

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
 Федеральное государственное бюджетное образовательное учреждение
 высшего образования
 "Уральский государственный университет путей сообщения"
 (ФГБОУ ВО УрГУПС)

Б1.В.ДВ.06.01 Дискретная математика рабочая программа дисциплины (модуля)

Закреплена за кафедрой	Естественнонаучные дисциплины		
Учебный план	10.03.01 ИБ-2023.plx 10.03.01 Информационная безопасность		
Направленность (профиль)	Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)		
Квалификация	Бакалавр		
Форма обучения	очная		
Объем дисциплины (модуля)	3 ЗЕТ		
Часов по учебному плану	108	Часов контактной работы всего, в том числе:	38,05
в том числе:		аудиторная работа	36
аудиторные занятия	36	текущие консультации по лабораторным занятиям	1,8
самостоятельная работа	36	прием зачета с оценкой	0,25
Промежуточная аттестация и формы контроля:			
зачет с оценкой 3			

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	3 (2.1)		Итого	
	УП	РП	УП	РП
Неделя	18			
Вид занятий	УП	РП	УП	РП
Лекции	18	18	18	18
Лабораторные	18	18	18	18
Элект	36	36	36	36
Итого ауд.	36	36	36	36
Контактная работа	72	72	72	72
Сам. работа	36	36	36	36
Итого	108	108	108	108

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1	Цель дисциплины - формирование у обучающихся методологического фундамента для анализа проблемных ситуаций на основе системного подхода; а также формирование и развитие у обучающихся способностей решать инженерные задачи с помощью математических методов.
1.2	Задачи дисциплины: обучение математическим методам, навыкам решения математических задач; формирование умений и навыков применять математические методы при описании, анализе и решении практических задач, формирование у обучающихся понятийного и методологического аппарата современной дискретной математики и основ его применения в информационно-коммуникационной сфере в соответствии с доктриной информационной безопасности Российской Федерации.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОП

Цикл (раздел) ОП:	Б1.В.ДВ.06
2.1 Требования к предварительной подготовке обучающегося:	
Математика Для изучения данной учебной дисциплины необходимы знания, умения и навыки, приобретенные при изучении дисциплины Математика. Обучающиеся должны: Знать основные элементарные математические факты в области алгебры, геометрии, тригонометрии, математического анализа. Уметь проводить элементарные преобразования алгебраических выражений и элементарных функций, расчеты числовых выражений с элементарными функциями. Владеть опытом решения математических задач в объеме курса математики.	
2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:	
Математическая логика и теория алгоритмов Основы теории кодирования Стеганография	

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

УК-1: Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач
УК-1.3: Выполняет поиск необходимой информации, ее критический анализ и обобщает результаты анализа для решения поставленной задачи
УК-1.2: Осуществляет систематизацию информации различных типов для анализа проблемных ситуаций. Вырабатывает стратегию действий для построения алгоритмов решения поставленных задач
УК-1.1: Анализирует проблемную ситуацию (задачу) и выделяет ее базовые составляющие. Рассматривает различные варианты решения проблемной ситуации (задачи), разрабатывает алгоритмы их реализации
ПК-2: Способен администрировать средства защиты информации прикладного и системного программного обеспечения
ПК-2.6: Умеет анализировать текущие процессы, выделять основные операции и определять участки, требующие автоматизации и оптимизации, в том числе с применением технологии блокчейн

В результате освоения дисциплины обучающийся должен

3.1	Знать:
3.1.1	основные понятия и методы дискретной математики;
3.2	Уметь:
3.2.1	формулировать цели работы, составлять план достижения цели; использовать простейшие математические методы и модели для решения практических задач; применять элементарные методы анализа изучаемых явлений, процессов и проектных решений.
3.3	Владеть:
3.3.1	навыками составления плана исследования; методами количественного анализа процесса обработки информации.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов (академических)	Компетенции	Литература	Активные формы
	Раздел 1. Теория множеств, комбинаторика и основы теории вероятностей					

