

МИНОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ  
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ  
Директор института прикладной  
прикладной  
математики и компьютерных наук  
А.В. Замятин  
« 02 » \_\_\_\_\_ 2021 г.



**Фонд оценочных средств по дисциплине**

Дискретная математика

Специальность

**10.05.01 Компьютерная безопасность**

*код и наименование специальности*

**Анализ безопасности компьютерных систем**

*наименование специализации*

ФОС составил(и):  
старший преподаватель



Е.В. Широкова

Рецензент:  
канд. техн. наук, доцент,  
зав. кафедрой компьютерной безопасности



С.А. Останин

Фонд оценочных средств одобрен на заседании учебно-методической комиссии  
института прикладной математики и компьютерных наук (УМК ИПМКН)

Протокол от 17 июня 2021 г. № 05

Председатель УМК ИПМКН,  
д-р техн. наук, профессор



С.П. Сущенко

**Фонд оценочных средств (ФОС)** является элементом системы оценивания сформированности компетенций у обучающихся в целом или на определенном этапе ее формирования.

ФОС разрабатывается в соответствии с рабочей программой (РП) дисциплины и включает в себя набор оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине.

### 1. Компетенции и результаты обучения, формируемые в результате освоения дисциплины

Компетенция	Индикатор компетенции	Код и наименование результатов обучения (планируемые результаты обучения, характеризующие этапы формирования компетенций)	Критерии оценивания результатов обучения			
			Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
ОПК-3. Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности	ИОПК-3.1 Демонстрирует навыки выполнения стандартных действий, решения типовых задач, формулируемых в рамках базовых математических дисциплин; ИОПК-3.2 Осуществляет применение основных понятий, фактов, концепций, принципов математики и информатики для решения задач профессиональной деятельности; ИОПК-3.3 Выявляет научную сущность проблем, возникающих в ходе профессиональной деятельности, и применяет	ОР-3.1.1 Обучающийся будет знать основные понятия и теоремы булевых функций и функций $k$ -значной логики. ОР-3.1.2 Обучающийся будет знать проблемы минимизации и функциональной полноты булевых функций. ОР-3.2.1 Обучающийся будет уметь применять алгоритмы и теоремы булевых и $k$ -значных функций в задачах защиты информации. ОР-3.3.1 Обучающийся будет владеть аппаратом функций булевых и $k$ -значной логики для задания структуры и поведения дискретных (цифровых) устройств, в частности, устройств шифрования.	Уверенно владеет основными понятиями и теоремами булевых функций и функций $k$ -значной логики. Уверенно знает проблемы минимизации и функциональной полноты булевых функций. Умеет эффективно применять алгоритмы и теоремы булевых и $k$ -значных функций в	Знает основные понятия и теоремы булевых функций и функций $k$ -значной логики. Знает проблемы минимизации и функциональной полноты булевых функций. Умеет применять алгоритмы и теоремы булевых и $k$ -значных функций в задачах защиты информации. Владеет аппаратом функций булевых	Поверхностно знает основные понятия и теоремы булевых функций и функций $k$ -значной логики. Поверхностно знает проблемы минимизации и функциональной полноты булевых функций. Неуверенно умеет применять алгоритмы и теоремы булевых и $k$ -	Не знает основные понятия и теоремы булевых функций и функций $k$ -значной логики. Не знает проблемы минимизации и функциональной полноты булевых функций. Не умеет применять алгоритмы и теоремы булевых и $k$ -значных функций в задачах защиты информации. Не владеет аппаратом функций булевых и $k$ -значной логики для

	<p>соответствующий математический аппарат для их формализации, анализа и выработки решения.</p>		<p>задачах защиты информации. Уверенно владеет аппаратом функций булевых и k-значной логики для задания структуры и поведения дискретных (цифровых) устройств, в частности, устройств шифрования.</p>	<p>и k-значной логики для задания структуры и поведения дискретных (цифровых) устройств, в частности, устройств шифрования.</p>	<p>значных функций в задачах защиты информации. Неуверенно владеет аппаратом функций булевых и k-значной логики для задания структуры и поведения дискретных (цифровых) устройств, в частности, устройств шифрования.</p>	<p>задания структуры и поведения дискретных (цифровых) устройств, в частности, устройств шифрования.</p>
--	---	--	---	---	---	--

