков. (2 час.)

1. Определители малых порядков.
2. Частные случаи теоремы Крамера.

Занятие 4. Определители n-го порядка (10 час.)

1. Свойства определителей.
2. Практические методы решения числовых определителей.
3. Методы вычисления определителей n-го порядка: приведение к диагональной и треугольной форме
4. Метод рекуррентных соотношений для вычисления определителей.
5. Определитель Вандермонда. Вычисление определителей по теореме Лапласа.

Занятие 5. Контрольная работа: определители n-го порядка (2 час.)

Занятие 6. Решение систем линейных алгебраических уравнений (6 час.)

1. Метод Крамера.
2. Обращение матриц. Решение систем линейных алгебраических уравнений методом обращения.
3. Общая теория решения линейных систем.

Занятие 7. Комплексные числа и действия над ними (6 час.)

1. Действия над комплексными числами в алгебраической и тригонометрической форме.
2. Возведение комплексного числа в степень с целым показателем и извлечение корней.
3. Решение уравнений в поле комплексных чисел. Корни из единицы. Группа корней из единицы, порождение ее первообразным корнем.
4. Решение уравнений 3-й и 4-й степени методами Кардано и Феррари.

Занятие 8. Контрольная работа: решение уравнений над полем комплексных чисел (2 час.)

Занятие 9. Деление (8 час.)

1. Делители. Множители и кратные. Деление целое Собственные делители. Простые числа.
2. Основная теорема арифметики (о существовании и единственности разложения).
3. Деление с остатком. Теорема о существовании и единственности деления с остатком.
4. Теорема о линейном представлении НОД. Алгоритм Евклида.
5. Связь НОД с НОК. Элементарные свойства делимости простых чисел.

Занятие 10. Дроби (6 час.)

1. Разложение действительного числа в непрерывную дробь.
2. Неполные частные и подходящие дроби. Схема вычислений (таблица).
3. Периодическая дробь. Период.

4. Разложение квадратичной иррациональности в непрерывную дробь.

5. Применение непрерывных дробей к решению в целых числах неопределенного уравнения первой степени с двумя неизвестными.

Занятие 11. Показатель степени с которым входит простое число в факториал (2 час.)

1. Показатель степени с которым входит простое число в факториал.
2. Мультипликативные функции и их свойства.
3. Сумма всех делителей и число всех делителей данного числа.

Занятие 12. Функции (4 час.)

1. Функция Мёбиуса, ее мультипликативность. Сумма произведений функции Мёбиуса на мультипликативную функцию по всем делителям: $\sum_{d|a} \mu(d)\theta(d)$.

2. Функция Эйлера. Теорема о вычислении функции Эйлера через каноническое разложение числа. Функция Эйлера от простого числа и степени простого числа.

Занятие 13. Сравнения (12 час.)

1. Решение сравнений первой степени. Сравнения и арифметические действия над ними.

2. Умножение и сокращение сравнений на число. Полная и приведенная система вычетов.

3. Решение сравнения первой степени $ax \equiv b \pmod m$ в случае, когда $(a, m) = 1$.

4. Решение сравнения первой степени $ax \equiv b \pmod m$ в случае, когда $(a, m) \neq 1$. Вопросы существования и количества решений.

5. Практическое решение сравнений первой степени методом подходящих дробей. (2 час.)

6. Практическое решение сравнений первой степени методом Эйлера. (2 час.)

Занятие 14. Кольцо классов вычетов по простому и произвольному модулю (2 час.)

Занятие 15. Контрольная работа по теории чисел (2 час.)

Занятие 16. Многочлены (6 час.)

1. Неприводимые многочлены.
2. Корни многочленов.
3. НОД многочленов. Алгоритм Евклида.

Занятие 17. Контрольная работа по теме “Многочлены». (2 час.)

Занятие 18. Группы (8 час.)

1. Определение группы. Левые, правые единицы и обратные.
2. Числовые группы. Группы классов вычетов. Группы подстановок. Матричные группы.
3. Подгруппы. Циклические подгруппы. Описание подгрупповой структуры групп малых размерностей (2, 3, 4, 6).
4. Группы движений правильных геометрических фигур и тел.

Занятие 19. Порождающие множества (2 час.)

