Министерство науки и высшего образования Российской Федерации

ФГБОУ ВО «Тверской государственный университет»

Утверждаю:

Руководитель ООП:

_____ Н.А. Семыкина

«_9_» _06_ 2023 г.

Рабочая программа дисциплины (с аннотацией)

АЛГЕБРА

Специальность

10.05.01 Компьютерная безопасность

Специализация

Математические методы защиты информации

Для студентов 1,2 курсов

Форма обучения

Очная

Составитель: к.ф.м.н., доцент К.Г. Некрасов

Тверь 2023

I. Аннотация

1. Наименование дисциплины (или модуля) в соответствии с учебным планом

Алгебра.

2. Цель и задачи дисциплины (или модуля)

Целями освоения дисциплины являются освоение основ фундаментальных знаний, позволяющих разобраться в математической основе, обеспечивающей возможность деятельности специалиста в той части, которая связана с алгеброй, решать стандартные задачи, давать интерпретацию полученным результатам.

3. Место дисциплины (или модуля) в структуре ООП

Дисциплина входит в базовую часть структуры ООП, формирующая общепрофессиональную компетенцию и изучается на 1-2 курсах.

Предварительные знания, необходимые для освоения дисциплины, — это знания, полученные при изучении школьной программы по алгебре и началам анализа, а также по геометрии.

Освоение данной дисциплины необходимо как предшествующее для следующих дисциплин: дифференциальные и разностные уравнения, численные методы, функциональный анализ, программирование, теория кодирования, криптография.

4. Объем дисциплины (или модуля):

16 зачетных единиц, 576 академических часов, **в том числе**

контактная работа: лекции 144 часа, практические занятия 144 часа, **самостоятельная работа: 126** часов, **контроль** 162 часа.

5. Перечень планируемых результатов обучения по дисциплине (или модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Планируемые результаты освоения	**Планируемые результаты обучения по дисциплине (или модулю)**

образовательной программы (формируемые компетенции)	
Базовый **ОПК-2** – способностью корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теория информации, теоретико-числовых методов	**Владеть:** навыками применения методов решения задач **Уметь:** формулировать понятия, используемые в рамках дисциплины, пользоваться знаниями для решения задач. **Знать:** понятия, изучаемые в рамках дисциплины, используемые обозначения, формулировки теорем, методы и подходы для решения задач.
Продвинутый	**Владеть:** навыками исследования и решения задач. **Уметь:** доказывать основные и вспомогательные теоремы, использовать алгебраические методы и теоремы при решении прикладных задач. **Знать:** основные методы и теоремы алгебры, требуемые для решения задач прикладной математики и информатики.

6. Форма промежуточной аттестации экзамен.

7. Язык преподавания русский**.**

II. Содержание дисциплины (или модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

Для студентов очной формы обучения

Учебная программа – наименование разделов и тем	Всего	Контактная работа (час.)		Самостоятельная работа и контроль (час.)
		Лекции	Практические (лабораторные) занятия	
1.1. Системы линейных уравнений. Метод Гаусса	16	4	4	13
1.2. Теория определителей	32	8	8	19
1.3. Арифметические пространства. Общая теория систем линейных уравнений.	48	10	10	25
1.4. Основные понятия в алгебре. Поле комплексных чисел.	48	10	10	25
2.1. Алгебра матриц	26	7	7	16
2.2. Кольцо многочленов от одной буквы	30	8	8	17
2.3. Линейные пространства	27	7	7	16
2.4. Линейные отображения	31	8	8	18
2.5. Евклидовы пространства	30	8	8	17
3.1. Квадратичные формы	32	8	8	18
3.2. Жорданова форма матриц	38	10	10	20
3.3. Основы теории групп	74	18	18	34
4.1. Основы теории колец. Расширения полей	38	14	14	18
4.2. Конечные поля	36	12	12	16
4.3. Теория чисел	34	12	12	16
Итого	576	144	144	288

III. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (или модулю)

Методические рекомендации по организации самостоятельной работы студентов

Раздел 1. Системы линейных уравнений. Метод Гаусса.