1.1	Элементы комбинаторики. Биномиальные коэффициенты. Разбиения. Правило произведения. Определение, множества и списки, объединение, пересечение, дополнение, симметрическая разность. Декартово произведение. Мощность, функции. Частотное определение вероятности. Комбинаторное правило вычисления вероятности. Функции, отображения, отношения, базы данных. Булевы функции /Лек/	3	4	УК-1.1 ПК-2.6	Л1.1Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4	
1.2	Комбинаторные функции. BBS /Лаб/	3	4	УК-1.2 УК-1.3	Л1.1Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4	Работа в группе по решению практико-ориентированных задач
1.3	Самостоятельное решение практических задач, ориентированное на тему :Комбинаторные задачи. /Ср/	3	10	УК-1.2 УК-1.3	Л1.1Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4	
Раздел 2. Теория отношений и алгебраических операций						
2.1	Представление бинарных отношений матрицами и орграфами. Отношения эквивалентности (разбиения и фактор-множества), отношения частичного порядка, диаграммы частично упорядоченного множества. Шифр Виженера. Автоматизация. Функция ПРОСМОТР Excel. Модулярная арифметика. /Лек/	3	4	УК-1.1 ПК-2.6	Л1.1Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4	
2.2	Шифр Виженера. Автоматизация. Функция ПРОСМОТР Excel. Бинарные отношения. Свойства отношений /Лаб/	3	4	УК-1.2 УК-1.3	Л1.1Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4	Работа в группе по решению практико-ориентированных задач
2.3	Самостоятельное решение практических задач, ориентированное на тему: теория отношений. /Ср/	3	6	УК-1.2 УК-1.3	Л1.1Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4	
Раздел 3. Алгебраические системы и модели						
3.1	Алгебраические системы и модели. Квазигруппы и совершенные шифры, подгруппоиды и подполугруппы. Группы. Проблема дискретного логарифма. Асимметричная криптография. Понятие кольца и поля. Булево кольцо. Кольцо вычетов Z_n по составному модулю n и поле Z_p . Неприводимые многочлены над простыми полями и построение полей данной характеристики и данной степени Поля разложения. /Лек/	3	4	УК-1.1 ПК-2.6	Л1.1Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4	
3.2	Первообразные корни. Проверка теорем Ферма и Эйлера. Дискретные логарифмы. Прямые и эллиптические кривые /Лаб/	3	4	УК-1.2 УК-1.3	Л1.1Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4	Работа в группе по решению практико-ориентированных задач

3.3	Самостоятельное решение практических задач, ориентированное на тему Дискретное логарифмирование. /Ср/	3	6	УК-1.2 УК-1.3	Л1.1Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4	
	Раздел 4. Приложения к конечным автоматам, теории кодирования и криптографии					
4.1	Различные определения конечных автоматов. Расшифровка и синтез конечных автоматов. Шифрующие и автономные конечные автоматы. Векторные пространства над полем действительных чисел, над полем комплексных чисел, над конечными полями. Полиномиальное кодирование. Совершенные шифры. Матроиды и жадные алгоритмы. Разграничения доступа к информации. Асимметричная криптография. /Лек/	3	6	УК-1.1 ПК-2.6	Л1.1Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4	
4.2	Моделирование работы LFSR. Построение таблиц полиномиального кодирования. Построение таблиц степеней корня неприводимого многочлена, в том числе использование GF(32) для кодирования русских букв. /Лаб/	3	6	УК-1.2 УК-1.3	Л1.1Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4	Работа в группе по решению практико-ориентированных задач
4.3	Самостоятельное решение практических задач, ориентированное на тему Операции над многочленами. Методы кодирования. /Ср/	3	6	УК-1.2 УК-1.3	Л1.1Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4	
4.4	Взаимодействие со студентами в электронной информационно-образовательной среде: Рецензирование контрольной работы и РГР /Элект/	3	36	УК-1.1 УК-1.2 УК-1.3 ПК-2.6	Л1.1Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4	
4.5	Подготовка к промежуточной аттестации. /Ср/	3	8	УК-1.1 УК-1.2 УК-1.3 ПК-2.6	Л1.1Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4	