1. GL (n, K).
2. SL (n, K).
3. S_n
4. A_n

Занятие 20. Классы смежности. (4 час.)

1. Теорема Лагранжа и ее применение.
2. Нормальные подгруппы.
3. Фактор-группа.
4. Гомоморфизмы и изоморфизмы.

III. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое обеспечение самостоятельной работы обучающихся по дисциплине «Основы алгебры в криптологии» 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. Введение в алгебру	ОПК-2	знает	ПР-7	1-10
			умеет	ПР-2	1-10
			владеет	ПР-2	1-10
2	Раздел II. Системы линейных уравнений	ОПК-2	знает	ПР-7	10-22
			умеет	ПР-2	10-22
			владеет	ПР-2	10-22
3	Раздел III. Основные алгебраические структуры	ОПК-2	знает	ПР-7	23-28
			умеет	ПР-2	23-28
			владеет	ПР-2	23-28
4	Раздел IV. Комплексные числа	ОПК-2	знает	ПР-7	29-34
			умеет	ПР-2	29-34
			владеет	ПР-2	29-34
5	Раздел V. Введение в теорию чисел	ОПК-2	знает	ПР-7	1-42

			умеет	ПР-2	1-42
			владеет	ПР-2	1-42
6	Раздел VI. Многочлены и их корни	ОПК-2	знает	ПР-7	43-50
			умеет	ПР-2	43-50
			владеет	ПР-2	43-50
7	Раздел VII. Теория групп	ОПК-2	знает	ПР-7	1-7
			умеет	ПР-2	1-7
			владеет	ПР-2	1-7
8	Раздел VIII. Линейная алгебра	ОПК-2	знает	ПР-7	8-20
			умеет	ПР-2	8-20
			владеет	ПР-2	8-20
9	Раздел IX. Квадратичные формы	ОПК-2	знает	ПР-7	21-29
			умеет	ПР-2	21-29
			владеет	ПР-2	21-29

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. Глухов, М.М. Алгебра [Электронный ресурс] : учебник / М.М. Глухов, В.П. Елизаров, А.А. Нечаев. — Электрон. дан. — Санкт-Петербург : Лань, 2015. — 608 с. — Режим доступа: https://e.lanbook.com/book/67458#book_name
2. Кадомцев, С.Б. Аналитическая геометрия и линейная алгебра [Электронный ресурс] : учебное пособие / С.Б. Кадомцев. — Электрон. дан. — Москва.: Физматлит, 2011. — 168 с. — Режим доступа: https://e.lanbook.com/book/2187#book_name
3. Шилин, И.А. Введение в алгебру. Группы [Электронный ресурс]: учебное пособие / И.А. Шилин. — Электрон. дан. — Санкт-Петербург: Лань, 2012. — 208 с. — Режим доступа: https://e.lanbook.com/book/4120#book_name

Дополнительная литература

2. Рябко, Б.Я., Фионов, А.Н. Криптографические методы защиты информации [Электронный ресурс] : Учебное пособие для вузов / Б.Я. Рябко, А.Н. Фионов. - 2-е издание, стереотип. - М.: Горячая линия - Телеком, 2012. – 229 с. – Режим доступа: http://www.studentlibrary.ru/book/ISBN9785991202862.html
3. Курош, А.Г. Теория групп [Электронный ресурс] / А.Г. Курош. — Электрон. дан. — Москва: Физматлит, 2011. — 806 с. — Режим доступа: https://lib.dvfu.ru:8443/lib/item?id=chamo:662750&theme=FEFU
3. Курс высшей алгебры : учебник для вузов / А. Г. Курош. — Электрон. дан. — Изд. 16-е, стер. — Санкт-Петербург : Лань, : Физматкнига, 2007. — 431 с. — Режим доступа: https://lib.dvfu.ru:8443/lib/item?id=chamo:250620&theme=FEFU

VI. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Количество аудиторных часов, отведенных на изучение дисциплины «Основы алгебры в криптологии», составляет 180 академических часов. На самостоятельную работу выделено 180 часов, из них 108 часов на подготовку к экзамену. При этом аудиторная нагрузка состоит из 90 лекционных часов и 90 часов практических занятий.

Обучающийся получает теоретические знания на лекционных занятиях, необходимые для последующего выполнения практических заданий. В ходе подготовки к лекциям должны использоваться источники из списка учебной литературы.