## 2. Этапы формирования компетенций и виды оценочных средств

№	Этапы формирования компетенций (разделы дисциплины)	Код и наименование результатов обучения	Вид оценочного средства (тесты, задания, кейсы, вопросы и др.)
1.	Основные понятия теории булевых функций	ОР-3.1.1, ОР-3.2.1, ОР-3.3.1	Задания, задачи
2.	Нормальные формы булевых функций	ОР-3.1.1, ОР-3.2.1, ОР-3.3.1	Задания, задачи
3.	Минимизация булевых функций	ОР-3.1.2, ОР-3.2.1, ОР-3.3.1	Задания, задачи
4.	Частичные булевы функции	ОР-3.1.1, ОР-3.1.2, ОР-3.2.1, ОР-3.3.1	Задания, задачи
5.	Важнейшие замкнутые классы и функциональная полнота	ОР-3.1.1, ОР-3.2.1, ОР-3.3.1	Задания, задачи
6.	Функции k-значной логики	ОР-3.1.1, ОР-3.2.1, ОР-3.3.1	Задания, задачи

## 3. Типовые контрольные задания или иные материалы, необходимые для оценки образовательных результатов обучения

3.1. Типовые задания для проведения текущего контроля успеваемости по дисциплине.

Текущая аттестация по дисциплине «Дискретная математика» осуществляется в форме оценивания результатов выполнения контрольных работ. Контрольные работы выполняются по следующим темам:

1. Булевы функции, булевы переменные, двойственные функции и двойственные формулы
2. Дизъюнктивные нормальные формы
3. Минимизация булевых функций
4. Полиномы Жегалкина, замкнутые классы, функциональная полнота систем булевых функций

### Примеры контрольных заданий.

1. Булевы функции, булевы переменные, двойственные функции и двойственные формулы.

1) Для функции  $f$ , заданной формулой  $F = x \rightarrow y \rightarrow (z \oplus \bar{x})y$  :

определить порядок операций в формуле;

построить таблицу значений;

найти двойственную функцию по таблице значений;

найти двойственную функцию по определению двойственной функции;

найти двойственную функцию согласно принципу двойственности;

найти и удалить фиктивные переменные.

2. Дизъюнктивные нормальные формы

1) Для функции  $f$ , заданной формулой  $F = x \rightarrow y \rightarrow (z \oplus \bar{x})y$ , построить ДНФ<sub>1</sub> с помощью подстановки кратчайших ДНФ элементарных булевых функций и ДНФ<sub>2</sub>

с помощью разложения Шеннона по переменным. Сравнить результаты, построив таблицы значений для  $F$ ,  $ДНФ_1$  и  $ДНФ_2$ .

2) Для функции  $f$ , заданной формулой  $F = x \rightarrow y \rightarrow (z \oplus \bar{x})y$ , найти совершенную ДНФ и совершенную КНФ с помощью таблицы значений.

3) Для функции  $f$ , заданной формулой  $F = x \rightarrow y \rightarrow (z \oplus \bar{x})y$ :  
построить таблицу значений;

задать функцию на матрице Грея;

найти сокращенную ДНФ по матрице Грея;

преобразовать сокращенную ДНФ в совершенную ДНФ;

найти кратчайшую ДНФ по матрице Грея;

построить для найденной кратчайшей ДНФ таблицу значений и сравнить ее с таблицей значений функции  $f$ .

### 3. Минимизация булевых функций

1) Для функции  $f$ , заданной формулой  $F = x \rightarrow y \rightarrow (z \oplus \bar{x})y$ :  
найти совершенную ДНФ;

найти сокращенную ДНФ по совершенной ДНФ методом Квайна – МакКласки;

найти сокращенную ДИФ по исходной формуле  $E$  методом Блейка – Порецкого;

построить таблицу Квайна;

найти кратчайшую ДНФ по таблице Квайна.

2) Для функции  $f$ , заданной формулой  $F = x \rightarrow y \rightarrow (z \oplus \bar{x})y$  найти приближенную кратчайшую ДНФ методом Закревского

3) Для не полностью определенной функции  $f$ , заданной на матрице Грея, найти приближенную кратчайшую ДНФ методом конкурирующих интервалов.

### 4. Полиномы Жегалкина, замкнутые классы, функциональная полнота систем булевых функций

1) Для функции  $f$ , заданной вектором значений 01100111:

построить таблицу значений;

найти совершенную ДНФ;

найти полином Жегалкина по совершенной ДНФ;

найти полином Жегалкина по таблице значений функции / методом неопределенных коэффициентов.

2) Для функции  $f$ , заданной формулой  $F = x \rightarrow y \rightarrow (z \oplus \bar{x})y$ :

найти полином Жегалкина, используя разложение Дэвио по переменным;

найти полином Жегалкина, используя полиномы элементарных булевых функций;

определить принадлежность функции  $f$  замкнутым классам  $T^0$ ,  $T^1$ ,  $L$ ,  $M$ ,  $S$  используя соответствующие алгоритмы;

определить является ли множество  $M = \{f\}$  функционально полной системой.

