Федеральное государственное бюджетное образовательное учреждение высшего образования
«Алтайский государственный технический университет им. И.И. Ползунова»

СОГЛАСОВАНО

Декан ФИТ А.С. Авдеев

Рабочая программа дисциплины

Код и наименование дисциплины: **Б1.О.16 «Дискретная математика и теория чисел»**

Код и наименование направления подготовки (специальности): **10.03.01 Информационная безопасность**

Направленность (профиль, специализация): **Организация и технологии защиты информации (в сфере техники и технологий, связанных с обеспечением защищенности объектов информатизации)**

Статус дисциплины: **обязательная часть**

Форма обучения: **очная**

Статус	Должность	И.О. Фамилия
Разработал	доцент	В.В. Лодейщикова
Согласовал	Зав. кафедрой «ВМ»	В.П. Зайцев
	руководитель направленности (профиля) программы	Е.В. Шарлаев

г. Барнаул

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция	Содержание компетенции	Индикатор	Содержание индикатора
ОПК-3	Способен использовать необходимые математические методы для решения задач профессиональной деятельности	ОПК-3.1	Применяет математический аппарат для решения задач

2. Место дисциплины в структуре образовательной программы

Дисциплины (практики), предшествующие изучению дисциплины, результаты освоения которых необходимы для освоения данной дисциплины.	Линейная алгебра и геометрия
Дисциплины (практики), для которых результаты освоения данной дисциплины будут необходимы, как входные знания, умения и владения для их изучения.	Методы и средства криптографической защиты информации, Теория вероятностей и математическая статистика, Теория информации и кодирования

3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающегося с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающегося

Общий объем дисциплины в з.е. /час: 4 / 144
Форма промежуточной аттестации: Экзамен

Форма обучения	Виды занятий, их трудоемкость (час.)				Объем контактной работы обучающегося с преподавателем (час)
	Лекции	Лабораторные работы	Практические занятия	Самостоятельная работа	
очная	32	0	48	64	84

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

Форма обучения: очная
Семестр: 2

Лекционные занятия (32ч.)

1. Элементы теории множеств, элементы комбинаторики.(6ч.)[3,4,5,6] Понятие множества, пустое и универсальное множества. Способы задания множеств. Числовые множества. Операции над множествами. Диаграммы Эйлера-Венна. Свойства операций над множествами. Булеан множества и его мощность. Разбиение множества. Декартово произведение множеств и его мощность в случае конечных сомножителей. Бинарные отношения. Конечные бинарные отношения, основные способы задания, представление отношений графами и матрицами. Виды бинарных отношений. Операции над бинарными отношениями, их свойства и выполнение в матричном виде. Основные свойства и матричные признаки специальных конечных однородных бинарных отношений. Замыкания. Матрицы основных замыканий конечного однородного отношения. Отношение эквивалентности и классы эквивалентности. Отношения порядка. Функции. Комбинаторные правила суммы и произведения. Сочетания, размещения, перестановки в схемах выбора с возвращением и без возвращения. Биномиальные коэффициенты и их свойства. Метод включений и исключений. Число функций, биекций, сюръекций.

2. Булевы функции (функции алгебры логики). {лекция с разбором конкретных ситуаций} (8ч.)[1,3,4,6] Понятие булевой функции, основные способы задания. Обзор всех булевых функций одного и двух переменных. Основные законы алгебры логики. Фиктивные и существенные переменные булевой функции. Дизъюнктивные и конъюнктивные нормальные формы булевых функций (ДНФ, КНФ). Совершенные дизъюнктивные и конъюнктивные нормальные формы (СДНФ, СКНФ). Полином Жегалкина. Понятие полноты системы булевых функций. Классы булевых функций. Критерий Поста о полноте. Минимизация булевых функций. Метод карт Карно. Контактные схемы. Функциональные элементы. Схемы из функциональных элементов. Задачи синтеза и анализа.

3. Элементы теории графов. {лекция с разбором конкретных ситуаций} (4ч.)[3,4,6] Определение графа. Ориентированные, неориентированные и смешанные графы. Изображение графа. Способы задания графов. Полные графы. Двудольные графы. Маршруты в графах. Деревья и их основные свойства. Основные теоремы теории графов. Каркас неориентированного графа, нахождение минимального каркаса неориентированного графа методом Краскала. Алгоритм Дейкстры для нахождения кратчайших маршрутов от одной из вершин до всех остальных вершин графа.