Введение. Цели и задачи курса. Общие сведения о науках, лежащих в основе курса.

- Системы линейных уравнений. Решение системы линейных уравнений; общее решение систем линейных уравнений.
- Эквивалентные системы линейных уравнений. Эквивалентные преобразования систем линейных уравнений.

Формулировка метода Гаусса. Теорема о методе Гаусса. Примеры.

Раздел 2. Теория определителей.

- Перестановки на n элементах. Количество различных перестановок порядка n. Транспозиция, инверсии. Связь между чётностью перестановок, полученных одна из другой транспозицией. Примеры.
- Подстановки n-го порядка, их количество, чётность. Связь между чётностями подстановки и перестановки. Примеры.

- Определение определителя n-го порядка, свойства определителя (транспонирование, перестановка двух строк, умножение строки на число, сумма двух определителей, определитель матрицы с нулевой строкой, определитель матрицы, в которой строка равна сумме двух строк, умноженных на коэффициенты). Примеры.
- Минор и алгебраическое дополнение. Теорема о разложении определителя по строке (столбцу). Теорема: сумма произведений элементов строки на алгебраические дополнения к элементам другой строки равна 0. Примеры.
- Связь определителей матриц с системами линейных уравнений: Теорема Крамера. Примеры.

Раздел 3. Арифметические пространства. Общая теория систем линейных уравнений.

- Определение арифметического линейного пространства. Линейная зависимость и линейная независимость системы векторов. Связь между линейной зависимостью и независимостью системы векторов и её подсистемы.
- Понятие подпространства арифметического пространства. Линейная оболочка и подпространство. Теорема о линейной (не)зависимости линейной комбинации.
- Понятие базиса и ранга. Корректность понятия ранга. Единственность разложения по базису. Теорема: любую линейно независимую систему векторов можно дополнить до базиса.
- Эквивалентные системы векторов. Ранг эквивалентных систем. Элементарные преобразования системы векторов.
- Определение ранга матрицы и минора k-го порядка. Теорема о ранге матрицы. Следствия из теоремы о ранге. Критерий равенства определителя нулю.
- Теорема о размерности подпространства решений системы однородных линейных уравнений.
- Теорема Кронекера–Капелли.
- Запись общего решения системы линейных уравнений.
- Определение фундаментальной системы решений системы линейных однородных уравнений. Теорема о количестве векторов в ФСР.

Раздел 4. Основные понятия в алгебре. Поле комплексных чисел.

- Понятие алгебраической операции. Примеры и контрпримеры. Понятие группы.
- Понятие кольца. Кольца с делителями нуля и без таковых. Понятие поля. Примеры и контрпримеры. Построение поля комплексных чисел (в виде множества пар чисел с комплексным сложением и умножением). Алгебраическая форма комплексного числа. Роль поля комплексных чисел в математике (понимание поля комплексных чисел как расширения поля действительных чисел; основная теорема алгебры (формулировка)).
- Другие формы представления комплексных чисел, связь этих представлений. Формула Муавра. Модуль комплексного числа. Свойство модуля.
  Корни n-ой степени из комплексного числа.

Раздел 5. Алгебра матриц

- Понятие кольца. Примеры.
- Кольцо матриц.
- Элементарные матрицы и элементарные преобразования.
- Обратная матрица. Существование обратной матрицы для элементарной матрицы.
- Определитель произведения матрицы и элементарной матрицы. Определитель произведения двух матриц.

- Критерий существования обратной матрицы.
- Нахождение обратной матрицы (два способа: через алгебраические дополнения и путём приписывания единичной матрицы).
- Связь систем линейных уравнений и матричных уравнений.

Раздел 6. Кольцо многочленов от одной буквы.

- Построение кольца многочленов от одной буквы над кольцом. Степень произведения многочленов.
- Многочлен как функция. Определение корня многочлена. Теорема Безу и следствие из неё. Схема Горнера. Случаи совпадения и несовпадения двух определений многочлена.
- Теорема о делении с остатком в кольце многочленов над полем. Определение делимости многочлена на многочлен.
- Определение наибольшего общего делителя. Алгоритм Евклида. Свойства взаимнопростых многочленов. Приводимые и неприводимые многочлены над данным полем. Существование и единственность разложения многочлена в произведение неприводимых.
- Основная теорема алгебры (без доказательства). Разложение многочлена в произведение неприводимых над полем комплексных чисел и над полем действительных чисел.
- Формальная производная. Показатель кратности неприводимого множителя. Отделение кратных множителей.
- Процедура отыскания рациональных корней многочлена.