### 3.2. Типовые задания для проведения промежуточной аттестации по дисциплине (вопросы к экзамену):

#### Раздел 1. Основные понятия теории булевых функций

1. Определения: булевы константы, булев вектор. Примеры.

2. Доказательство теоремы о числе булевых векторов.

3. Представление множества булевыми векторами. Примеры.
4. Представление чисел булевыми векторами. Примеры.
5. Расстояние между векторами. Примеры.
6. Соседние, противоположные, сравнимые булевы векторы. Примеры.
7. Определение булева пространства.
8. Способы задания булева пространства.
9. Определение интервала. Внутренние и внешние компоненты интервала.
10. Доказательство теоремы о мощности интервала.
11. Алгоритм распознавания интервала и поиска его границ. Примеры.
12. Способы задания интервала. Примеры.
13. Алгоритм распознавания интервала на матрице Грея. Примеры.
14. Определение соседних интервалов. Примеры.
15. Доказательство теоремы о пересечении и объединении соседних интервалов.
16. Определение булевых переменных и булевой функции.
17. Способы задания булевых функций. Примеры.
18. Доказательство теоремы о числе булевых функций.
19. Фиктивные переменные. Алгоритм распознавания фиктивных переменных по таблице значений булевой функции. Достаточное условие отсутствия фиктивных переменных.
20. Фиктивные переменные. Алгоритм распознавания фиктивных переменных булевой функции, заданной на матрице Грея.
21. Алгоритм добавления фиктивных переменных. Алгоритм удаления фиктивных переменных. Примеры.
22. Формула как способ задания булевых функций. Примеры.
23. Определение равносильных формул. Основные равносильности.
24. Определение двойственной функции. Алгоритм построения таблицы значений двойственной функции.
25. Способы построения двойственной булевой функции. Примеры.
26. Доказательство свойств двойственной функции.
27. Определение двойственной формулы. Примеры.
28. Доказательство принципа двойственности.

## Раздел 2. Нормальные формы булевых функций

1. Разложение Шеннона по одной переменной. Примеры.
2. Разложение Шеннона по  $A$  переменным. Примеры.
3. Определение совершенной ДНФ. Теорема о единственности совершенной ДНФ булевой функции.
4. Алгоритм построения совершенной ДНФ по таблице значений булевой функции.
5. Определение совершенной КНФ. Теорема о единственности совершенной КНФ булевой функции. Построение совершенной КНФ из совершенной ДНФ.
6. Определения элементарной, полной, ортогональной, соседней и смежной конъюнкций. Примеры.
7. Определения ДНФ, длина и ранг ДНФ. Примеры.
8. Алгоритм преобразования ДНФ в совершенную ДНФ. Примеры.
9. Доказательство теоремы о конъюнкции и интервале.

10. Определения импликанты, простой импликанты, сокращенной ДНФ.  
Примеры.
11. Определения импликанты, простой импликанты, сокращенной ДНФ.  
Примеры.
12. Доказательство леммы об импликанте.
13. Определения кратчайшей и минимальной ДНФ. Примеры.
14. Доказательство теоремы о минимальной ДНФ.
15. Доказательство теоремы о кратчайшей ДНФ.
16. Определение безызбыточной ДНФ. Примеры.
17. Кратчайшие ДНФ элементарных булевых функций. Примеры.

### Раздел 3. Минимизация булевых функций

1. Доказательство теоремы Квайна.
2. Алгоритм Квайна - МакКласки. Примеры.
3. Доказательство теоремы Блейка.
4. Алгоритм Блейка - Порецкого. Примеры.
5. Проблема минимизации булевых функций.
6. Таблица Квайна. Покрытия таблицы Квайна. Примеры.
7. Алгоритм поиска всех безызбыточных покрытий таблицы Квайна. Примеры.
8. Алгоритм поиска одного кратчайшего покрытия таблицы Квайна. Примеры.
9. Алгоритм поиска приближенной кратчайшей ДНФ методом Закревского. Примеры.

### Раздел 4. Частичные булевы функции

1. Определение не полностью определенной булевой функции. Способы задания не полностью определенных булевых функций. Примеры.
2. Доопределение не полностью определенной булевой функции. Доказательство теоремы о числе доопределений не полностью определенной булевой функции.
3. Проблема минимизации не полностью определенных булевых функций.
4. Алгоритм поиска одной кратчайшей ДНФ не полностью определенной булевой функции. Примеры.
5. Алгоритм поиска приближенной кратчайшей ДНФ не полностью определенной булевой функции методом Закревского. Примеры.
6. Алгоритм поиска приближенной кратчайшей ДНФ не полностью определенной булевой функции методом конкурирующих интервалов. Примеры.
7. Способы задания булевых и не полностью определенных систем булевых функций.  
Примеры.
8. Проблема минимизации не полностью систем булевых функций. Определения кратчайшей минимальной и безызбыточной ДНФ системы булевых функций. Примеры.
9. Алгоритм поиска одной кратчайшей ДНФ системы булевых функций с общей областью определения. Примеры.

