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 сентября 2019 г.	30 сентября 2019 г.

Кафедра «Математическое моделирование и системный анализ»

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

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Дискретная математика. Алгебра и теория чисел (дополнительные главы)

Направление подготовки:	10.03.01 – Информационная безопасность
Профиль:	Безопасность компьютерных систем
Квалификация выпускника:	Бакалавр
Форма обучения:	очная
Год начала подготовки	2017

Одобрено на заседании	Одобрено на заседании кафедры
Учебно-методической комиссии института Протокол № 2 30 сентября 2019 г. Председатель учебно-методической комиссии Н.А. Клычева	Протокол № 10 24 июня 2019 г. И.о. заведующего кафедрой Г.А. Зверкина

Москва 2019 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Дисциплина 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 (дополнительные главы)" относится к блоку 1 "Дисциплины (модули)" и входит в его вариативную часть.

2.1. Наименования предшествующих дисциплин

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

2.1.1. Математика:

Знания: матричная алгебра, многочлены

Умения: проводить операции с матрицами, многочленами

Навыки: работа с матрицами, многочленами

2.1.2. Математическая логика и теория алгоритмов:

Знания: множества, отношения на множествах, классы эквивалентности

Умения: определять отношения эквивалентности

Навыки: работа с классами эквивалентности

2.2. Наименование последующих дисциплин

Результаты освоения дисциплины используются при изучении последующих учебных дисциплин:

2.2.1. Криптографические методы защиты информации

2.2.2. Криптографические протоколы

2.2.3. Числовые методы криптографии

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 способностью применять соответствующий математический аппарат для решения профессиональных задач	Знать и понимать: основные теоремы и формулы алгебры, теории чисел и дискретной математики, взаимосвязи между их отдельными областями. Уметь: решать задачи, связанные с делимостью чисел, строить конечные поля, работать с группами обратимых элементов конечных полей. Владеть: методами решения задач теории чисел, алгебры и теории групп
2	ПСК-1.2 способность использовать математические методы обработки, анализа и синтеза результатов профессиональных исследований (ПСК 1.2);	Знать и понимать: современную информационную картину мира в образовательной и профессиональной деятельности; основные методы, способы и средства получения, хранения, переработки информации; способы работы с информацией в глобальных компьютерных сетях. Уметь: применять различные методы обработки информации; работать с компьютером как средством управления информацией; обрабатывать информацию при помощи глобальных компьютерных сетей; определять место и сущность информационных процессов в современном обществе; Владеть: различными методами обработки информации, теоретического и экспериментального исследования; методами компьютерной обработки информации; методами поиска информации в глобальных компьютерных сетях; методами соблюдения требований информационной безопасности.

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

4.1. Общая трудоемкость дисциплины составляет:

2 зачетные единицы (72 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 4
Контактная работа	37	37,15
Аудиторные занятия (всего):	37	37
В том числе:		
лекции (Л)	16	16
практические (ПЗ) и семинарские (С)	18	18
Контроль самостоятельной работы (КСР)	3	3
Самостоятельная работа (всего)	35	35
ОБЩАЯ трудоемкость дисциплины, часы:	72	72
ОБЩАЯ трудоемкость дисциплины, зач.ед.:	2.0	2.0
Текущий контроль успеваемости (количество и вид текущего контроля)	ПК1, ПК2	ПК1, ПК2
Виды промежуточной аттестации (экзамен, зачет)	ЗЧ	ЗЧ

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	4	Раздел 1 Арифметикацелых чисел и колец вычетов	6/0		6/2	1	10	23/2	
2	4	Тема 1.1 Целые числа, метод математической индукции	2/0					2/0	
3	4	Тема 1.2 Алгоритм Евклида	2/0					2/0	
4	4	Тема 1.3 Сравнения по модулю	2			1		3	ПК1
5	4	Раздел 2 Алгебраические структуры.	6		6/2	1	10	23/2	
6	4	Тема 2.1 Кольца вычетов	2					2	
7	4	Тема 2.2 Кольца	2					2	ПК2
8	4	Тема 2.3 Поля	2			1		3	
9	4	Раздел 3 Кольца многочленов. Расширение колец и полей.	4/0		6/2	1	15	26/2	
10	4	Тема 3.1 Кольцо многочленов,Алгоритм Евклида	2/0					2/0	
11	4	Тема 3.2 Расширения полей	2/0					2/0	
12	4	Тема 3.3 Конечные поля				1		1	ЗЧ
13		Всего:	16/0		18/6	3	35	72/6	

4.4. Лабораторные работы / практические занятия

Лабораторные работы учебным планом не предусмотрены.

Практические занятия предусмотрены в объеме 18 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	4	РАЗДЕЛ 1 Арифметикацелых чисел и колец вычетов	Целые числа, метод математической индукции	2
2	4	РАЗДЕЛ 1 Арифметикацелых чисел и колец вычетов	Алгоритм Евклида	2
3	4	РАЗДЕЛ 1 Арифметикацелых чисел и колец вычетов	Сравнения по модулю(интерактив)	2 / 2
4	4	РАЗДЕЛ 2 Алгебраические структуры.	Кольца вычетов	2
5	4	РАЗДЕЛ 2 Алгебраические структуры.	Кольца	2
6	4	РАЗДЕЛ 2 Алгебраические структуры.	Поля(интерактив)	2 / 2
7	4	РАЗДЕЛ 3 Кольца многочленов. Расширение колец и полей.	Кольцо многочленов,Алгоритм Евклида	2
8	4	РАЗДЕЛ 3 Кольца многочленов. Расширение колец и полей.	Расширения полей	2
9	4	РАЗДЕЛ 3 Кольца многочленов. Расширение колец и полей.	Конечные поля(интерактив)	2 / 2
			ВСЕГО:	18/6

4.5. Примерная тематика курсовых проектов (работ)

Курсовые работы (проекты) не предусмотрены.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Преподавание дисциплины Б1.В.ОД.2 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	4	РАЗДЕЛ 1 Арифметикацелых чисел и колец вычетов	Целые числа, метод математической индукции	3
2	4	РАЗДЕЛ 1 Арифметикацелых чисел и колец вычетов	Алгоритм Евклида	3
3	4	РАЗДЕЛ 1 Арифметикацелых чисел и колец вычетов	Сравнения по модулю	4
4	4	РАЗДЕЛ 2 Алгебраические структуры.	Кольца вычетов	4
5	4	РАЗДЕЛ 2 Алгебраические структуры.	Кольца	3
6	4	РАЗДЕЛ 2 Алгебраические структуры.	Поля	3
7	4	РАЗДЕЛ 3 Кольца многочленов. Расширение колец и полей.	Кольцо многочленов,Алгоритм Евклида	5
8	4	РАЗДЕЛ 3 Кольца многочленов. Расширение колец и полей.	Расширения полей	4
9	4	РАЗДЕЛ 3 Кольца многочленов. Расширение колец и полей.	Конечные поля	6
			ВСЕГО:	35

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	Все разделы
2	Сборник задач по линейной алгебре	Проскуряков И.В.	М: Бином, 2005	Все разделы
3	Грани алгебры	Аршинов М. Н., Садовский Л.Е.	М: Факториал Пресс, 2008	Все разделы
4	Алгебра, тригонометрия и элементарные функции	О. В. Александрова, Ю. С. Семенов	М.: Илекса, 2015	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	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.