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.

При подготовке к практическим занятиям также необходимо повторить теоретический материал.

Промежуточная форма аттестации по данной дисциплине – экзамен. Вопросы к экзамену соответствуют темам, изучаемым на лекционных занятиях. Таким образом, при самостоятельной подготовке к зачету студенту необходимо воспользоваться конспектами лекций, а также иными источниками из списка литературы для более глубокого понимания материала.

VII. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус L, ауд. L 608, 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 – 30) Оборудование: Доска аудиторная, переносной компьютер (ноутбук Lenovo) с сумкой – 1 шт.

Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус L, ауд. L 560. 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 – 60) Оборудование: Доска аудиторная, переносной компьютер (ноутбук Lenovo) с сумкой – 1 шт. экран проекционный SENSSCREEN ES-431150 150* настенно-потолочный моторизированный, покрытие Matte White, 4:3, размер рабочей поверхности 305*229 , проектор BenQ MW 526 E
Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус L, ауд. L 609, Учебная аудитория для проведения занятий лекционного, практического и семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Помещение укомплектовано специализированной учебной мебелью (посадочных мест – 28) Оборудование: Доска аудиторная, переносной компьютер (ноутбук Lenovo) с сумкой – 1 шт.
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,	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

групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. 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	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.
Приморский край, г. Владивосток, Фрунзенский р-н, Русский Остров, ул. Аякс п., д. 10, корпус D, ауд. D 654(752), 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. 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 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 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

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 «Основы алгебры в 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)	72	Отчет о выполнении практического задания
2	Сессия	Подготовка и сдача экзамена	108	Экзамен

Рекомендации по самостоятельной работе студентов

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

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

Методические указания к выполнению отчета по занятию

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

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

Приложение 2

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

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Основы алгебры в криптологии»
Направление подготовки 10.05.01 Компьютерная безопасность
специализация «Математические методы защиты информации»
Форма подготовки очная

Владивосток
2019

Паспорт ФОС

Код и формулировка компетенция	**Этапы формирования компетенций**	
(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	основные понятия и методы матричного исчисления; теорию определителе; методы решения различных систем уравнений; элементы векторной алгебры; основные методы аналитической геометрии на плоскости и в пространстве
	Умеет	применять методы линейной алгебры при решении инженерных задач
	Владеет	инструментом для решения математических задач в своей предметной области

№ п/п	Контролируемые разделы / темы дисциплины	Коды и этапы формирования компетенций		Оценочные средства	
				текущий контроль	промежуточная аттестация
1	Раздел I. Введение в алгебру	ОПК-2	знает	ПР-7	1-10
			умеет	ПР-2	1-10
			владеет	ПР-2	1-10
2	Раздел II. Системы линейных уравнений	ОПК-2	знает	ПР-7	10-22
			умеет	ПР-2	10-22
			владеет	ПР-2	10-22
3	Раздел III. Основные алгебраические	ОПК-2	знает	ПР-7	23-28

	структуры		умеет	ПР-2	23-28
			владеет	ПР-2	23-28
4	Раздел IV. Комплексные числа	ОПК-2	знает	ПР-7	29-34
			умеет	ПР-2	29-34
			владеет	ПР-2	29-34
5	Раздел V. Введение в теорию чисел	ОПК-2	знает	ПР-7	1-42
			умеет	ПР-2	1-42
			владеет	ПР-2	1-42
6	Раздел VI. Многочлены и их корни	ОПК-2	знает	ПР-7	43-50
			умеет	ПР-2	43-50
			владеет	ПР-2	43-50
7	Раздел VII. Теория групп	ОПК-2	знает	ПР-7	1-7
			умеет	ПР-2	1-7
			владеет	ПР-2	1-7
8	Раздел VIII. Линейная алгебра	ОПК-2	знает	ПР-7	8-20
			умеет	ПР-2	8-20
			владеет	ПР-2	8-20
9	Раздел IX. Квадратичные	ОПК-2	знает	ПР-7	21-29