Раздел 7. Линейные пространства.

- Линейные пространства. Примеры. Линейная зависимость и линейная независимость. Понятие базиса. Примеры.
- Размерность пространства. Единственность разложения по базису. Замена базиса. Матрица перехода. Утверждение: $T_{a\to e} \times T_{e\to a} = E$. Следствия. Изменение координат вектора при переходе к другому базису.
- Подпространства. Сумма и пересечение подпространств. Критерий того, что L_1 является подпространством L.
- Линейная оболочка. Утверждение: всякая линейная оболочка является подпространством и всякое подпространство является линейной оболочкой.
- Замкнутость множества подпространств данного пространства относительно суммы и пересечения. Связь между размерностями подпространств и размерностями их суммы и пересечения. Прямая сумма подпространств. Связь между размерностями подпространств и размерностью их прямой суммы.
- Изоморфизм линейных подпространств. Свойства изоморфизма линейных подпространств. Изоморфность подпространств. Утверждение: отношение изоморфности подпространств является эквивалентности.
- Теорема об изоморфности линейных пространств одинаковой размерности.

Раздел 8. Линейные отображения.

- Понятие линейного отображения. Ядро и образ линейного отображения. Утверждение: ядро и образ являются линейными подпространствами. Ранг и дефект линейного отображения. Связь ранга и дефекта линейного отображения с размерностью конечномерного пространства-прообраза.
- Матрица линейного преобразования в базисе. Изменение координат вектора при действии на него линейного отображения. Изменение матрицы отображения при переходе к другому базису.

- Отношение подобия матриц. Утверждение: отношение подобия матриц является эквивалентностью.
- Собственные числа и собственные векторы линейного отображения. Характеристический многочлен. Равенство характеристических многочленов подобных матриц.
- Теорема: число является собственным числом линейного преобразования тогда и только тогда, когда оно является корнем характеристического многочлена этого преобразования.
- Критерий подобия матрицы линейного преобразования диагональной матрице. Следствие.

Раздел 9. Евклидовы пространства.

- Евклидовы пространства и подпространства. Их связь с геометрией. Унитарные пространства.
- Неравенство Коши. Следствие. Длина вектора. Теорема косинусов. Следствия.
- Ортогональность векторов. Процесс ортогонализации.
- Ортонормированный базис. Существование ортонормированного базиса евклидова пространства.
- Скалярное произведение в ортонормированном базисе.
- Изоморфизм евклидовых пространств. Теорема об изоморфности евклидовых пространств одинаковой размерности.
- Подпространства евклидова пространства. Ортогональное дополнение, свойства ортогонального дополнения.
- Группа ортогональных матриц. Ортогональные матрицы как матрицы перехода.
- Симметрические преобразования. Симметрические матрицы. Связь между симметрическими преобразованиями и симметрическими матрицами.
- Характеристические корни симметрического преобразования. Существование ортонормированного базиса, состоящего из собственных векторов симметрического преобразования.
- Ортогональные преобразования. Канонический вид матрицы ортогонального преобразования.

Третий семестр (4 зачетные единицы)

Раздел 10. Квадратичные формы.

- Понятие квадратичной формы. Линейная замена букв квадратичной формы. Изменение матрицы формы при замене букв. Следствие.
- Метод Лагранжа приведения квадратичной формы к каноническому виду.
- Нормальный вид квадратичной формы. Приводимость действительной квадратичной формы к нормальному виду.
- Приведение квадратичной формы к главным осям.
- Закон инерции квадратичных форм.
- Положительно определённые квадратичные формы. Утверждение: действительная квадратичная форма является положительно определённой тогда и только тогда, когда на ненулевых наборах она принимает положительные значения.
- Критерий Сильвестра положительной определённости квадратичной формы.
- Связь квадратичных форм и скалярного произведения.
- симметрического преобразования.

