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-2020.plx
Направление подготовки 10.03.01 Информационная безопасность
Направленность (профиль) "Организация и технология защиты информации (на транспорте)"

Направленность (профиль) направленность (профиль) N 2 "Организация и технология защиты информации" (по отрасли или в сфере профессиональной деятельности)

Квалификация **Бакалавр**

Форма обучения **очная**

Объем дисциплины (модуля) **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
аудиторные занятия 36
самостоятельная работа 72

Часов контактной работы всего, в том числе: 38,05
аудиторная работа 36
текущие консультации по лабораторным занятиям 1,8
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	
Недель	18			
Вид занятий	УП	РП	УП	РП
Лекции	18	18	18	18
Лабораторные	18	18	18	18
Итого ауд.	36	36	36	36
Контактная работа	36	36	36	36
Сам. работа	72	72	72	72
Итого	108	108	108	108

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Сформировать у обучающихся понятийный и методологический аппарат современной дискретной математики, заложить основы его применения в информационно-коммуникационной сфере в соответствии с доктриной информационной безопасности Российской Федерации. Программа курса ставит своей целью последовательное формирование, в процессе непрерывного математического образования, математической картины мира, во многом определяющей ключевые компетентности современного инженера путей сообщения и специалиста по информационным коммуникационным технологиям и системам.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОП	
Цикл (раздел) ОП:	Б1.В.ДВ.06

2.1 Требования к предварительной подготовке обучающегося:

Для изучения данной дисциплины необходимы знаниях, навыки и умениях, полученных студентами в процессе освоения школьной программы общеобразовательной школы по предмету Математика.
Студенты должны:
Знать основные элементарные математические факты в области алгебры, геометрии, тригонометрии, начал анализа.
Уметь проводить элементарные преобразования алгебраических выражений и элементарных функций, расчеты числовых выражений с элементарными функциями.
Владеть опытом решения математических задач в объеме курсов, изучаемых в общеобразовательном учреждении.

2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:

Криптографические методы защиты информации
Математическая логика и теория алгоритмов
Основы теории кодирования
Стеганография

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
ОПК-2: способностью применять соответствующий математический аппарат для решения профессиональных задач	
Знать:	
Уровень 1	основные формулы дискретной математики
Уровень 2	способы применения математического аппарата в профессиональной деятельности.
Уровень 3	способы использования математического аппарата при выявлении сущности проблем, возникающих в профессиональной деятельности.
Уметь:	
Уровень 1	находить способы использования основных математических формул.
Уровень 2	использовать математический аппарат в профессиональной деятельности.
Уровень 3	применять математический аппарат при выявлении сущности проблем, возникающих в профессиональной деятельности.
Владеть:	
Уровень 1	-
Уровень 2	-
Уровень 3	-

ПК-7: способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	
Знать:	
Уровень 1	приемы применения методов анализа изучаемых явлений, процессов и проектных решений.
Уровень 2	способы применения методов анализа изучаемых процессов и проектных решений.
Уровень 3	методы анализа изучаемых явлений и процессов.
Уметь:	
Уровень 1	анализировать изучаемые явления и данные.
Уровень 2	использовать методы анализа изучаемых явлений, процессов и проектных решений под руководством преподавателя
Уровень 3	самостоятельно применять методы анализа изучаемых явлений, процессов и проектных решений.
Владеть:	
Уровень 1	методами анализа изучаемых явлений, исходных данных для проектирования посдсистем и средств информационной безопасности
Уровень 2	-
Уровень 3	-

ПСК-4: способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	
Знать:	
Уровень 1	основные методы сбора исходных данных
Уровень 2	основные методы анализа исходных данных при решении практических задач
Уровень 3	методы сбора и анализа исходных данных для проектирования продуктов обеспечения информационнной безопасности
Уметь:	
Уровень 1	использовать методы сбора исходных данных при решении практических задач
Уровень 2	использовать методы сбора и анализа исходных данных при решении практических задач
Уровень 3	использовать методы сбора и анализа исходных данных при решении задач, связанных с проектированием средсств информационной безопасности
Владеть:	
Уровень 1	способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности при решении простых учебных задач
Уровень 2	способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности при решении задач повышенной сложности
Уровень 3	способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности при решении научно-исследовательских задач

