

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



УТВЕРЖДАЮ

Проректор по образовательной деятельности КФУ

Проф. Таюрский Д.А.



\_\_\_\_\_ 20\_\_ г.

*подписано электронно-цифровой подписью*

### Программа дисциплины

Математическая логика и теория алгоритмов Б2.В.2

Направление подготовки: 090900.62 - Информационная безопасность

Профиль подготовки: Информационная безопасность автоматизированных систем

Квалификация выпускника: бакалавр

Форма обучения: очное

Язык обучения: русский

**Автор(ы):**

Иваньшин П.Н.

**Рецензент(ы):**

Егорова А.И.

### **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 698217

Казань  
2017

## Содержание

1. Цели освоения дисциплины
2. Место дисциплины в структуре основной образовательной программы
3. Компетенции обучающегося, формируемые в результате освоения дисциплины /модуля
4. Структура и содержание дисциплины/ модуля
5. Образовательные технологии, включая интерактивные формы обучения
6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов
7. Литература
8. Интернет-ресурсы
9. Материально-техническое обеспечение дисциплины/модуля согласно утвержденному учебному плану

Программу дисциплины разработал(а)(и) доцент, к.н. (доцент) Иваньшин П.Н. Кафедра геометрии отделение математики , Pyotr.Ivanshin@kpfu.ru

### 1. Цели освоения дисциплины

Студенты, завершившие изучение данной дисциплины должны:

знать основные положения математической логики и теории алгоритмов;

овладеть методами решения соответствующих задач;

уметь использовать эти методы при работе с конкретными приложениями, программами и базами данных.

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

Данная учебная дисциплина включена в раздел " Б2.В.2 Общепрофессиональный" основной образовательной программы 090900.62 Информационная безопасность и относится к вариативной части. Осваивается на 3 курсе, 6 семестр.

Для усвоения дисциплины необходимо усвоить дисциплины Алгебра и теория графов --- первая часть дисциплины Дискретная Математика

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

В результате освоения дисциплины формируются следующие компетенции:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОК-11 (общекультурные компетенции)	фундаментальная подготовка по основам профессиональных знаний и готовность к использованию их в профессиональной деятельности
ОК-12 (общекультурные компетенции)	навыки работы с компьютером
ОК-8 (общекультурные компетенции)	способность приобретать новые знания, используя современные образовательные и информационные технологии
ОК-9 (общекультурные компетенции)	способность понимать сущность и значение информации в развитии современного общества, соблюдение основных требований информационной безопасности, в том числе защиты государственных интересов и приоритетов
ПК-1 (профессиональные компетенции)	определение общих форм, закономерностей и инструментальных средств отдельной предметной области
ПК-17 (профессиональные компетенции)	умение извлекать полезную научно-техническую информацию из электронных библиотек, реферативных журналов, сети Интернет
ПК-2 (профессиональные компетенции)	умение понять поставленную задачу

В результате освоения дисциплины студент:

1. должен знать:

знать основные положения математической логики и теории алгоритмов;

2. должен уметь:

уметь использовать эти методы при работе с конкретными приложениями, программами и базами данных.

3. должен владеть:

овладеть методами решения соответствующих задач;

4. должен демонстрировать способность и готовность:

знать основные положения математической логики и теории алгоритмов;

овладеть методами решения соответствующих задач;

уметь использовать эти методы 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 зачет в 6 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	Практические занятия	Лабораторные работы	
1.	Тема 1. Элементы теории множеств.	6	1	2	2	0	Устный опрос
2.	Тема 2. Исчисление высказываний (ИВ)	6	2	2	2	0	Устный опрос
3.	Тема 3. Эквивалентность формул.	6	3	2	2	0	Устный опрос
4.	Тема 4. Непротиворечивость ИВ	6	4	2	2	0	Контрольная работа
5.	Тема 5. Исчисление предикатов (ИП).	6	5	2	2	0	Устный опрос
6.	Тема 6. Общезначимость в ИП.	6	6	2	2	0	Устный опрос