Раздел 11. Жорданова форма матриц над полем С.

- Корневые векторы и корневые подпространства.

- Разложение пространства в прямую сумму корневых подпространств.
- Жорданова форма матрицы линейного преобразования, имеющего единственное собственное значение.
- Единственность жордановой формы матрицы преобразования.

Раздел 12. Основы теории групп.

- Полугруппы. Свойства степеней. Понятие группы. Простейшие свойства. Критерий группы.
- Подгруппы. Подгруппа четных подстановок.
- Изоморфизм групп. Примеры. Теорема Кэли.
- Смежные классы. Разложение группы по подгруппе. Теорема Лагранжа о делимости порядка группы на порядок подгруппы. Порядок элемента. Циклические группы. Подгруппы циклических групп. Строение групп простого порядка.
- Нормальные подгруппы. Примеры нормальных подгрупп. Контрпримеры. Нормальность подгрупп индекса 2. Понятие факторгруппы и его корректность. Примеры построения факторгрупп.
- Понятие гомоморфизма групп. Теорема о гомоморфизме групп. Восстановление подгруппы в прообразе из подгруппы в образе.
- Отношение сопряженности в группе. Свойства сопряженных элементов группы.Централизатор элемента. Теорема об индексе централизатора элемента конечной группы. Центр группы. Нетривиальность центра p-группы.
- Существование в коммутативной группе порядка делящегося на простое p элемента порядка p. Формулировка теоремы Силова. Доказательство теоремы Силова в части «существование».
- Прямые произведения групп. Критерий разложения группы в прямое произведение своих подгрупп. Теорема о строении конечных коммутативных групп.

Раздел 13. Основы теории колец. Расширения полей.

1. Понятие кольца. Подкольца. Кольцо классов вычетов по данному модулю. Понятие идеала. Сумма и пересечение идеалов. Примеры. Кольцо классов вычетов по данному модулю. Главные идеалы. Кольцо целых чисел как кольцо главных идеалов. Кольцо многочленов над полем как кольцо главных идеалов. Пример кольца, которое не является кольцом главных идеалов.

- Факторкольцо. Кольцо классов вычетов как пример факторкольца. Поле классов вычетов по простому модулю.Теорема существования корня. Поле разложения многочлена. Поле комплексных чисел как факторкольцо.
- Понятие поля. Пример поля, которое содержит иррациональные числа, содержится в поле действительных чисел, но не совпадает с ним.
- Построение поля частных.

Раздел 14. Конечные поля.

- Характеристика поля. Простые конечные поля. Число элементов в конечном поле. Изоморфизм минимальных полей, в которых данный неприводимый многочлен имеет корень. Наименьшая степень расширения поля, в котором неприводимый многочлен имеет корень.
- Существование конечного поля каждого порядка, являющегося степенью простого числа. Изоморфизм полей данного порядка. Цикличность мультипликативной группы конечного поля. Подполя конечного поля.
- Существование многочлена произвольной степени над конечным полем, который неприводим над этим полем. Конечное поле как множество корней некоторого многочлена.
- Некоторые критерии неприводимости данного многочлена над конечным полем и их применение.

Раздел 15. Теория чисел.

- Делимость целых чисел. Деление с остатком. Алгоритм Евклида. Разложение НОД. Критерий взаимной простоты. Простые числа. Существование и единственность разложения на простые множители.
- Классы вычетов по данному модулю. Решение сравнений первой степени.
- Решение сравнений второй степени. Квадратичные вычеты. Закон взаимности квадратичных вычетов.
- Функция Эйлера, её вычисление и применение.
- Функция Мёбиуса. Формула обращения Мёбиуса.
- Первообразные корни и индексы. Дискретный логарифм.
- **IV. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (или модулю)**

Типовые контрольные задания для проверки уровня сформированности компетенции ПК-2. Способностью участвовать в теоретических т экспериментальных научно-исследовательских работах по оценке защищенности информации в компьютерных системах, составлять научные отчеты, обзоры по результатам выполнения исследований.