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; навыками публичной речи, аргументации, изложения собственной точки зрения; 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. Биноминальные 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	ОПК-2 ПК-7 ПСК-4	Л1.1Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
1.2	Комбинаторные функции. BBS /Лаб/	3	4	ОПК-2 ПК-7 ПСК-4	Л1.1Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3 Э4	Работа в группе по решению практико - ориентированных задач
1.3	Решение практических задач по теме :Комбинаторные задачи. /Ср/	3	18	ОПК-2 ПК-7 ПСК-4	Л1.1Л3.1 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	ОПК-2 ПК-7 ПСК-4	Л1.1Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
2.2	Шифр Виженера. Автоматизация. Функция ПРОСМОТР Excel.Бинарные отношения. Свойства отношений /Лаб/	3	4	ОПК-2 ПК-7 ПСК-4	Л1.1Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3 Э4	Работа в группе по решению практико - ориентированных задач
2.3	Решение задач по теории отношений. /Ср/	3	18	ОПК-2 ПК-7 ПСК-4	Л1.1Л3.1 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 Zn по составному модулю n и поле Zp. Неприводимые многочлены над простыми полями и построение полей данной характеристики и данной степени Поля разложения. /Лек/	3	4	ОПК-2 ПК-7 ПСК-4	Л1.1Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	
3.2	Первообразные корни. Проверка теорем Ферма и Эйлера. Дискретные логарифмы. Прямые и эллиптические кривые /Лаб/	3	4	ОПК-2 ПК-7 ПСК-4	Л1.1Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3 Э4	Работа в группе по решению практико - ориентированных задач
3.3	Дискретное логарифмирование. /Ср/	3	18	ОПК-2 ПК-7 ПСК-4	Л1.1Л3.1 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 игформации. Асимметричная криптография. /Лек/	3	6	ОПК-2 ПК-7 ПСК-4	Л1.1Л2.1 Л2.2Л3.1 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	ОПК-2 ПК-7 ПСК-4	Л1.1Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3 Э4	Работа в группе по решению практико - ориентированных задач
4.3	Операции над многочленами. Методы кодирования. /Ср/	3	8	ОПК-2 ПК-7 ПСК-4	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4	

4.4	Подготовка к промежуточной аттестации. /Ср/	3	10	ОПК-2 ПК-7 ПСК-4	Л1.1Л2.1 Л2.2 Л2.3 Л2.4Л3.1 Л3.2 Э1 Э2 Э3 Э4	

5. ФОНД ОЦЕНОЧНЫХ МАТЕРИАЛОВ

Фонд оценочных материалов по дисциплине, состоящий из ФОМ для текущего контроля и проведения промежуточной аттестации обучающихся, разрабатывается по каждой дисциплине и хранится на кафедре. Оценочные материалы дублируются 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)

6.1.1. Основная учебная литература

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л1.1	Шевелев Ю. П.	Дискретная математика	Москва: Лань", 2016	http://e.lanbook.com

6.1.2. Дополнительная учебная литература

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л2.1	Канцедал С. А.	Дискретная математика: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2017	http://znanium.com
Л2.2	Гусева А.И., Киреев В.С.	Дискретная математика: Учебник	Москва: ООО "КУРС", 2017	http://znanium.com
Л2.3	Гусева А.И., Киреев В.С.	Дискретная математика. Сборник задач: Учебник Учебное пособие	Москва: ООО "КУРС", 2017	http://znanium.com
Л2.4	Гусева А.И., Киреев В.С.	Дискретная математика. Сборник задач: Учебное пособие	Москва: ООО "КУРС", 2018	http://znanium.com

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л3.1	Геут 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/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
Л3.2	Геут 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 Expenenta.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". Компьютерный класс - Учебная аудитория для проведения практических (занятий семинарского типа) и лабораторных занятий	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 контроля и промежуточной аттестации	Специализированная мебель
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.

Студенту рекомендуется ознакомиться со списком основной и дополнительной литературы и взять в библиотеке издания (необходимо иметь при себе персонифицированную 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 студентов 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.
Методические материалы, разработанные для обеспечения образовательного процесса представлены в электронном каталоге УрГУПС.
Формы самостоятельной работы студентов по данной дисциплине разнообразны. Они включают в себя:
- изучение лекционного и дополнительного материала (учебной, научной, методической литературы, материалов периодических изданий);
- подготовку к занятиям, предусмотренных РПД, мероприятиям текущего контроля и промежуточной аттестации
Выполнять самостоятельную работу и отчитываться по ее результатам студент должен в соответствии с календарным планом изучения дисциплины, видами и сроками отчетности.
При выполнении самостоятельной работы студент должен руководствоваться методическими указаниями, размещенными на странице данного курса в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru), а также учебно-методическими материалами, которые указаны для СРС по темам дисциплины в разделе 4 РПД "Структура и содержание дисциплины (модуля)".
Перечень 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).