5. ФОНД ОЦЕНОЧНЫХ МАТЕРИАЛОВ

Фонд оценочных материалов по дисциплине (модулю), состоящий из ФОМ для текущего контроля и проведения промежуточной аттестации обучающихся, разрабатывается по каждой дисциплине. Оценочные материалы размещаются на странице данного курса в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru), доступной через личный кабинет обучающегося.

Фонд оценочных материалов для проведения промежуточной аттестации обучающихся по дисциплине (модулю), включая порядок проведения промежуточной аттестации, систему оценивания результатов промежуточной аттестации и критерии выставления оценок, примеры типовых заданий или иных материалов, необходимых для оценки знаний, умений, навыков, используемых для промежуточной аттестации по дисциплине, приведен в приложении 1 к рабочей программе дисциплины.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

6.1.2. Дополнительная учебная литература

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л2.1	Гусева А.И., Киреев В.С.	Дискретная математика. Сборник задач: Учебное пособие	Москва: ООО "КУРС", 2021	http://znanium.com

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л2.2	Канцедал С.А.	Дискретная математика: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2019	http://znanium.com
Л2.3	Гусева А.И., Киреев В.С.	Дискретная математика: Учебник	Москва: ООО "КУРС", 2019	http://znanium.com

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л3.1	Геуг К. Л., Коновалова С. С., Титов С. С.	Дискретная математика: учебное пособие для занятий и самостоятельной работы студентов по дисциплине «Дискретная математика» направления подготовки 10.03.01 - «Информационная безопасность» очной формы обучения	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru
Л3.2	Геуг К. Л., Титов С. С.	Дискретная математика: методические указания к выполнению лабораторных работ для обучающихся по направлению подготовки 10.03.01 «Информационная безопасность» очной формы обучения	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Э1	Электронно-библиотечная система(www.e.lanbook.com)
Э2	Система электронной поддержки обучения Blackboard Learn (bb.usurt.ru)
Э3	Единый портал интернет-тестирования в сфере образования (www.i-exam.ru)
Э4	Образовательный математический сайт Exponenta.ru (old.exponenta.ru)

6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем

6.3.1 Перечень программного обеспечения

6.3.1.1	Неисключительные права на ПО Windows
6.3.1.2	Неисключительные права на ПО Office
6.3.1.3	Система электронной поддержки обучения Blackboard Learn
6.3.1.4	Mathcad

6.3.2 Перечень информационных справочных систем и профессиональных баз данных

6.3.2.1	Автоматизированная система правовой информации на железнодорожном транспорте АСПИ ЖТ (профессиональная БД)
6.3.2.2	Интерактивный справочник по математике, физике, химии (ИСС открытого доступа, https://www.fxyz.ru).
6.3.2.3	Мир математических уравнений (ИСС открытого доступа, http://eqworld.ipmnet.ru/indexr.htm)
6.3.2.4	MathTree - каталог математических интернет-ресурсов (ИСС открытого доступа, http://www.mathtree.ru).
6.3.2.5	Образовательный математический сайт Exponenta.ru (БД и ИСС открытого доступа по решению математических и прикладных задач в среде математических пакетов Mathcad, Matlab, Maple, Mathematica, Statistica, http://www.old.exponenta.ru)

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Назначение	Оснащение
Лаборатория "Математическое моделирование". Учебная аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также для самостоятельной работы. Компьютерный класс.	Специализированная мебель Компьютерная техника с установленным лицензионным ПО, предусмотренным пунктом 6.3.1 РПД, с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета
Учебная аудитория для проведения текущего	Специализированная мебель