Этап формирования компетенции, в котором участвует дисциплина	**Типовые контрольные задания для оценки знаний, умений, навыков (2-3 примера)**	**Показатели и критерии оценивания компетенции, шкала оценивания**
Базовый **владеть**	1. Используя алгоритм Евклида, определить наибольший общий делитель. 2. Сформулируйте и докажите теорему Крамера.	Имеется полное верное решение, включающее правильный ответ – 1 балла Решение не дано или дано неверное решение – 0 баллов
Базовый уметь	1) Найти матрицу X=$\begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix}$. При условии $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} = \begin{pmatrix} 3 & 5 \\ 5 & 9 \end{pmatrix}$. 2) Найти определитель матрицы $\begin{pmatrix} 2 & -1 & -1 \\ 3 & 4 & -2 \\ 3 & -2 & 4 \end{pmatrix}$ 3) Перемножить матрицы $\begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$	Имеется полное верное решение, включающее правильный ответ – 1 балла Решение не дано или дано неверное решение – 0 баллов
Базовый знать	1. Сформулировать теорему о ранге матрицы.	Имеется полное верное решение,

	2. Дать обеление определителя матрицы, и перечислить его свойства.	включающее правильный ответ – 1 балла Решение не дано или дано неверное решение – 0 баллов

V. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (или модуля)

а) Основная литература:

1. Огнева Э. Н. Математика: Раздел 1. Алгебра и геометрия : учебное пособие / Э. Н. Огнева/ - Кемерово : Кемеровский государственный университет культуры и искусств (КемГУКИ), 2011. - 227 с. : табл., схем. - Режим доступа : https://biblioclub.ru/index.php?page=book&id=227759
2. Бортаковский А. С. Линейная алгебра и аналитическая геометрия. Практикум : учебное пособие / А. С. Бортаковский, А. В. Пантелеев; Московский авиационный институт (национальный исследовательский университет). - 1. - Москва : ООО "Научно-издательский центр ИНФРА-М", 2023. - 352 с. - (Высшее образование: Бакалавриат). - ВО - Бакалавриат. – Режим доступа: https://znanium.com/catalog/document?id=432197
3. Шевцов Г. С. Линейная алгебра: теория и прикладные аспекты : учебное пособие / Г. С. Шевцов; Пермский государственный национальный исследовательский университет. - Москва : Издательство "Магистр", 2023. - 544 с. - ВО - Бакалавриат. – Режим доступа : https://znanium.com/catalog/document?id=432182

б) Дополнительная литература

4. Курош А. Г. Курс высшей алгебры [Электронный ресурс] : учебник для вузов / А. Г. Курош. - 24-е изд., стер. - Санкт-Петербург : Лань, 2023. - 432 с. – Режим доступа: https://e.lanbook.com/book/322661

5. Бухштаб А. А. Теория чисел [Электронный ресурс] / А. А. Бухштаб. - 6-е изд., стер. - Санкт-Петербург : Лань, 2022. - 384 с. – Режим доступа : https://e.lanbook.com/book/189329

VI. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (или модуля)

1. ЭБС Лань https://e.lanbook.com/ Договор № 4-е/23 от 02.08.2023 г.
2. ЭБС Znanium.com https://znanium.com/ Договор № 1106 эбс от 02.08.2023 г.
3. ЭБС Университетская библиотека online https://biblioclub.ru Договор № 02-06/2023 от 02.08.2023 г.
4. ЭБС ЮРАЙТ https://urait.ru/ Договор № 5-е/23 от 02.08.2023 г.
5. ЭБС IPR SMART https://www.iprbookshop.ru/ Договор № 3-е/23К от 02.08.2023 г.

6. https://cyberleninka.ru/ научная электронная библиотека «Киберленинка».
7. Научная электронная библиотека eLIBRARY.RU (подписка на журналы) https://elibrary.ru/projects/subscription/rus_titles_open.asp? ;
8. Репозитарий ТвГУ http://eprints.tversu.ru

VII. Методические указания для обучающихся по освоению дисциплины

Требования к рейтинг-контролю.

Модуль 1.

