МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
"Казанский (Приволжский) федеральный университет"
Институт физики

УТВЕРЖДАЮ
Проректор по образовательной деятельности КФУ
Проф. Д.А. Таюрский
_____ «___»_____20__г.

подписано электронно-цифровой подписью

Программа дисциплины

Математическая логика и теория алгоритмов Б1.Б.32

Направление подготовки: 10.03.01 - Информационная безопасность
Профиль подготовки: Безопасность автоматизированных систем
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский

Автор(ы):

Патрин Е.В.

Рецензент(ы):

Аминова А.В.

СОГЛАСОВАНО:

Заведующий(ая) кафедрой: Сушков С. В.
Протокол заседания кафедры No ___ от "____" _____ 201__г
Учебно-методическая комиссия Института физики:
Протокол заседания УМК No ____ от "____" _____ 201__г

Регистрационный No 698819

Содержание

Программу дисциплины разработал(а)(и) ассистент, к.н. Патрин Е.В. Кафедра теории относительности и гравитации Отделение физики , Evgeny.Patrin@kpfu.ru

1. Цели освоения дисциплины

Целью освоения дисциплины является создание у обучающихся необходимой базы знаний для последующего изучения и усвоения других дисциплин математического и естественнонаучного цикла.

2. Место дисциплины в структуре основной образовательной программы высшего профессионального образования

Данная учебная дисциплина включена в раздел Б1.Б.32 Дисциплины (модули)' основной профессиональной образовательной программы 10.03.01 'Информационная безопасность (Безопасность автоматизированных систем)' и относится к базовой (общепрофессиональной) части.

Осваивается на 3 курсе в 5 семестре.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОПК-2 (профессиональные компетенции)	способность применять соответствующий математический аппарат для решения профессиональных задач

В результате освоения дисциплины студент:

4. должен демонстрировать способность и готовность:

применять основные положения математической логики и теории алгоритмов при работе с конкретными приложениями, программами и базами данных.

4. Структура и содержание дисциплины/ модуля

Общая трудоемкость дисциплины составляет 4 зачетных(ые) единиц(ы) 144 часа(ов).

Форма промежуточного контроля дисциплины: экзамен в 5 семестре.

Суммарно по дисциплине можно получить 100 баллов, из них текущая работа оценивается в 50 баллов, итоговая форма контроля - в 50 баллов. Минимальное количество для допуска к зачету 28 баллов.

86 баллов и более - "отлично" (отл.);

71-85 баллов - "хорошо" (хор.);
55-70 баллов - "удовлетворительно" (удов.);
54 балла и менее - "неудовлетворительно" (неуд.).

4.1 Структура и содержание аудиторной работы по дисциплине/ модулю

Тематический план дисциплины/модуля

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практи-ческие занятия	Лабора-торные работы	
1.	Тема 1. Элементы теории множеств.	5		7	0	7	
2.	Тема 2. Исчисление высказываний	5		7	0	7	
3.	Тема 3. Булевы и псевдобулевы функции	5		7	0	7	
4.	Тема 4. Исчисление предикатов	5		7	0	7	Устный опрос
5.	Тема 5. Понятие алгоритма	5		8	0	8	Контрольная работа
.	Тема . Итоговая форма контроля	5		0	0	0	Экзамен
	Итого			36	0	36	

4.2 Содержание дисциплины

Тема 1. Элементы теории множеств.

лекционное занятие (7 часа(ов)):

Элементы теории множеств. Понятия: алфавит, буква, слово, ис-числение, аксиома, теорема. Операции теории множеств: пересече-ние, объединение, свойства операций. Исчисление высказываний (ИВ). Понятия: алфавит ИВ, формула ИВ, терм. Правила вывода. Теорема о дедукции. Эквивалентность формул. Основные эквивалентные формулы. Цепи эквивалентностей. Таблицы истинности. Непротиворечивость ИВ, правила введения и удаления, полнота. Главная интерпретация ИВ (на множестве {0, 1}). Независимость ИВ.

лабораторная работа (7 часа(ов)):

решение задач по теме.

Тема 2. Исчисление высказываний

лекционное занятие (7 часа(ов)):

Исчисление предикатов (ИП). Понятия: предикат, n-местное отно-шение (его свойства), функция как двуместное отношение, квантор. ИВ как часть ИП. Общезначимость в ИП. Теорема о дедукции в ИП. Непротиворечивость и правила вывода теории доказательств ИП. Утверждения о полноте и непротиворечивости ИП. Теоремы Лин-денбаума и Геделя.

лабораторная работа (7 часа(ов)):

решение задач по теме.