N	Раздел Дисциплины/ Модуля	Семестр	Неделя семестра	Виды и часы аудиторной работы, их трудоемкость (в часах)			Текущие формы контроля
				Лекции	Практические занятия	Лабораторные работы	
7.	Тема 7. Утверждения о полноте и непротиворечивости ИП.	6	7	2	2	0	Устный опрос
8.	Тема 8. Булевы и псевдобулевы функции.	6	8	2	6	0	Устный опрос
9.	Тема 9. Преобразование Фурье	6	9	2	4	0	Устный опрос
10.	Тема 10. Криптографические свойства булевых функций.	6	10,11	4	4	0	Контрольная работа
11.	Тема 11. Многозначные логики.	6	12,13	2	0	0	
12.	Тема 12. Функция k-значной логики.	6	14	4	0	0	
13.	Тема 13. Понятие алгоритма	6	15,16	4	4	0	Устный опрос
14.	Тема 14. Сложность алгоритма.	6	17	2	4	0	Контрольная работа
15.	Тема 15. Реляционная алгебра	6	18	2	0	0	
	Итого			36	36	0	

## 4.2 Содержание дисциплины

### Тема 1. Элементы теории множеств.

#### **лекционное занятие (2 часа(ов)):**

Элементы теории множеств. Понятия: алфавит, буква, слово, исчисление, аксиома, теорема. Операции теории множеств: пересечение, объединение, свойства операций.

#### **практическое занятие (2 часа(ов)):**

Практика: Игошин В. Задачи и упражнения по математической логике, 2007, стр. 6-15, задачи 1-10

### Тема 2. Исчисление высказываний (ИВ)

#### **лекционное занятие (2 часа(ов)):**

Исчисление высказываний (ИВ). Понятия: алфавит ИВ, формула ИВ, терм. Правила вывода. Теорема о дедукции.

#### **практическое занятие (2 часа(ов)):**

Практика: Игошин В. Задачи и упражнения по математической логике, 2007, стр. 15-33, задачи 21-36

### Тема 3. Эквивалентность формул.

#### **лекционное занятие (2 часа(ов)):**

Эквивалентность формул. Основные эквивалентные формулы. Цепи эквивалентностей. Таблицы истинности.

#### **практическое занятие (2 часа(ов)):**

Практика: Игошин В. Задачи и упражнения по математической логике, 2007, стр. 39-40, задачи 41-49

#### **Тема 4. Непротиворечивость ИВ**

##### **лекционное занятие (2 часа(ов)):**

Непротиворечивость ИВ, правила введения и удаления, полнота. Главная интерпретация ИВ (на множестве  $\{0, 1\}$ ). Независимость ИВ.

##### **практическое занятие (2 часа(ов)):**

Практика: Игошин В. Задачи и упражнения по математической логике, 2007, стр. 15-33, задачи 70-71

#### **Тема 5. Исчисление предикатов (ИП).**

##### **лекционное занятие (2 часа(ов)):**

Исчисление предикатов (ИП). Понятия: предикат,  $n$ -местное отношение (его свойства), функция как двуместное отношение, квантор. ИВ как часть ИП.

##### **практическое занятие (2 часа(ов)):**

Практика: Игошин В. Задачи и упражнения по математической логике, 2007, стр. 162-188, задачи 1-36

#### **Тема 6. Общезначимость в ИП.**

##### **лекционное занятие (2 часа(ов)):**

Общезначимость в ИП. Теорема о дедукции в ИП. Непротиворечивость и правила вывода теории доказательств ИП.

##### **практическое занятие (2 часа(ов)):**

Практика: Игошин В. Задачи и упражнения по математической логике, 2007, стр. 213-221, задачи 1-20

#### **Тема 7. Утверждения о полноте и непротиворечивости ИП.**

##### **лекционное занятие (2 часа(ов)):**

Утверждения о полноте и непротиворечивости ИП. Теоремы Линденбаума и Геделя.

##### **практическое занятие (2 часа(ов)):**

Практика: Игошин В. Задачи и упражнения по математической логике, 2007, стр. 204-213, задачи 1-18

#### **Тема 8. Булевы и псевдобулевы функции.**

##### **лекционное занятие (2 часа(ов)):**

Булевы и псевдобулевы функции. Представление булевой функции в виде полинома. Степень представления. Псевдобулевы функции. Определение, представление в виде полиномов и позиформ (минимизация булевой функции). Пример: алгоритмическая теория графов.