Максимальная сумма баллов по модулю – 50, из них 30 баллов отводится на текущий контроль учебной работы студента, 20 баллов на рубежный контроль по модулю. Текущая работа студента складывается из ответов в аудитории (min – 0 баллов, max - 3 балла). Рубежный контроль проводится в форме контрольной работы.

Модуль 2.

Максимальная сумма баллов по модулю – 50, из них 30 баллов отводится на текущий контроль учебной работы студента, 20 баллов на рубежный контроль по модулю. Текущая работа студента складывается из ответов в аудитории (min – 0 баллов, max – 3 балла). Рубежный контроль проводится в форме контрольной работы.

Экзаменационные вопросы

Первый семестр.

1. Метод Гаусса: доказательство теоремы о возможности приведения системы к трапецоидальному виду. Общее и частное решение.
2. Свойства перестановок. Свойства подстановок.
3. Понятие определителя, его свойства.
4. Миноры и алгебраические дополнения. Разложение определителя.
5. Теорема Крамера.
6. Определитель Вандермонда.
7. Понятие арифметического пространства, определения линейно зависимой и независимой системы векторов. Критерий линейной зависимости.
8. Теорема о линейной зависимости линейных комбинаций и следствия из нее.
9. Базис и ранг системы векторов.

10. Эквивалентные системы векторов: их свойства, доказательство равенства рангов эквивалентных систем.
11. Теорема о ранге матрицы.
12. Равенство рангов системы строк и столбцов матрицы. Неизменность ранга при элементарных преобразованиях матрицы. Перечисление базисов системы векторов.
13. Критерий того, что определитель квадратной матрицы равен 0.
14. Система линейных однородных уравнений. Ранг и базис множества решений.
15. Системы неоднородных линейных уравнений: теорема Кронекера-Капелли; связь с соответствующей системой линейных однородных уравнений.
16. Понятие алгебраической операции. Примеры и контр-примеры. Понятие полугруппы. Единственность единицы. Единственность обратного элемента в полугруппах.
17. Группы. Группа подстановок. Примеры подгрупп.
18. Понятие кольца. Понятие поля. Делители нуля в кольце и их отсутствие в поле. Примеры.
19. Построение поля комплексных чисел.
20. Тригонометрическая форма комплексного числа. Действия с комплексными числами в этой форме. Формула Муавра. Свойства модуля комплексного числа.
21. Извлечение корня n-ой степени из комплексного числа в тригонометрической форме. Расположение корней на плоскости.
22. Группа корней из единицы. Понятие первообразного корня, примеры.

Второй семестр.

1. Действия с матрицами. Кольцо квадратных матриц над кольцом.
2. Элементарные матрицы. Связь элементарных преобразований с элементарными матрицами.
3. Ранг произведения матриц.
4. Определитель произведения матриц.
5. Критерий обратимости квадратной матрицы над полем. Построение обратной матрицы способом, связанным с алгебраическими дополнениями.
6. Критерий обратимости квадратной матрицы над полем. Способ построения обратной матрицы, связанный с приписыванием единичной матрицы.
7. Построение кольца многочленов от одной буквы над кольцом.
8. Теорема о делении с остатком для кольца многочленов над полем.
9. Многочлен как функция. Схема Горнера. Теорема Безу. Теорема о числе корней. Достаточные условия совпадения двух определений многочлена.