4. Алгебраические структуры. {лекция с разбором конкретных ситуаций} (4ч.)[3,5] Понятие алгебраической операции и алгебраической структуры. Определение и свойства групп. Циклические, симметрические группы. Теорема Кэли. Группа подстановок. Разложение группы по подгруппе. Теорема Лагранжа. Определение и свойства колец. Идеалы, классы вычетов, фактор-кольца. Определение и свойства полей. Поле вычетов. Конечные поля и их свойства.

5. Основы теории чисел. {лекция с разбором конкретных ситуаций} (10ч.)[2,5] Теория делимости. Основные понятия и теоремы. Наибольший общий делитель. Алгоритм Евклида. Наименьшее общее кратное. Простые числа и их

свойства. Единственность разложения на простые сомножители. Решето Эратосфена. Непрерывные дроби и их связь с алгоритмом Евклида. Понятие сравнения по данному модулю. Простейшие свойства сравнений. Полная система вычетов по модулю. Функция Эйлера и её основные свойства. Приведенная система вычетов. Теоремы Эйлера и Ферма. Китайская теорема об остатках. Сравнения первой степени. Система сравнений первой степени. Примеры использования математических методов теории чисел для решения задач профессиональной деятельности.

Практические занятия (48ч.)

1. Элементы теории множеств, элементы комбинаторики.(12ч.)[3,4,5,6] Множества и операции над ними. Операции над множествами. Анализ теоретико-множественных соотношений с помощью диаграмм Эйлера-Венна. Применение свойств операций над множествами. Бинарные отношения и операции над ними, специальные бинарные отношения. Замыкания. Матрицы основных замыканий конечного однородного отношения. Отношения порядка и эквивалентности. Способы задания, основные матрицы графов. Применение комбинаторных правил суммы и произведения. Применение сочетаний, размещений и перестановок в задачах пересчёта. Метод включений и исключений. Применение математического аппарата теории множеств для решения задач. Контрольная работа по теме "Элементы теории множеств, элементы комбинаторики".

2. Булевы функции (функции алгебры логики).(14ч.)[1,3,4,6] Построение таблиц истинности булевых функций. Доказательство равенства булевых функций с помощью таблиц истинности. Применение основных законов алгебры логики для доказательства равенства булевых функций. Представление булевых функций в виде ДНФ, КНФ. Исследование на существенность переменных булевой функции. Представление булевых функций в виде СДНФ, СКНФ. Представление булевой функции в виде полинома Жегалкина. Исследование системы булевых функций на полноту с помощью критерия Поста. Минимизация булевых функций методом карт Карно. Решение задач синтеза и анализа контактных схем и схем из функциональных элементов. Применение математического аппарата математической логики для решения задач. Контрольная работа по теме "Булевы функции".

3. Элементы теории графов.(8ч.)[3,4,6] Способы задания, основные матрицы графов. Эйлеровы и гамильтоновы графы. Планарные графы. Раскраска графов. Нахождение кратчайшего каркаса неориентированного графа методом Краскала. Алгоритм Дейкстры для нахождения кратчайших маршрутов от одной из вершин до всех остальных вершин графа. Применение математического аппарата теории графов для решения задач. Защита индивидуального домашнего задания по теме "Графы".

4. Алгебраические структуры.(4ч.)[3,5] Группы. Циклические группы. Группа подстановок. Кольца. Конечные поля.

5. Основы теории чисел.(10ч.)[2,5] Делимость целых чисел. Простые и

составные числа. Наибольший общий делитель и наименьшее общее кратное. Конечные непрерывные дроби. Числовые функции. Теоремы Эйлера и Ферма. Числовые сравнения. Системы вычетов. Сравнения первой степени. Системы сравнений первой степени. Применение математического аппарата теории чисел для решения задач. Контрольная работа по теме "Основы теории чисел".

Самостоятельная работа (64ч.)