##### **практическое занятие (6 часа(ов)):**

Практика: Игошин В. Задачи и упражнения по математической логике, 2007, стр. 15-33, задачи 21-36

#### **Тема 9. Преобразование Фурье**

##### **лекционное занятие (2 часа(ов)):**

Преобразование Фурье булевой и псевдобулевой функции. Вес Хэмминга булевой функции. Свойства дискретного преобразования Фурье.

##### **практическое занятие (4 часа(ов)):**

Практика: Игошин В. Задачи и упражнения по математической логике, 2007, стр. 92-101, задачи 1-26

#### **Тема 10. Криптографические свойства булевых функций.**

##### **лекционное занятие (4 часа(ов)):**

Криптографические свойства булевых функций. Аффинная эквивалентность, алгебраическая степень, нелинейность, сбалансированность и  $k$ -резилентность. Линейные ядро и структура.

##### **практическое занятие (4 часа(ов)):**

Практика: Игошин В. Задачи и упражнения по математической логике, 2007, стр. 101-123, задачи 1-17

### **Тема 11. Многозначные логики.**

#### **лекционное занятие (2 часа(ов)):**

Многозначные логики. Основные типы: Лукашевича, Геделя, t-норм система, трехзначная, четырехзначная система Данна-Беллпапа, система произведения.

### **Тема 12. Функция k-значной логики.**

#### **лекционное занятие (4 часа(ов)):**

Функция k-значной логики. Отношение эквивалентности на множестве функций k-значной логики. Циклический полином. Лемма Бернсайда. Теоремы де Брюина и Поля.

### **Тема 13. Понятие алгоритма**

#### **лекционное занятие (4 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. Эффективные алгоритмы.

#### **практическое занятие (4 часа(ов)):**

Практика: Игошин В. Задачи и упражнения по математической логике, 2007, стр. 221-240, задачи 1-34

### **Тема 14. Сложность алгоритма.**

#### **лекционное занятие (2 часа(ов)):**

Сложность алгоритма. Оценки функции сложности. Пример: сложность арифметических операций. Классы задач P и NP. Тезис Колмогорова.

#### **практическое занятие (4 часа(ов)):**

Практика: Игошин В. Задачи и упражнения по математической логике, 2007, стр. 240-248, задачи 1-16

### **Тема 15. Реляционная алгебра**

#### **лекционное занятие (2 часа(ов)):**

Реляционная алгебра, реляционное исчисление, понятие реляционной схемы, его характеристики. Операции реляционной алгебры. Базы данных.

## **4.3 Структура и содержание самостоятельной работы дисциплины (модуля)**

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
1.	Тема 1. Элементы теории множеств.	6	1	подготовка к устному опросу	6	устный опрос
2.	Тема 2. Исчисление высказываний (ИВ)	6	2	подготовка к устному опросу	6	устный опрос
3.	Тема 3. Эквивалентность формул.	6	3	подготовка к устному опросу	6	устный опрос
4.	Тема 4. Непротиворечивость ИВ	6	4	подготовка к контрольной работе	6	контрольная работа
5.	Тема 5. Исчисление предикатов (ИП).	6	5	подготовка к устному опросу	6	устный опрос
6.	Тема 6. Общезначимость в ИП.	6	6	подготовка к устному опросу	6	устный опрос

N	Раздел Дисциплины	Семестр	Неделя семестра	Виды самостоятельной работы студентов	Трудоемкость (в часах)	Формы контроля самостоятельной работы
7.	Тема 7. Утверждения о полноте и непротиворечивости ИП.	6	7	подготовка к устному опросу	6	устный опрос
8.	Тема 8. Булевы и псевдобулевы функции.	6	8	подготовка к устному опросу	6	устный опрос
9.	Тема 9. Преобразование Фурье	6	9	подготовка к устному опросу	6	устный опрос
10.	Тема 10. Криптографические свойства булевых функций.	6	10,11	подготовка к контрольной работе	6	контрольная работа
13.	Тема 13. Понятие алгоритма	6	15,16	подготовка к устному опросу	6	устный опрос
14.	Тема 14. Сложность алгоритма.	6	17	подготовка к контрольной работе	6	контрольная работа
	Итого				72	

## 5. Образовательные технологии, включая интерактивные формы обучения

проектор, ноутбук, мультимедийная аудитория

## 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.

устный опрос , примерные вопросы:

найти пересечение, объединение множеств, доказать закон де Моргана

### Тема 2. Исчисление высказываний (ИВ)

устный опрос , примерные вопросы:

построить таблицу истинности

### Тема 3. Эквивалентность формул.

устный опрос , примерные вопросы:

найти КНФ, ДНФ формулы

### Тема 4. Непротиворечивость ИВ

контрольная работа , примерные вопросы:

Построить полином Жегалкина, найти КНФ, ДНФ

### Тема 5. Исчисление предикатов (ИП).

устный опрос , примерные вопросы:

Найти множество истинности предиката

### Тема 6. Общезначимость в ИП.

устный опрос , примерные вопросы:

проверить предикат на общезначимость

### Тема 7. Утверждения о полноте и непротиворечивости ИП.



устный опрос , примерные вопросы:

найти для предиката предваренную НФ

### **Тема 8. Булевы и псевдобулевы функции.**

устный опрос , примерные вопросы:

построить базис данной системы булевых функций

### **Тема 9. Преобразование Фурье**

устный опрос , примерные вопросы:

найти дискретное преобразование Фурье от данной бф

### **Тема 10. Криптографические свойства булевых функций.**

контрольная работа , примерные вопросы:

найти код по матрице

### **Тема 11. Многозначные логики.**

### **Тема 12. Функция k-значной логики.**

### **Тема 13. Понятие алгоритма**

устный опрос , примерные вопросы:

построить машину Тьюринга

### **Тема 14. Сложность алгоритма.**

контрольная работа , примерные вопросы:

определить примитивно рекурсивна ли функция

### **Тема 15. Реляционная алгебра**

Примерные вопросы к зачету:

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  $((A \rightarrow B) \vee (B \rightarrow C)) \wedge (A \vee B)$

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  $((A \vee B) \rightarrow (B \wedge C)) \rightarrow (A \rightarrow B)$

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  $((A \rightarrow B) \vee (B \rightarrow C)) \wedge (A \vee (B \rightarrow C))$

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  $((A \wedge B) \rightarrow (B \vee C)) \rightarrow (A \cdot B)$

\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  $((A \rightarrow B) + (B \rightarrow C)) \wedge (C|B')$

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  $((A \vee B) \rightarrow (B \wedge C)) \rightarrow (A \rightarrow B)$

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?

$$f(x, y) = r(x, y) + 4 \lfloor y/x \rfloor$$

2. Найти функцию, определенную с помощью оператора минимизации.

$$f(x, y) = \mu z (z - x^2 + x^3 = y^2).$$

### 7.1. Основная литература:

А.К. Гуц, Математическая логика и теория алгоритмов, Омск, 2003.

А.А. Марков, Н.М. Нагорный, Теория алгоритмов, Москва, Наука, 1984.

С.К. Клини, Математическая логика, Москва, Мир, 1973.

А.В. Черемушкин, Лекции по арифметическим алгоритмам в криптографии, Москва, МЦНМО, 2002.

Н. Коблиц, Курс теории чисел и криптографии, Москва, ТВП, 2001.

Игошин В. Задачи и упражнения по математической логике, 2007

Игошин В. Математическая логика, 2007,

### 7.2. Дополнительная литература:

1. E. Boros, P.L. Hammer, Pseudo-Boolean optimisation, survey, 2001.

2. Y. Crama, P.L. Hammer, Boolean functions. Theory, algorithms and applications, first draft, 2006.

3. C. Carlet, Boolean Functions for Cryptography and Error Correcting Codes, To appear soon as a chapter of the volume "Boolean Methods and Models", published by Cambridge University Press, Eds Yves Crama and Peter Hammer.

### 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/>

Криптографический ликбез - <http://www.ssl.stu.neva.ru/psw/crypto.html>

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

## 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 оборудование имеет соответствующее лицензионное программное обеспечение.

ноутбук, проектор

Программа составлена в соответствии с требованиями ФГОС ВПО и учебным планом по направлению 090900.62 "Информационная безопасность" и профилю подготовки Информационная безопасность автоматизированных систем .

Автор(ы):

Иваньшин П.Н. \_\_\_\_\_

"\_\_" \_\_\_\_\_ 201\_\_ г.

Рецензент(ы):

Егорова А.И. \_\_\_\_\_

"\_\_" \_\_\_\_\_ 201\_\_ г.