10. Наибольший общий делитель двух многочленов. Алгоритм Евклида. Ассоциированность наибольших общих делителей.
11. Разложение НОД. Критерий взаимной простоты. Свойства взаимно простых многочленов.
12. Понятие приводимого многочлена над полем. Взаимная простота неприводимых неассоциированных многочленов. Теорема о разложении многочлена над полем в произведение многочленов, неприводимых над этим полем.
13. Кратность неприводимого множителя в каноническом разложении многочлена; ее связь с кратностью этого множителя в производной. Отделение кратных множителей.
14. Формулировка основной теоремы алгебры комплексных чисел. Вид неприводимых многочленов над полями комплексных и действительных чисел.
15. Понятие линейного пространства. Базис конечномерного линейного пространства. Ранг системы векторов в конечномерном пространстве. Корректность определения ранга.
16. Замена базиса в конечномерном линейном пространстве. Матрица перехода. Связь между координатами одного вектора в разных базисах.
17. Подпространства линейного пространства. Сумма подпространств. Пересечение подпространств. Связь размерности суммы с размерностью пересечения.
18. Построение базиса суммы двух подпространств. Построение базиса пересечения двух подпространств. Прямая сумма подпространств.
19. Изоморфизм линейных пространств.
20. Линейные отображения. Ядро и образ. Теорема о связи между рангом и дефектом линейного отображения.Способы определения (введения) линейного отображения.
21. Матрица линейного преобразования конечномерного линейного пространства и ее изменения при переходе к другому базису. Подобные матрицы.
22. Понятие алгебры. Алгебра многочленов от одной буквы над полем. Алгебра квадратных матриц над полем. Изоморфизм алгебр. Алгебра линейных преобразований линейного пространства и ее изоморфизм подходящей алгебры матриц.
23. Совпадение характеристических корней и собственных чисел линейного преобразования. Линейная независимость системы собственных векторов, принадлежащих попарно различным собственным значениям. Собственные подпространства.
24. Критерий того, что матрица подобна диагональной. Инвариантные подпространства.
25. Определение евклидова пространства. Ортогонализация. Существование ортонормированного базиса.

26. Определение евклидова пространства. Вычисление скалярных произведений в произвольном базисе. Вычисление скалярных произведений в ортонормированном базисе. Изоморфизм евклидовых пространств.
27. Подпространства евклидова пространства. Дополнение ортонормированного базиса подпространства до ортонормированного базиса пространства. Ортогональное дополнение. Свойства ортогональных дополнений.
28. Неравенство Коши. Определения длины вектора и угла между вектором и подпространством. Их корректность. Неравенство треугольника.
29. Ортогональные матрицы как матрицы перехода в евклидовом пространстве. Симметрические преобразования евклидовых пространств.
30. Существование инвариантных подпространств размерности 1 или 2 в линейном пространстве над полем действительных чисел. Ортогональные преобразования евклидовых пространств.

Третий семестр.

1. Инвариантные подпространства. Корневые подпространства и их инвариантность. Пересечения корневых подпространств, относящихся к различным собственным значениям.
2. Разложение линейного пространства в прямую сумму корневых подпространств.
3. Линейная зависимость системы векторов относительно подпространства. Жорданова форма матрицы линейного преобразования, имеющего единственное собственное число.
4. Доказательство теоремы о существовании жордановой матрицы линейного преобразования линейного пространства над полем комплексных чисел.
5. Доказательство единственности жордановой формы матрицы.
6. Полугруппы. Свойства степеней. Понятие группы. Простейшие свойства. Критерий группы.
7. Подгруппы. Подгруппа четных подстановок.
8. Изоморфизм групп. Примеры. Теорема Кэли.
9. Смежные классы. Разложение группы по подгруппе. Теорема Лагранжа о делимости порядка группы на порядок подгруппы.
10. Порядок элемента. Циклические группы. Подгруппы циклических групп. Строение групп простого порядка.
11. Нормальные подгруппы. Примеры нормальных подгрупп. Контрпримеры. Нормальность подгрупп индекса 2.
12. Понятие факторгруппы и его корректность. Примеры построения факторгрупп.
13. Понятие гомоморфизма групп. Теорема о гомоморфизме групп.

14. Восстановление подгруппы в прообразе из подгруппы в образе.
15. Отношение сопряженности в группе. Свойства сопряженных элементов группы.
16. Централизатор элемента. Теорема об индексе централизатора элемента конечной группы.
17. Центр группы. Нетривиальность центра ***p***-группы.
18. Существование в коммутативной группе порядка делящегося на простое ***p*** элемента порядка ***p.***
19. Формулировка теоремы Силова. Доказательство теоремы Силова в части «существование».
20. Прямые произведения групп. Критерий разложения группы в прямое произведение своих подгрупп.
21. Теорема о строении конечных коммутативных групп.

Четвертый семестр.