1. Изучение теоретического материала.(8ч.)[1,2,3,4,5,6,7,8]
2. Подготовка к практическим занятиям.(8ч.)[1,2,3,4,5,6,7,8]
3. Подготовка к контрольным работам.(8ч.)[1,2,3,4,5,6,7,8]
5. Выполнение индивидуального домашнего задания.(4ч.)[1,2,3,4,5,6,7,8]
5. Подготовка к экзамену.(36ч.)[1,2,3,4,5,6,7,8]

5. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

Для каждого обучающегося обеспечен индивидуальный неограниченный доступ к электронно-библиотечным системам: Лань, Университетская библиотека он-лайн, электронной библиотеке АлтГТУ и к электронной информационно-образовательной среде:

1. Лодейщикова В.В. Функции алгебры логики [Электронный ресурс]: Учебное пособие.— Электрон. дан.— Барнаул: АлтГТУ, 2016.— Режим доступа: http://elib.altstu.ru/eum/download/vm/FunkAL.pdf, авторизованный.

6. Перечень учебной литературы

6.1. Основная литература

2. Виноградов, И. М. Основы теории чисел : учебное пособие / И. М. Виноградов. — 14-е изд., стер. — Санкт-Петербург : Лань, 2020. — 176 с. — ISBN 978-5-8114-5329-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/139285. — Режим доступа: для авториз. пользователей.

3. Кузнецов, О. П. Дискретная математика для инженера : учебное пособие / О. П. Кузнецов. — 6-е изд., стер. — Санкт-Петербург : Лань, 2021. — 400 с. — ISBN 978-5-8114-0570-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167753. — Режим доступа: для авториз. пользователей.

4. Шевелев, Ю. П. Дискретная математика : учебное пособие / Ю. П. Шевелев. — 3-е изд., стер. — Санкт-Петербург : Лань, 2018. — 592 с. — ISBN 978-5-8114-0810-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/107270. — Режим доступа: для авториз. пользователей.

6.2. Дополнительная литература

5. Мартынов, Л. М. Алгебра и теория чисел для криптографии : учебное пособие / Л. М. Мартынов. — Санкт-Петербург : Лань, 2020. — 456 с. — ISBN 978-5-8114-4424-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/140740. — Режим доступа: для авториз. пользователей.

6. Шевелев, Ю. П. Сборник задач по дискретной математике (для практических занятий в группах) : учебное пособие / Ю. П. Шевелев, Л. А. Писаренко, М. Ю. Шевелев. — Санкт-Петербург : Лань, 2021. — 528 с. — ISBN 978-5-8114-1359-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/168500. — Режим доступа: для авториз. пользователей.

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

7. https://intuit.ru/studies/courses/1084/192/info
8. https://intuit.ru/studies/courses/552/408/info

8. Фонд оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации

Содержание промежуточной аттестации раскрывается в комплекте контролирующих материалов, предназначенных для проверки соответствия уровня подготовки по дисциплине требованиям ФГОС, которые хранятся на кафедре-разработчике РПД в печатном виде и в ЭИОС.

Фонд оценочных материалов (ФОМ) по дисциплине представлен в приложении А.

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

Для успешного освоения дисциплины используются ресурсы электронной информационно-образовательной среды, образовательные интернет-порталы, глобальная компьютерная сеть Интернет. В процессе изучения дисциплины происходит интерактивное взаимодействие обучающегося с преподавателем через личный кабинет студента.

№пп	Используемое программное обеспечение
1	LibreOffice
2	Windows
3	Антивирус Kaspersky

№пп	Используемые профессиональные базы данных и информационные справочные системы
1	Бесплатная электронная библиотека онлайн "Единое окно к образовательным ресурсам" для студентов и преподавателей; каталог ссылок на образовательные интернет-ресурсы (http://Window.edu.ru)
2	Национальная электронная библиотека (НЭБ) — свободный доступ читателей к фондам российских библиотек. Содержит коллекции оцифрованных документов (как открытого доступа, так и ограниченных авторским правом), а также каталог изданий, хранящихся в библиотеках России. (http://нэб.рф/)

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Наименование специальных помещений и помещений для самостоятельной работы
учебные аудитории для проведения учебных занятий
помещения для самостоятельной работы

Материально-техническое обеспечение и организация образовательного процесса по дисциплине для инвалидов и лиц с ограниченными возможностями здоровья осуществляется в соответствии с «Положением об обучении инвалидов и лиц с ограниченными возможностями здоровья».