	формы		умеет	ПР-2	21-29
			владеет	ПР-2	21-29

Оценочные средства для промежуточной аттестации
Список вопросов на экзамен

1 семестр

1. Множества. Упорядоченная пара. Декартово произведение. Отображения. Сюръективное, инъективное, биективное отображения. Единичное отображение, вложение, сужение.
2. Композиция отображений. Теорема об ассоциативности композиции.
3. Обратные отображения. Теорема о существовании обратного отображения и ее следствия.
4. Теорема об инъективности преобразования конечного множества.
5. Перестановки. Транспозиция. Теорема о числе всех перестановок из **n** элементов.
6. Теорема о переходе от одной перестановке к другой с помощью транспозиций.
7. Инверсии. Четные и нечетные перестановки. Теорема о транспозиции в перестановке.
8. Теорема о перестановке элементов перестановки и ее следствия.
9. Теорема о числе четных и нечетных перестановок.
10. Группа подстановок.
11. Определители малых порядков
12. Определение определителя n-го порядка
13. Свойства определителей
14. Миноры и алгебраические дополнения
15. Теорема Крамера и ее следствия
16. Теорема об определителе ступенчатой матрицы, ее следствие. Теорема Лапласа
17. Определение векторного пространства и алгебры над полем. Примеры
18. Действия сложения и умножения на число над матрицами
19. Ассоциативность умножения матриц. Дистрибутивность умножения матриц
20. Транспонирование суммы и произведения матриц. Обзор действий над матрицами
21. Определитель произведения матриц
22. Обращение матриц
23. Понятие о бинарной алгебраической операции. Группа. Примеры. Подгруппы

24. Кольца и поля
25. Кольца и их подкольца. Расширения колец, тел, полей. Присоединение множества к телу. Простые расширения
26. Делители нуля. Примеры. Целостные кольца
27. Теорема о конечном целостном кольце
28. Теорема о кольце классов вычетов по простому модулю
29. Определение комплексных чисел. Свойства действий. Поле комплексных чисел
30. Тригонометрическая форма комплексного числа
31. Возведение комплексного числа в степень с целым показателем. Формула Муавра
32. Теорема о первообразных корнях из единицы и следствие
33. Группа корней из единицы, порождение ее первообразным корнем.
34. Решение уравнений 3-й и 4-й степени методами Кардано и Феррари

2 семестр

1. Понятие делимости. Делители. Множители и кратные. Деление целое
2. Деление с остатком. Теорема о существовании и единственности деления с остатком
3. Общий делитель. Взаимно простые числа. Теорема о представлении НОД
4. Алгоритм Евклида
5. Собственные делители. Простые числа. Основная теорема арифметики
6. Основная теорема арифметики (о существовании и единственности разложения)
7. Теорема Евклида (о бесконечности множества всех простых чисел)
8. Делимость произведения и делимость сомножителей
9. Сокращение (умножение) на общий множитель
10. Вынесение общего множителя (делителя) из НОД
11. Связь НОД с НОК
12. Элементарные свойства делимости простых чисел
13. Теорема Дирихле
14. Разложение действительного числа в непрерывную дробь
15. Неполные частные и подходящие дроби. Схема вычислений (таблица)
16. Периодическая дробь. Период. Разложение квадратичной иррациональности в непрерывную дробь
17. Теорема о иррациональности периодической непрерывной дроби и ее обращение
18. Лемма о связи P_i и Q_i .
19. Применение непрерывных дробей к решению в целых числах неопределенного уравнения первой степени с двумя неизвестными