1. Понятие кольца. Подкольца. Понятие идеала. Сумма и пересечение идеалов. Примеры.
2. Сравнимость по данному модулю. Кольцо классов вычетов по данному модулю.
3. Главные идеалы. Кольцо целых чисел как кольцо главных идеалов. Кольцо кольцо многочленов над полем как кольцо главных идеалов. Пример кольца, которое не является кольцом главных идеалов.
4. Факторкольцо. Кольцо классов вычетов как пример факторкольца. Поле классов вычетов по простому модулю.
5. Поле комплексных чисел как факторкольцо.
6. Построение поля частных.
7. Теорема существования корня. Поле разложения многочлена.
8. Понятие поля. Пример поля, которое содержит иррациональные числа, содержится в поле действительных чисел, но не совпадает с ним.
9. Понятие простого поля. Поле рациональных чисел как наименьшее поле, содержащее кольцо целых чисел.
10. Характеристика поля. Простые конечные поля. Число элементов в конечном поле.
11. Изоморфизм минимальных полей, в которых данный неприводимый многочлен имеет корень. Наименьшая степень расширения поля, в котором неприводимый многочлен имеет корень.
12. Существование конечного поля каждого порядка, являющегося степенью простого числа.
13. Цикличность мультипликативной группы конечного поля.
14. Подполя конечного поля.
15. Существование многочлена произвольной степени над конечным полем, который неприводим над этим полем. Конечное поле как множество корней некоторого многочлена.

16. Критерий Батлера неприводимости данного многочлена над конечным полем и его применение.
17. Делимость целых чисел. Деление с остатком. Алгоритм Евклида. Разложение НОД. Критерий взаимной простоты. Простые числа и их бесконечность. Существование и единственность разложения на простые множители.
18. Решение сравнений первой степени. Использование алгоритма Евклида.
19. Решение сравнений второй степени. Квадратичные вычеты. Закон взаимности квадратичных вычетов.
20. Функция Эйлера, её вычисление и применение.
21. Функция Мёбиуса. Формула обращения Мёбиуса.
22. Первообразные корни и индексы. Дискретный логарифм.

VIII. Перечень педагогических и информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (по необходимости)

Adobe Acrobat Reader DC - Russian	бесплатно
Cadence SPB/OrCAD 16.6	Государственный контракт на поставку лицензионных программных продуктов 103 - ГК/09 от 15.06.2009
Git version 2.5.2.2	бесплатно
Google Chrome	бесплатно
Kaspersky Endpoint Security 10 для Windows	Акт на передачу прав ПК545 от 16.12.2022
Lazarus 1.4.0	бесплатно
Mathcad 15 M010	Акт предоставления прав ИС00000027 от 16.09.2011;
MATLAB R2012b	Акт предоставления прав № Us000311 от 25.09.2012;
Многофункциональный редактор ONLYOFFICE	бесплатно
ОС Linux Ubuntu бесплатное ПО	бесплатно
Microsoft Web Deploy 3.5	бесплатно
MiKTeX 2.9	бесплатно
MSXML 4.0 SP2 Parser and SDK	бесплатно
MySQL Workbench 6.3 CE	бесплатно
NetBeans IDE 8.0.2	бесплатно
Notepad++	бесплатно
Origin 8.1 Sr2	договор №13918/M41 от 24.09.2009 с ЗАО «СофтЛайн Трейд»;
PostgreSQL 9.6	бесплатно
Python 3.4.3	бесплатно
Visual Studio 2010 Prerequisites - English	Акт на передачу прав №785 от 06.08.2021 г.

WCF RIA Services V1.0 SP2	бесплатно
WinDjView 2.1	бесплатно
WinPcap 4.1.3	бесплатно
Wireshark 2.0.0 (64-bit)	бесплатно
R studio	бесплатно

IX. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Учебная аудитория с мультимедийной установкой (Ноутбук, проектор, колонки), наличие классной доски.

X. Сведения об обновлении рабочей программы дисциплины (или модуля)

№п. п.	Обновленный раздел рабочей программы дисциплины (или модуля)	Описание внесенных изменений	Дата и протокол заседания кафедры, утвердившего изменения
1.			
2.			