Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДАЮ:
Директор
_____А. В. Замятин
« 16 » _____ 2023 г.

Рабочая программа дисциплины

Математическая логика и теория алгоритмов

по направлению подготовки / специальности

10.05.01 Компьютерная безопасность

Направленность (профиль) подготовки / специализация:
Анализ безопасности компьютерных систем

Форма обучения
Очная

Квалификация
Специалист по защите информации

Год приема
2023

Код дисциплины в учебном плане: Б1.О.02.02

СОГЛАСОВАНО:
Руководитель ОП
_____В.Н. Тренькаев

Председатель УМК
_____С.П. Сущенко

Томск – 2023

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

– ОПК-3 – Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

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 соответствующий математический аппарат для их формализации, анализа и выработки решения.

2. Задачи освоения дисциплины

– освоить основные понятия математической логики
– научиться анализировать математические доказательства средствами математической логики
– овладеть основными теоретическими положениями логики высказываний, логики предикатов, теории алгоритмов.

3. Место дисциплины в структуре образовательной программы

Дисциплина относится к обязательной части образовательной программы. Дисциплина входит в модуль «Математика».

4. Семестр(ы) освоения и форма(ы) промежуточной аттестации по дисциплине

Четвертый семестр, зачет с оценкой

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: «Введение в математику», «Дискретная математика».

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 3 з.е., 108 часов, из которых:
-лекции: 32 ч.
-практические занятия: 32 ч.
Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Логика высказываний
Формулы логики нулевого порядка. Эквивалентные преобразования. РКС.
КНФ, ДНФ, СКНФ, СДНФ
Логическое следование
Метод резолюций
Тема 2. Исчисление высказываний
Дедуктика Клини. Выводимость.

Свойства выводимости.
Тема 3.Логика предикатов. Исчисление предикатов.
Предикаты
Язык логики первого порядка. Термы, формулы. Выполнимость, опровержимость, общезначимость.
Эквивалентные преобразования.
Общезначимость.
Логическое следование.
Метод резолюций.
Аксиоматические системы. Исчисление предикатов.
Тема 4. Выразимость. Элиминация кванторов.
Тема 5. Рекурсивные функции.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем контроля посещаемости, проведения контрольных работ, двух зачетов по лекционному материалу, самостоятельных работ по темам, выполнения домашних и индивидуальных заданий, и фиксируется в форме контрольной точки не менее одного раза в семестр.

За практику Часть 1 (Тема 1,2) ставится оценка в зависимости от набранных баллов (ДЗ, СР, ответы у доски). Общее ДЗ (1 балл) ИДЗ (1 балл за задачу) СР на занятии (1 балл за задачу) Ответ у доски (1 балл)	44%-58% - оценка 3, 59%-75% - оценка 4, 76%-100% - оценка 5. Например, при максимуме 36 баллов, 16-21 балл - оценка 3, 22-27 баллов - оценка 4, 28-36 баллов оценка 5
Теоретическая Часть 1. 1 (Тема 1,2) В середине семестра	Оценивается по 5 бальной системе в зависимости от полноты ответа на вопросы билета
За практику Часть 2 (Темы 3 ,4) ставится оценка в зависимости от набранных баллов баллов (ДЗ, СР, ответы у доски, КР). Общее ДЗ (1 балл) ИДЗ (1 балл за задачу) СР на занятии (1 балл за задачу) Ответ у доски (1 балл) КР - 16 баллов	44%-58% - оценка 3, 59%-75% - оценка 4, 76%-100% - оценка 5.
Теоретическая Часть 2. (Темы 3 ,4) В конце семестра	Оценивается по 5 бальной системе в зависимости от полноты ответа на вопросы билета

10. Порядок проведения и критерии оценивания промежуточной аттестации

Зачет с оценкой в четвертом семестре проводится по следующей схеме: итоговая оценка выставляется как среднее арифметическое всех оценок за практику и теорию. При спорной оценке задаётся дополнительный вопрос.

Обе теоретические части сдаются в устной форме, с предварительной письменной подготовкой по билетам. Билет теоретической части содержит два вопроса (часть1) и четыре вопроса (часть 2). Продолжительность зачета 1,5 часа.