### Раздел 5. Важнейшие замкнутые классы и функциональная полнота

1. Определение замкнутого класса булевых функций. Определение класса  $T^0$  булевых функций, сохраняющих константу 0. Доказательство замкнутости класса  $T^0$ . Доказательство теоремы о мощности класса  $T^0$ .



2. Определение замкнутого класса булевых функций. Определение класса  $T^1$  булевых функций, сохраняющих константу 1. Доказательство замкнутости класса  $T^1$ . Доказательство теоремы о мощности класса  $T^0$ .

3. Доказательство теоремы о булевой функции, не сохраняющей константу 0.

4. Определение класса  $L$ , линейных булевых функций. Доказательство замкнутости класса  $L$ . Доказательство теоремы о мощности класса  $L$ .

5. Доказательство теоремы о нелинейной булевой функции.

6. Определение класса  $S$  самодвойственных булевых функций. Доказательство замкнутости класса  $S$ . Доказательство теоремы о мощности класса  $S$ . Алгоритм определения самодвойственности булевой функции. Достаточное условие несамодвойственности булевой функции.

7. Доказательство теоремы о несамодвойственной булевой функции.

8. Определение класса  $M$  монотонных булевых функций. Доказательство замкнутости класса  $M$ . Доказательство теоремы об условии немонотонности. Алгоритм определения монотонности булевой функции.

9. Доказательство теоремы о немонотонной булевой функции.

10. Определение положительной конъюнкции. Доказательство леммы о числе положительных конъюнкций. Номер положительной конъюнкции. Представление полинома Жегалкина в форме с коэффициентами. Примеры.

11. Определение полинома Жегалкина, длина и ранг полинома. Примеры.

12. Доказательство теоремы о возможности представления булевой функции полиномом Жегалкина.

13. Доказательство теоремы о единственности представления булевой функции полиномом Жегалкина.

14. Алгоритмы построения полиномов Жегалкина. Примеры.

15. Проблема функциональной полноты систем булевых функций. Примеры.

16. Доказательство теоремы о двух функционально полных системах.

17. Принадлежность замкнутым классам элементарных булевых функций.

Примеры.

18. Доказательство теоремы Поста - Яблонского о функциональной полноте.

## Раздел 6. Функции $k$ -значной логики

1. Элементарные функции  $k$ -значной логики. Свойства.

2. Совершенные формы. Теоремы о 1-й и 2-й совершенных формах

3. Полиномы по  $\text{mod } k$ . Теорема о задании функций  $k$ -значных логик полиномами.

4. Малая теорема Ферма.

5. Построение полиномов методом неопределенных коэффициентов

6. Построение полиномов быстрым методом

7. Доказательство полноты системы Поста

8. Свойства функций в  $P_k$ , существенно зависящих не менее, чем от двух аргументов

9. Доказательство критерия полноты С.В.Яблонского

#### **4. Методические материалы, определяющие процедуры оценивания образовательных результатов обучения**

4.1. Методические материалы для оценки текущего контроля успеваемости по дисциплине.

Текущий контроль осуществляется при помощи выполнения контрольных заданий обучающимися. Для успешного прохождения текущего контроля необходимо выполнить все контрольные задания. Проверка заданий осуществляется демонстрацией решённых задач и выполненных практических заданий с комментариями обучающихся.

4.2. Методические материалы для проведения промежуточной аттестации по дисциплине.

Промежуточная аттестация по дисциплине проводится в форме устного экзамена по теоретическому материалу. К промежуточной аттестации допускаются только студенты, успешно прошедшие текущие аттестации по практическим занятиям.

Каждый билет для промежуточной аттестации состоит из трех теоретических вопросов по темам из разных разделов дисциплины. В качестве дополнительных вопросов во время проведения промежуточной аттестации используются контрольные вопросы, предлагаемые для самостоятельной работы обучающегося.

Оценки при проведении экзамена формируются в соответствии с нижеприведенной таблицей.

Неудовлетворительно	Удовлетворительно	Хорошо	Отлично
Не ответил ни на один из основных вопросов.	Ответил на два из основных вопросов и на один - два из трех дополнительных вопросов.	Ответил на все вопросы, содержащиеся в экзаменационном билете, и на дополнительные вопросы, но с замечаниями.	Уверенно и правильно ответил на все основные и дополнительные вопросы.