МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

СОГЛАСОВАНО:	УТВЕРЖДАЮ:
Выпускающая кафедра ВССиИБ	Директор ИУЦТ
Заведующий кафедрой ВССиИБ	
Б.В. Желенков	С.П. Вакуленко
30 апреля 2020 г.	30 апреля 2020 г.

Кафедра «Цифровые технологии управления транспортными процессами»

Автор Семенов Юрий Станиславович, к.ф.-м.н., доцент

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Дискретная математика. Алгебра и теория чисел.

Направление подготовки:	10.03.01 – Информационная безопасность
Профиль:	Безопасность компьютерных систем
Квалификация выпускника:	Бакалавр
Форма обучения:	очная
Год начала подготовки	2020

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 4 30 апреля 2020 г. Председатель учебно-методической комиссии Н.А. Клычева	Протокол № 1 27 апреля 2020 г. Доцент В.Е. Нутович

Москва 2020 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Дисциплина "Дискретная математика. Алгебра и теория чисел." предназначена для получения знаний при решении следующих профессиональных задач: основы алгебры, теории чисел, теории групп; задачи, связанные с делимостью чисел, построение конечных полей, работа с группами обратимых элементов конечных полей.

Дисциплина формирует знания и умения для решения следующих профессиональных задач (в соответствии с видами профессиональной деятельности).

Эксплуатационная:
- установка, настройка, эксплуатация и поддержание в работоспособном состоянии компонентов системы обеспечения информационной безопасности с учетом установленных требований;
- администрирование подсистем информационной безопасности объекта, участие в проведении аттестации объектов информатизации по требованиям безопасности информации и аудите информационной безопасности автоматизированных систем;

Проектно-технологическая:
- сбор и анализ исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности;
- проведение проектных расчетов элементов систем обеспечения информационной безопасности;
- участие в разработке технологической и эксплуатационной документации;
- проведение предварительного технико-экономического обоснования проектных расчетов

Экспериментально-исследовательская деятельность:
- сбор, изучение научно-технической информации, отечественного и зарубежного опыта по тематике исследования;
- проведение экспериментов по заданной методике, обработка и анализ их результатов;
- проведение вычислительных экспериментов с использованием стандартных программных средств

Организационно-управленческая деятельность:
- осуществление организационно-правового обеспечения информационной безопасности объекта защиты;
- организация работы малых коллективов исполнителей;
- участие в совершенствовании системы управления информационной безопасностью;
- изучение и обобщение опыта работы других учреждений, организаций и предприятий в области защиты информации, в том числе информации ограниченного доступа;
- контроль эффективности реализации политики информационной безопасности объекта защиты.

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Учебная дисциплина "Дискретная математика. Алгебра и теория чисел." относится к блоку 1 "Дисциплины (модули)" и входит в его базовую часть.

2.1. Наименования предшествующих дисциплин

Для изучения данной дисциплины необходимы следующие знания, умения и навыки, формируемые предшествующими дисциплинами:

2.1.1. Основы управления информационной безопасностью:

Знания: принципы работы с информацией, основные угрозы информационной безопасности и методы защиты от них; основные нормативные документы, определяющие политику безопасности предприятия; современные принципы разработки ИБ, процессов управления ИБ и направления их развития

Умения: использовать информационные системы для поиска необходимой информации, оценивать степень угрозы информационной безопасности эксплуатируемой системы; анализировать текущее состояние ИБ на предприятии, определять цели и задачи, решаемые создаваемыми процессами управления ИБ; применять процессный подход к управлению к обеспечению информационной безопасности объекта защиты

Навыки: основными приемами обнаружения и предотвращения угроз информационной безопасности; навыками управления информационной безопасностью объектов, терминологией и методами построения СУИБ.

2.1.2. Программно-аппаратные средства защиты информации:

Знания: : методы и средства конфигурирования и контроля работоспособности средств безопасности, предоставляемых аппаратно-программными комплексами; эксплуатационные параметры и технические характеристики аппаратных и технических средств защиты информации

Умения: контролировать работу подсистем и изменять конфигурационные параметры при необходимости, применять методы и средства контроля работоспособности средств безопасности, предоставляемых аппаратно-программными комплексами; проверять работоспособность элементов системы защиты с помощью необходимых технических средств

Навыки: навыками по настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации.