20. Важнейшие функции в теории чисел
21. Показатель степени с которым входит простое число в факториал
22. Мультипликативные функции и их свойства
23. Сумма всех делителей и число всех делителей данного числа
24. Функция Мёбиуса, ее мультипликативность
25. Сумма произведений функции Мёбиуса на мультипликативную функцию по всем делителям: $\sum_{d|a} \mu(d)\theta(d)$
26. Важные частные случаи: 1) сумма значений функции Мёбиуса по всем делителям $\sum_{d|a} \mu(d)$, 2) $\sum_{d|a} \frac{\mu(d)}{d}$
27. Выражение S' через S_d с помощью функции Мебиуса (техническая лемма)
28. Функция Эйлера. Теорема о вычислении функции Эйлера через каноническое разложение числа.
29. Функция Эйлера от простого числа и степени простого числа
30. Сумма значений функции Эйлера по всем делителям $\sum_{d|a} \varphi(d)$
31. Определение сравнения по модулю, простейшие свойства
32. Сравнения и арифметические действия над ними
33. Умножение и сокращение сравнений на число
34. Полная и приведенная система вычетов
35. Малая теорема Ферма
36. Теорема Эйлера
37. Сравнение первой степени $ax \equiv b \pmod m$ в случае, когда $(a,m) = 1$
38. Сравнение первой степени $ax \equiv b \pmod m$ в случае, когда $(a,m) \neq 1$. Вопросы существования и количества
39. Практическое решение сравнений первой степени методом подходящих дробей
40. Практическое решение сравнений первой степени методом Эйлера
41. Сравнения высших степеней. Теоремы 1,2 о количестве решений
42. Теорема Вильсона
43. Алгебраические и трансцендентные элементы.
44. Теорема о кольце многочленов над произвольным кольцом. Теорема о кольце многочленов над целостным кольцом. Степень суммы и произведения
45. Делимость в кольце многочленов. Деление с остатком. Свойства делимости, Алгоритм Евклида. Теорема о выражении НОД в виде линейной комбинации данных многочленов
46. Неприводимые многочлены. Свойства. Теорема об однозначном разложении
47. Схема Горнера. Теорема о делении на линейный многочлен. Теорема Безу
48. Кратные корни и производные. Основная теорема алгебры и ее следствия. Формулы Виета

49. Целые корни многочлена с целыми коэффициентами
50. Рациональные корни многочлена с целыми коэффициентами

3 семестр

1. Определение группы. Левые, правые единицы и обратные
2. Группа подстановок **n**–й степени
3. Примеры групп. Классические линейные группы
4. Подгруппы. Необходимое и достаточное условие подгруппы. Примеры подгрупп
5. Описание подгрупповой структуры групп $\mathbf{S_3}$ и $\mathbf{S_4}$
6. Теорема Кэли. Циклические подгруппы
7. Порождающие множества $\mathbf{GL(n , K), SL(n , K), S_n, A_n}$
8. Теоремы о классах смежности. Теорема Лагранжа и ее следствия
9. Нормализатор и централизатор. Теорема о числе множеств, сопряженных данному
10. Нормальные подгруппы. Фактор-группа
11. Гомоморфизмы и изоморфизмы. Предложение о ядре гомоморфизма и полных прообразах. Теоремы о гомоморфизмах
12. Эндоморфизмы и автоморфизмы. Внутренние автоморфизмы
13. Центр и коммутант. Фактор-группа по коммутанту
14. Действие групп на множествах. Отношение эквивалентности. Стационарные подгруппы. Длина орбиты. Сопряженность стационарных подгрупп
15. Примеры действия групп
16. Классы сопряженных элементов в симметрической группе
17. Центр конечной p-группы
18. Ложность обращения теоремы Лагранжа. Теоремы Силова
19. Внешнее прямое произведение. Разложение группы в прямое произведение
20. Конечные абелевы группы
21. Определение квадратичной формы. Матрица квадратичной формы
22. Линейное преобразование переменных в квадратичной форме
23. Канонический вид. Теорема Лагранжа
24. Вещественные квадратичные формы
25. Положительно определенные квадратичные формы
26. Критерий Сильвестра
27. Закон инерции квадратичных форм
28. Приведение квадратичной формы к каноническому ортогональному преобразованию.
29. Приведение общего уравнения кривой или поверхности второго порядка к главным осям

Критерии выставления оценки на экзамене

Оценка	Требования к сформированным компетенциям
«отлично»	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач по методологии научных исследований.
«хорошо»	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.
«удовлетворительно»	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ
«неудовлетворительно»	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Как правило, оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение без дополнительных занятий по

	соответствующей дисциплине.

Оценочные средства для текущей аттестации

№ п/п	Код ОС	Наименование оценочного средства	Кроткая характеристика оценочного средства	Представление оценочного средства в фонде
1	ОУ-1	Собеседование	Средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определённому разделу, теме, проблеме и т.п.	Вопросы по темам/разделам дисциплины
2	ОУ-2	Коллоквиум	Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования преподавателя с обучающимися.	Вопросы по темам/разделам дисциплины
4	ПР-7	Конспект	Продукт самостоятельной работы обучающегося, отражающий основные идеи заслушанной лекции, сообщения и т.д.	Темы/разделы дисциплины