Тема 3. Булевы и псевдобулевы функции

лекционное занятие (7 часа(ов)):

Булевы и псевдобулевы функции. Представление булевой функции в виде полинома. Степень представления. Псевдобулевы функции. Определение, представление в виде полиномов и позиформ (миними-зация булевой функции). Пример: алгоритмическая теория графов. Преобразование Фурье булевой и псевдобулевой функции. Вес Хэмминга булевой функции. Свойства дискретного преобразования Фурье. Криптографичекие свойства булевых функций. Аффинная экви-валентность, алгебраическая степень, нелинейность, сбалансирован-ность и k-резилентность. Линейные ядро и структура.

лабораторная работа (7 часа(ов)):

решение задач по теме.

Тема 4. Исчисление предикатов

лекционное занятие (7 часа(ов)):

Многозначные логики. Основные типы: Лукашевича, Геделя, t-норм система, трехзначная, четырехзначная система Данна-Беллнапа, система произведения. Функция k-значной логики. Отношение эквивалентности на мно-жестве функций k-значной логики. Циклический полином. Лемма Бернсайда. Теоремы де Брюина и Полиа.

лабораторная работа (7 часа(ов)):

решение задач по теме.

Тема 5. Понятие алгоритма

лекционное занятие (8 часа(ов)):

Понятие алгоритма и вычислимой функции. Примитивно и частично рекурсивные функции. Тезис Черча. Машина Тьюринга-Поста. Вычисления функций на машине Тьюринга-Поста. Универсальная машина Тьюринга. Теорема об универсальном алгоритме. Эффектив-ные алгоритмы. Сложность алгоритма. Оценки функции сложности. Пример: слож-ность арифметических операций. Классы задач P и NP. Тезис Колмо-горова. Реляционная алгебра, реляционное исчисление, понятие реляцион-ной схемы, его характеристики. Операции реляционной алгебры. Ба-зы данных.

лабораторная работа (8 часа(ов)):

решение задач по теме.

4.3 Структура и содержание самостоятельной работы дисциплины (модуля)

N	Раздел дисциплины	Се-местр	Неде-ля семе стра	Виды самостоятельной работы студентов	Трудо-емкость (в часах)	Формы контроля самосто-ятельной работы
4.	Тема 4. Исчисление предикатов	5		подготовка к устному опросу	18	Устный опрос
5.	Тема 5. Понятие алгоритма	5		подготовка к контрольной работе	18	Контроль-ная работа
	Итого				36	

5. Образовательные технологии, включая интерактивные формы обучения

Курс лекций и практических занятий, организованных по стандартной технологии в интерактивной форме с живым диалогом между преподавателем и студентом.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

Тема 1. Элементы теории множеств.

Тема 2. Исчисление высказываний

Тема 3. Булевы и псевдобулевы функции

Тема 4. Исчисление предикатов

Устный опрос , примерные вопросы:

понятие множества равенство и включение множеств Операции над множествами: пересечение, объединение, Разность, декартово произведение. Отношения (нуль, у,би, n-арные) Отношения эквивалентности и порядка. функции как бинарные отношения. мощность множеств системы аксиом теории множеств. континуум гипотеза.

Тема 5. Понятие алгоритма

Контрольная работа , примерные вопросы:

Решение задач по теме. Примерные вопросы и задачи: 1. Найти такую формулу f, что $f(0, 0, 0, 1)=f(1,0,0,1)=1$, остальные значения --- 0. Найти ее полином Жегалкина, СКН, СДН. 2. Построить таблицу истинности для выражения $((A \to B) \vee (B \leftrightarrow C))\wedge(A|B)$ II. 1. Найти такую формулу f, что $f(0, 0, 1, 1)=f(1,1,0,0)=1$, остальные значения --- 0. Найти ее полином Жегалкина, СКН, СДН. 2. Построить таблицу истинности для выражения $((A \vee B) \downarrow (B \wedge C))\leftrightarrow(A \to B)$ III. 1. Найти такую формулу f, что $f(0, 0, 0, 1)=f(1,0,1,1)=1$, остальные значения --- 0. Найти ее полином Жегалкина, СКН, СДН. 2. Построить таблицу истинности для выражения $((A \leftrightarrow B) \vee (B \downarrow C))\wedge(A|(B \to C))$ IV. 1. Найти такую формулу f, что $f(0, 0, 0, 1)=f(1,0,0,1)=1$, остальные значения --- 0. Найти ее полином Жегалкина, СКН, СДН. 2. Построить таблицу истинности для выражения $((A \wedge B) \downarrow (B \vee C))\leftrightarrow(A \cdot B)$ \pagebreak V. 1. Найти такую формулу f, что $f(0, 1, 0, 1)=f(1,0,0,1)=1$, остальные значения --- 0. Найти ее полином Жегалкина, СКН, СДН. 2. Построить таблицу истинности для выражения $((A \to B) + (B \leftrightarrow C))\wedge(C|B')$ VI. 1. Найти такую формулу f, что $f(1, 0, 1, 0)=f(1,0,0,1)=1$, остальные значения --- 0. Найти ее полином Жегалкина, СКН, СДН. 2. Построить таблицу истинности для выражения $((A \vee B) \downarrow (B \wedge C))\leftrightarrow(A \to B)$ XV 1. Является ли предикат примитивно-рекурсивным? $x+y=10$ 2. Найти функцию, определенную с помощью оператора минимизации. $f(x, y)=\mu z(-2^x+ \log z=y).$ XVI 1. Является ли функция примитивно-рекурсивной? $f(x, y)=r(x,y)+4 [y/ x]$ 2. Найти функцию, определенную с помощью оператора минимизации. $f(x, y)=\mu z(z-x^2+x^3=y^2).$