2.1.3. Техническая защита информации:

Знания: концепции инженерно-технической защиты информации, основных угроз безопасности информации, порядка организации инженерно-технической защиты информации;основных руководящих и нормативных документов по инженерно-технической защите информации

Умения: выявлять угрозы и технические каналы утечки информации; контролировать эффективность мер защиты;

Навыки: Применять необходимые технические средства защиты информации для обеспечения ИБ.

2.2. Наименование последующих дисциплин

Результаты освоения дисциплины используются при изучении последующих учебных дисциплин:

2.2.1. Преддипломная практика

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

В результате освоения дисциплины студент должен:

№ п/п	Код и название компетенции	Ожидаемые результаты
1	ОПК-2 Способен использовать совокупность необходимых математических методов для решения задач обеспечения защиты информации;	ОПК-2.1 Знать необходимые математические методы для решения задач обеспечения защиты информации. ОПК-2.2 Уметь совокупность необходимых математических методов для решения задач обеспечения защиты информации. ОПК-2.3 Владеть навыками применения совокупности необходимых математических методов для решения задач обеспечения защиты информации.
2	ПКО-11 Способность проводить обработку и анализ результатов проведения экспериментов по изучению и тестированию системы обеспечения информационной безопасности или ее отдельных элементов;	ПКО-11.1 Знать методы обработки и анализа результатов проведения экспериментов. ПКО-11.2 Уметь выбирать необходимые методы для обработки и анализа результатов проведения экспериментов. ПКО-11.3 Владеть навыками обработки и анализа результатов проведения экспериментов по изучению и тестированию системы обеспечения информационной безопасности или ее отдельных элементов.
3	УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач.	УК-1.1 Знать принципы поиска информации. УК-1.2 Уметь применять системный подход для решения поставленных задач. УК-1.3 Владеть методом поиска и критического анализа информации. УК-1.4 Способен анализировать основные закономерности физических явлений и процессов.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ) В ЗАЧЕТНЫХ ЕДИНИЦАХ И АКАДЕМИЧЕСКИХ ЧАСАХ

4.1. Общая трудоемкость дисциплины составляет:

3 зачетных единиц (108 ак. ч.).

4.2. Распределение объема учебной дисциплины на контактную работу с преподавателем и самостоятельную работу обучающихся

	Количество часов	
Вид учебной работы	Всего по учебному плану	Семестр 3
Контактная работа	32	32,15
Аудиторные занятия (всего):	32	32
В том числе:		
лекции (Л)	16	16
практические (ПЗ) и семинарские (С)	16	16
Самостоятельная работа (всего)	76	76
ОБЩАЯ трудоемкость дисциплины, часы:	108	108
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	3.0	3.0
Текущий контроль успеваемости (количество и вид текущего контроля)	ПК1, ПК2	ПК1, ПК2
Виды промежуточной аттестации (экзамен, зачет)	ЗаО	ЗаО

4.3. Содержание дисциплины (модуля), структурированное по темам (разделам)

№ п/п	Семестр	Тема (раздел) учебной дисциплины	Виды учебной деятельности в часах/ в том числе интерактивной форме						Формы текущего контроля успеваемости и промежу-точной аттестации
			Л	ЛР	ПЗ/ТП	КСР	СР	Всего	
1	2	3	4	5	6	7	8	9	10
1	3	Раздел 1 Арифметикацелых чисел и колец вычетов	5		5		24	34	
2	3	Тема 1.1 Целые числа, метод математической индукции	1					1	
3	3	Тема 1.2 Алгоритм Евклида	2					2	
4	3	Тема 1.3 Сравнения по модулю	2					2	ПК1
5	3	Раздел 2 Алгебраические структуры.	6		6		24	36	
6	3	Тема 2.1 Кольца вычетов	2					2	
7	3	Тема 2.2 Кольца	2					2	ПК2
8	3	Тема 2.3 Поля	2					2	
9	3	Раздел 3 Кольца многочленов. Расширение колец и полей.	5		5		28	38	
10	3	Тема 3.1 Кольцо многочленов,Алгоритм Евклида	2					2	
11	3	Тема 3.2 Расширения полей	2					2	
12	3	Тема 3.3 Конечные поля	1					1	
13	3	Раздел 4 Итоговая аттестация						0	ЗаО
14		Всего:	16		16		76	108	

4.4. Лабораторные работы / практические занятия

Лабораторные работы учебным планом не предусмотрены.

Практические занятия предусмотрены в объеме 16 ак. ч.