контроля и промежуточной аттестации	
Учебная аудитория для проведения занятий лекционного типа	Специализированная мебель Демонстрационное оборудование - Комплект мультимедийного оборудования Учебно-наглядные пособия - презентационные материалы
Центр тестирования - Учебная аудитория для проведения текущего контроля и промежуточной аттестации	Специализированная мебель Моноблоки с установленным лицензионным ПО, включая ПО АСТ-Тест, с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета
Компьютерный класс - Учебная аудитория для проведения текущего контроля и промежуточной аттестации	Специализированная мебель Компьютерная техника с установленным лицензионным ПО, включая ПО АСТ-Тест, с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета
Компьютерный класс - Учебная аудитория для проведения практических (занятий семинарского типа) и лабораторных занятий, групповых и индивидуальных консультаций	Специализированная мебель Компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета Технические средства обучения - Комплект мультимедийного оборудования
Читальный зал Информационно-библиотечного центра ИБК УрГУПС - Аудитория для самостоятельной работы	Специализированная мебель Компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ) И ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Эффективное освоение дисциплины предполагает регулярное посещение всех видов аудиторных занятий, выполнение плана самостоятельной работы в полном объеме и прохождение аттестации в соответствии с календарным учебным графиком. Обучающемуся рекомендуется ознакомиться со списком основной и дополнительной литературы и взять в библиотеке издания (необходимо иметь при себе персонализированную электронную карту и уметь пользоваться электронным каталогом «ИРБИС»). Доступ к информационным ресурсам библиотеки и информационно-справочным системам сети «Интернет» организован в читальных залах библиотеки, в компьютерных классах, в помещениях для самостоятельной работы обучающихся со стационарных ПЭВМ, либо с личного ПЭВМ (ноутбука, планшетного компьютера или иного мобильного устройства) посредством беспроводного доступа при активации индивидуальной учетной записи. Пользование информационными ресурсами расширяет возможности освоения теоретического курса, выполнения самостоятельной работы и позволяет получить информацию для реализации творческих образовательных технологий. Комплект учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины (модуля), размещен на странице данного курса в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru), доступной через личный кабинет обучающегося. Перечень учебно-методических материалов (учебно-методического обеспечения) для самостоятельной работы обучающихся по дисциплине указан по темам дисциплины в разделе 4 РПД "Структура и содержание дисциплины (модуля)", материалы размещены на странице данного курса в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru). Методические материалы, разработанные для обеспечения образовательного процесса представлены в электронном каталоге УрГУПС. Для закрепления теоретического материала в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru) размещены тестовые материалы. Число тренировочных попыток ограничено. Тестовые материалы сформированы в логической последовательности в соответствии с изученными темами. Совместная деятельность преподавателя и обучающихся по проверке выполнения мероприятий текущего контроля, предусмотренных рабочей программой дисциплины (модуля) организована в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru). Для корректной работы в системе обучающиеся в разделе "Личные сведения" должны ввести актуальный адрес своей электронной почты. Формы самостоятельной работы обучающихся по данной дисциплине разнообразны. Они включают в себя: - изучение теоретического материала (учебной, научной, методической литературы, материалов периодических изданий); - подготовку к занятиям, предусмотренным РПД, мероприятиям текущего контроля, промежуточной аттестации и т.д. Выполнять самостоятельную работу и отчитываться по ее результатам обучающийся должен в соответствии с календарным планом изучения дисциплины, видами и сроками отчетности. При выполнении самостоятельной работы обучающемуся рекомендуется руководствоваться учебно-методическими материалами, размещенными на странице данного курса в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru), а также учебно-методическими материалами, которые указаны для самостоятельной работы по темам дисциплины в разделе 4 РПД "Структура и содержание дисциплины (модуля)".

При применении дистанционных образовательных технологий и электронного обучения освоение дисциплины (модуля) осуществляется в электронно-информационной образовательной среде (образовательная платформа электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru)) в рамках созданного курса, что позволяет реализовывать асинхронное и синхронное взаимодействие участников образовательных отношений.