Итоговая форма контроля

экзамен (в 5 семестре)

Примерные вопросы к экзамену:

Вопросы к экзамену:

1. Понятия теории множеств: алфавит, буква, слово, исчисление, аксиома, теорема. Определения и ос-новные свойства.

2. Операции теории множеств: пересечение, объединение, свойства операций.

3. Основные понятия исчисления высказываний: алфавит ИВ, формула ИВ, терм, коньюнкция, дизьюнк-ция и их свойства.

4. Правила вывода ИВ. Теорема о дедукции ИВ.

5. Эквивалентность формул ИВ. Основные эквивалентные формулы ИВ (с доказательством). Цепи экви-валентностей ИВ.

6. Теорема о замене связок ИВ.

7. Таблицы истинности в ИВ. Теорема о подстановке вместо атомов.

8. Основная теорема о подстановках.

9. Теорема о дедукции ИВ и ее следствия.

10. Понятия доказуемости и выводимости в ИВ. Теоремы о формальных доказательствах и выводах.

11. Правила введения и удаления ИВ.
12. Теорема о полноте ИВ.
13. Главная интерпретация ИВ (на множестве {0, 1}).
14. Основные понятия ИП: предикат, n-местное отношение (его свойства), функция как двуместное отно-шение, квантор. ИВ как часть ИП.
15. Таблица истинности формулы ИП. Общезначимость в ИП.
16. Основные утверждения об общезначимости ИП.
17. Понятия следование, доказуемости и выводимости ИП.
18. Теорема о дедукции ИП.
19. Правила введения и удаления в ИП. Непротиворечивость ИП.
20. Цепи эквивалентностей ИП. Теорема о замене.
21. Теорема об изменении кванторов (основные формулы).
22. Утверждения о полноте ИП. Лемма Линденбаума.
23. Теорема Геделя о полноте ИП.
24. Булевы функции. Определение, свойства. Булевы выражения.
25. Двойственность для булевой функции. Свойства двойственных функций.
26. Алгебраическая нормальная форма булевой функции. Теорема о представлении булевой функции в нормальной форме.
27. Алгоритм получения нф булевой функции. Алгебраическая степень представления булевой функции в нормальной форме.
28. Численная нормальная форма булевой и псевдобулевой функции. Обобщенная степень булевой функ-ции.
29. Основные представления булевых функций. Представление в виде позиформ.
30. Алгоритмическая теория графов.
31. Псевдобулевы функции. Определение, примеры, свойства.
32. Представление псевдобулевой функции в виде полинома.
33. Дискретное преобразование Фурье (Адамара) псевдобулевой функции. Алгоритм вычиления преобра-зования Фурье от данной функции. Вес Хэмминга.
34. Свойства преобразование Фурье (Адамара) псевдобулевой функции.
35. Криптографические характеристики булевой функции: алгебраическая степень и нелинейность.
36. Криптографические характеристики булевой функции: нелинейность порядка r и сбалансированность.
37. Криптографическая характеристика булевой функции: отсутствие ненулевой линейной структуры.
38. Многозначные логики. Основные типы: Лукашевича, Геделя, t-норм система, трехзначная, четырех-значная система Данна-Беллнапа, система произведения.
39. Функция k-значной логики. Отношение эквивалентности на множестве функций k-значной логики. Циклический полином. Лемма Бернсайда.
40. Теоремы де Брюина и Полиа для классов функций k-значной логики.
41. Понятие алгоритма и вычислимой функции. Примитивно и частично рекурсивные функции.
42. Тезис Черча. Машина Тьюринга-Поста.
43. Вычисления функций на машине Тьюринга-Поста. Универсальная машина Тьюринга.
44. Теорема об универсальном алгоритме.
45. Эффективные алгоритмы. Алгоритмически неразрешимые проблемы.
46. Сложность алгоритма. Оценки функции сложности.
47. Сложность арифметических операций.
48. Классы задач P и NP. Тезис Колмогорова.

49. Реляционная алгебра, реляционное исчисление, понятие реляционной схемы, его характеристики.