Результаты зачета с оценкой определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Примерный состав билетов по теории. Часть 1.

1	Дать определения: язык нулевого порядка, формула логики высказываний, ранг формулы. Сформулировать законы алгебры логики высказываний, доказать з-ны де Моргана. Дать определение СДНФ, СКНФ. Рассказать алгоритмы приведения к СДНФ, СКНФ.	Пусть $\alpha^{\sigma} = \begin{cases} \alpha, & если \quad \sigma = 1 \\ \_ & \\ \alpha, & если \quad \sigma = 0 \end{cases}$ Пусть α формула, все буквы которой содержатся среди букв $A_1, A_2, ..., A_k$, и φ некоторая интерпретация. Тогда $A_1^{\varphi(A_1)}, A_2^{\varphi(A_2)}, ..., A_k^{\varphi(A_k)} \mid -\alpha^{\varphi(\alpha)}$.
2	Дать определения: контрарная пара литер, элементарная конъюнкция, дизъюнкция, ДНФ, КНФ. Рассказать алгоритм приведения к ДНФ и к КНФ. Доказать критерий тождественной истинности формулы через КНФ (критерий ТЛ через ДНФ).	Доказать, что тавтология является выводимой формулой (в дедуктике Клини).
3	Дать определения: интерпретация языка нулевого порядка, продолжение интерпретации на множество формул логики высказываний. ТИ, ТЛ, выполнимость, эквивалентность на языке интерпретаций. Выполнимое (невыполнимое) множество формул, модель множества формул.	Доказать теорему о семантической полноте дедуктики Клини: для любой формулы α множества формул Γ выполняется $\Gamma \mid = \alpha \quad \Rightarrow \Gamma \mid - \alpha$
4	Дать определение: формула α является логическим следствием множества формул $\Gamma \quad \Gamma \mid = \alpha$, $\varnothing \mid = \alpha$. Доказать принцип дедукции: $\Gamma \mid = \alpha \to \beta \quad \Leftrightarrow \quad \Gamma, \alpha \mid = \beta$.	Дать определение непротиворечивости исчисления (дедуктики). Доказать, что исчисление высказываний непротиворечиво.
5	Доказать, что следующие утверждения для произвольных формул $\alpha_1, \alpha_2, ...\alpha_n, \beta$ логики высказываний эквивалентны: $\alpha_1, \alpha_2, ...\alpha_n \mid = \beta$; $\alpha_1 \wedge \alpha_2 \wedge ... \wedge \alpha_n \mid = \beta$; $\mid = \alpha_1 \wedge \alpha_2 \wedge ... \wedge \alpha_n \to \beta$; $\alpha_1 \wedge \alpha_2 \wedge ... \wedge \alpha_n, \overline{\beta}$ невыполнимо	Доказать семантическую корректность дедуктики Клини.
6	Дать определение: формула α выводима из множества Γ с помощью дедуктики D, вывод формулы α, Дедуктика Клини (Аксиомы 1-10, MP).	Доказать теорему компактности логики высказываний.
7	Доказать, следующие утверждения: для каждой формулы α выполняется $\mid - \alpha \to \alpha$; каждая аксиома является выводимой формулой; если $\Gamma \subseteq \Gamma'$ и $\Gamma \mid - \alpha$, то $\Gamma' \mid - \alpha$	Доказать, что любая резольвента двух данных дизъюнктов является их логическим следствием. Дать определение резолютивного вывода. Доказать теорему о семантической корректности метода резолюций.
8	Доказать свойства выводимости: $\Gamma, \alpha \mid - \alpha$ пр-ло повторения посылки; Если $\Gamma \mid - \alpha$, то $\Gamma, \beta \mid - \alpha$ пр-ло введения посылки; Если $\Gamma \mid - \alpha \to \beta$, то $\Gamma, \alpha \mid - \beta$ пр-ло удаления импликации	Доказать теорему о полноте метода резолюций (в логике высказываний).
9	Доказать свойства выводимости: $\Gamma, \alpha, \beta \mid - \alpha \wedge \beta$ пр-ло введения конъюнкции; $\Gamma, \alpha \wedge \beta \mid - \alpha$; $\Gamma, \alpha \wedge \beta \mid - \beta$ пр-ло удаления конъюнкции; $\Gamma, \alpha \mid - \alpha \vee \beta$; $\Gamma, \beta \mid - \alpha \vee \beta$ пр-ло введения дизъюнкции	Определить операции в трёхзначной логике Лукасевича. Какие законы классической логики не выполняются в логике Лукасевича, доказать.
10	Доказать свойства выводимости: $\Gamma, \overline{\overline{\alpha}} \mid - \alpha$ удаление	Определить операции в трёхзначной логике Лукасевича. Какие законы классической логики выполняются в логике Лукасевича,