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Наименование занятий	Всего часов/ из них часов в интерактивной форме
1	2	3	4	5
1	3	РАЗДЕЛ 1 Арифметикацелых чисел и колец вычетов	Целые числа, метод математической индукции	1
2	3	РАЗДЕЛ 1 Арифметикацелых чисел и колец вычетов	Алгоритм Евклида	2
3	3	РАЗДЕЛ 1 Арифметикацелых чисел и колец вычетов	Сравнения по модулю(интерактив)	2
4	3	РАЗДЕЛ 2 Алгебраические структуры.	Кольца вычетов	2
5	3	РАЗДЕЛ 2 Алгебраические структуры.	Кольца	2
6	3	РАЗДЕЛ 2 Алгебраические структуры.	Поля(интерактив)	2
7	3	РАЗДЕЛ 3 Кольца многочленов. Расширение колец и полей.	Кольцо многочленов,Алгоритм Евклида	2
8	3	РАЗДЕЛ 3 Кольца многочленов. Расширение колец и полей.	Расширения полей	2
9	3	РАЗДЕЛ 3 Кольца многочленов. Расширение колец и полей.	Конечные поля(интерактив)	1
			ВСЕГО:	16/0

4.5. Примерная тематика курсовых проектов (работ)

Курсовые работы (проекты) не предусмотрены.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины " Дискретная математика. Алгебра и теория чисел (дополнительные главы)" осуществляется в форме лекций и практических занятий. Лекции проводятся в традиционной классно-урочной организационной форме, по типу управления познавательной деятельностью и на 100% являются традиционными классически-лекционными (объяснительно-иллюстративные.
Практические занятия организованы с использованием технологий развивающего обучения. Часть практического курса выполняется в виде традиционных практических занятий (объяснительно-иллюстративное решение задач) в объёме 12 часов. Остальная часть практического курса (6 часов) проводится с использованием интерактивных (диалоговые) технологий, в том числе разбор и анализ конкретных ситуаций, дискуссии (решение проблемных поставленных задач и исследование моделей); технологий, основанных на коллективных способах обучения (возможны видеоконференции при подготовке курсовых работ).
Самостоятельная работа студента организована с использованием традиционных видов работы и интерактивных технологий. К традиционным видам работы относятся отработка лекционного материала и отработка отдельных тем по учебным пособиям. К интерактивным (диалоговым) технологиям относится отработка отдельных тем по электронным пособиям, подготовка к текущему и промежуточному контролю, интерактивные консультации в режиме реального времени по специальным разделам и технологиям, основаным на коллективных способах самостоятельной работы студентов.
Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Фонды оценочных средств освоенных компетенций включают как вопросы теоретического характера для оценки знаний, так и задания практического содержания для оценки умений и навыков. Теоретические знания проверяются путём применения таких организационных форм, как индивидуальные и групповые решения задач, решение индивидуальных заданий с использованием компьютеров или на бумажных носителях.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

№ п/п	№ семестра	Тема (раздел) учебной дисциплины	Вид самостоятельной работы студента. Перечень учебно-методического обеспечения для самостоятельной работы	Всего часов
1	2	3	4	5
1	3	РАЗДЕЛ 1 Арифметикацелых чисел и колец вычетов	Целые числа, метод математической индукции	8
2	3	РАЗДЕЛ 1 Арифметикацелых чисел и колец вычетов	Алгоритм Евклида	8
3	3	РАЗДЕЛ 1 Арифметикацелых чисел и колец вычетов	Сравнения по модулю	8
4	3	РАЗДЕЛ 2 Алгебраические структуры.	Кольца вычетов	8
5	3	РАЗДЕЛ 2 Алгебраические структуры.	Кольца	8
6	3	РАЗДЕЛ 2 Алгебраические структуры.	Поля	8
7	3	РАЗДЕЛ 3 Кольца многочленов. Расширение колец и полей.	Кольцо многочленов,Алгоритм Евклида	8
8	3	РАЗДЕЛ 3 Кольца многочленов. Расширение колец и полей.	Расширения полей	8
9	3	РАЗДЕЛ 3 Кольца многочленов. Расширение колец и полей.	Конечные поля	12
			ВСЕГО:	76

7. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Основная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
1	Введение в алгебру	Кострикин А.И.	М:Физматлит, 2004 Библиотека РУТ МИИТ	Все разделы
2	Сборник задач по линейной алгебре	Проскуряков И.В.	М: Бином, 2005 Библиотека РУТ МИИТ	Все разделы
3	Грани алгебры	Аршинов М. Н., Садовский Л.Е.	М: Факториал Пресс, 2008 Библиотека РУТ МИИТ	Все разделы
4	Алгебра, тригонометрия и элементарные функции	О. В. Александрова, Ю. С. Семенов	М.: Илекса, 2015 Библиотека РУТ МИИТ	Все разделы