50. Операции реляционной алгебры. Базы данных.

7.1. Основная литература:

Микони, С.В. Дискретная математика для бакалавра: множества, отношения, функции, графы [Электронный ресурс] : учеб. пособие ? Электрон. дан. ? Санкт-Петербург : Лань, 2012. ? 192 с. ? Режим доступа: https://e.lanbook.com/book/4316. ? Загл. с экрана.

Глухов, М.М. Математическая логика. Дискретные функции. Теория алгоритмов [Электронный ресурс] : учеб. пособие / М.М. Глухов, А.Б. Шишков. ? Электрон. дан. ? Санкт-Петербург : Лань, 2012. ? 416 с. ? Режим доступа: https://e.lanbook.com/book/4041. ? Загл. с экрана.

Кожухов, С.Ф. Сборник задач по дискретной математике [Электронный ресурс] : учеб. пособие / С.Ф. Кожухов, П.И. Совертков. ? Электрон. дан. ? Санкт-Петербург : Лань, 2017. ? 324 с. ? Режим доступа: https://e.lanbook.com/book/93769. ? Загл. с экрана.

7.2. Дополнительная литература:

Бабенко, М.А. Введение в теорию алгоритмов и структур данных [Электронный ресурс] / М.А. Бабенко, М.В. Левин. ? Электрон. дан. ? Москва : МЦНМО, 2016. ? 144 с. ? Режим доступа: https://e.lanbook.com/book/80136. ? Загл. с экрана.

Марченков, С.С. Основы теории булевых функций [Электронный ресурс] : учеб. пособие ? Электрон. дан. ? Москва : Физматлит, 2014. ? 136 с. ? Режим доступа: https://e.lanbook.com/book/59714. ? Загл. с экрана.

Шевелев, Ю.П. Сборник задач по дискретной математике (для практических занятий в группах) [Электронный ресурс] : учеб. пособие / Ю.П. Шевелев, Л.А. Писаренко, М.Ю. Шевелев. ? Электрон. дан. ? Санкт-Петербург : Лань, 2013. ? 528 с. ? Режим доступа: https://e.lanbook.com/book/5251. ? Загл. с экрана.

7.3. Интернет-ресурсы:

Андреева Т.Ю., Саушкин М.Н. ?Логические парадоксы? - http://ermine.narod.ru/math/stat/andsau/andsau.htm

Electronic colloquium on computational complexity - http://www.eccc.uni-trier.de/eccc/

архив статей по криптографии - http://eprint.iacr.org/

Математическая логика по всему миру - http://world.logic.at/

Учебно-образовательная физико-математическая библиотека - http://eqworld.ipmnet.ru/ru/library.htm

8. Материально-техническое обеспечение дисциплины(модуля)

Освоение дисциплины "Математическая логика и теория алгоритмов" предполагает использование следующего материально-технического обеспечения:

Мультимедийная аудитория, вместимостью более 60 человек. Мультимедийная аудитория состоит из интегрированных инженерных систем с единой системой управления, оснащенная современными средствами воспроизведения и визуализации любой видео и аудио информации, получения и передачи электронных документов. Типовая комплектация мультимедийной аудитории состоит из: мультимедийного проектора, автоматизированного проекционного экрана, акустической системы, а также интерактивной трибуны преподавателя, включающей тач-скрин монитор с диагональю не менее 22 дюймов, персональный компьютер (с техническими характеристиками не ниже Intel Core i3-2100, DDR3 4096Mb, 500Gb), конференц-микрофон, беспроводной микрофон, блок управления оборудованием, интерфейсы подключения: USB,audio, HDMI. Интерактивная трибуна преподавателя является ключевым элементом управления, объединяющим все устройства в единую систему, и служит полноценным рабочим местом преподавателя. Преподаватель имеет возможность легко управлять всей системой, не отходя от трибуны, что позволяет проводить лекции, практические занятия, презентации, вебинары, конференции и другие виды аудиторной нагрузки обучающихся в удобной и доступной для них форме с применением современных интерактивных средств обучения, в том числе с использованием в процессе обучения всех корпоративных ресурсов. Мультимедийная аудитория также оснащена широкополосным доступом в сеть интернет. Компьютерное оборудованием имеет соответствующее лицензионное программное обеспечение.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен студентам. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, УМК, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего профессионального образования (ФГОС ВПО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань" , доступ к которой предоставлен студентам. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех авторских и смежных прав.

Учебные аудитории для проведения лекционных и практических занятий.

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 10.03.01 "Информационная безопасность" и профилю подготовки Безопасность автоматизированных систем .

Автор(ы):
Патрин Е.В. _____
"__" _____ 201 __ г.

Рецензент(ы):
Аминова А.В. _____
"__" _____ 201 __ г.