7.2. Дополнительная литература

№ п/п	Наименование	Автор (ы)	Год и место издания Место доступа	Используется при изучении разделов, номера страниц
5	Классическое введение в современную теорию чисел	К. Айерлэнд,И. Роузен	М: МИР, 1987 Библиотека РУТ МИИТ	Все разделы

8. ПЕРЕЧЕНЬ РЕСУРСОВ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ "ИНТЕРНЕТ", НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

http://library.miit.ru/ - электронно-информационная система НТБ МИИТ

9. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Не требуется

10. ОПИСАНИЕ МАТЕРИАЛЬНО ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

10.1. Требования к аудиториям (помещениям, кабинетам) для проведения занятий с указаниям соответствующего оснащения
- Доска, мел, тряпка (губка) для стирания; компьютерное и мультимедийное оборудование: компьютер, проектор, экран;

10.2. Требования к программному обеспечению при прохождении учебной дисциплины
- пакет прикладных обучающих программ: MATHCAD, Maple

11. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Регулярно выполнять домашние задания, изучать дополнительные материалы, повторять темы из предыдущих семестров. Интересующимся студентам рекомендуется участвовать в студенческих олимпиадах.
Лекционные занятия составляют основу теоретического обучения и должны давать систематизированные основы знаний по дисциплине, раскрывать состояние и перспективы развития соответствующей области науки, концентрировать внимание обучающихся на наиболее сложных и узловых вопросах, стимулировать их активную познавательную деятельность и способствовать формированию творческого мышления.
Главная задача лекционного курса – сформировать у обучающихся системное представление об изучаемом предмете, обеспечить усвоение будущими специалистами основополагающего учебного материала, принципов и закономерностей развития соответствующей научно-практической области, а также методов применения полученных знаний, умений и навыков.
Выполнение практических заданий служит важным связующим звеном между теоретическим освоением данной дисциплины и применением ее положений на практике. Они способствуют развитию самостоятельности обучающихся, более активному освоению учебного материала, являются важной предпосылкой формирования профессиональных качеств будущих специалистов.
Проведение практических занятий не сводится только к органическому дополнению лекционных курсов и самостоятельной работы обучающихся. Их вместе с тем следует рассматривать как важное средство проверки усвоения обучающимися тех или иных положений, даваемых на лекции, а также рекомендуемой для изучения литературы; как форма текущего контроля за отношением обучающихся к учебе, за уровнем их знаний, а следовательно, и как один из важных каналов для своевременного подтягивания отстающих обучающихся.
При подготовке специалиста важны не только серьезная теоретическая подготовка. Этому способствует форма обучения в виде практических занятий. Задачи практических занятий: закрепление и углубление знаний, полученных на лекциях и приобретенных в процессе самостоятельной работы с учебной литературой, формирование у обучающихся умений и навыков работы с исходными данными, научной литературой и специальными документами. Практическому занятию должно предшествовать ознакомление с лекцией на соответствующую тему и литературой, указанной в плане этих занятий.
Самостоятельная работа может быть успешной при определенных условиях, которые необходимо организовать. Ее правильная организация, включающая технологии отбора целей, содержания, конструирования заданий и организацию контроля, систематичность самостоятельных учебных занятий, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.
Каждому студенту следует составлять еженедельный и семестровый планы работы, а также план на каждый рабочий день. С вечера всегда надо распределять работу на завтра. В конце каждого дня целесообразно подводить итог работы: тщательно проверить, все ли выполнено по намеченному плану, не было ли каких-либо отступлений, а если были, по какой причине это произошло. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Если что- то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана.
Компетенции обучающегося, формируемые в результате освоения учебной дисциплины, рассмотрены через соответствующие знания, умения и владения. Для проверки уровня освоения дисциплины предлагаются вопросы к экзамену и тестовые материалы, где каждый вариант содержит задания, разработанные в рамках основных тем учебной дисциплины и включающие терминологические задания.

Фонд оценочных средств является составной частью учебно-методического обеспечения процедуры оценки качества освоения образовательной программы и обеспечивает повышение качества образовательного процесса и входит как приложение в состав рабочей программы дисциплины.