	отрицания; Если $\Gamma \mid -\alpha$, $\Gamma \mid -\alpha \to \beta$, то $\Gamma \mid -\beta$ пр-ло МР;	доказать законы де Моргана..
11	Доказать теорему дедукции для исчисления высказываний (в дедуктике Клини).	Дать определения: хорновский дизъюнкт, единичный дизъюнкт, позитивный дизъюнкт. Рассказать алгоритм проверки множества хорновских дизъюнктов на выполнимость (от факта).

Примерный состав билетов по теории Часть 2.

1.1.Дать определение терма языка 1 порядка. 1.2. Пусть сигнатура языка содержит целые числа в качестве констант, двуместные функциональные символы + и г , предикатный символ J и пусть x,y – переменные. Какие из следующих выражений будут термами в данной сигнатуре: А) xг $(y+2)$ Б) x В) xJ $(y+2)$ Г) $y+2$	1.3. Доказать, что интерпретация (алгебраическая система) $\langle$ў,=,S,0$\rangle$ допускает элиминацию кванторов. 1.4. Расскажите алгоритм приведения формулы языка 1 порядка к Сколемовской нормальной форме, приведите пример.
2.1.Дать определение сигнатуры языка 1 порядка, формулы языка 1 порядка. 2.2.Пусть сигнатура языка содержит целые числа в качестве констант, двуместные функциональные символы + и г , предикатный символ J и пусть x,y – переменные. Какие из следующих выражений будут формулами в данной сигнатуре: А) xг $(y+2)$ Б) x В) xJ $(y+2)$ Г) xг $(y+2)$J 0	2.3. Сформулируйте теорему о подстановке терма, свободного для переменной в формуле. Докажите общезначимость формулы $"xa(x) \to a(t)$, где терм t свободен для переменной x в формуле $a(x)$. 2.4. Докажите по определению равносильность $\overline{\$xA(x)}$ є $"x\overline{A(x)}$
3.1.Дать определение общезначимой (тождественно истинной) формулы языка 1 порядка. 3.2. Какие из следующих формул являются общезначимыми для произвольной формулы $A(x)$ с одной свободной переменной для любой сигнатуры А) $"yA(y) \to \$xA(x)$ Б) $\$yA(y) \to "xA(x)$ С) $"y\overline{(A(y)$Щ$\overline{A(y)})}$ Ответ объясните.	3.3. Дайте определение аксиоматической теории 1 порядка. 3.4. Какие вы знаете основные равносильные преобразования формул? Докажите по определению равносильность $"xA(x)$Щ'$xB(x)$ є $"x(A(x)$Щ$B(x))$
4.1.Дать определение выполнимой формулы языка 1 порядка. 4.2. Какие из следующих формул являются выполнимыми для произвольной формулы $A(x)$ с одной свободной переменной А) $"x(A(x)$Щ$\overline{A(x)})$ Б) $\$xA(x) \to "yA(y)$ С) $\overline{"yA(y) \to \$xA(x)}$ Ответ объясните.	4.3. Дайте определение вывода формулы из множества формул для аксиоматической теории. 4.4. Дать определение общезначимой формулы. Доказать, что из $\alpha_1 \wedge \alpha_2 \wedge \ldots \wedge \alpha_n \to \beta$ общезначима, следует, что $\alpha_1 \wedge \alpha_2 \wedge \ldots \wedge \alpha_n, \overline{\beta}$ невыполнимо.

5.1. Рассказать алгоритм приведения к Сколемовской нормальной форме формулы языка 1 порядка. 5.2. Доказать, что из $\alpha_1 \wedge \alpha_2 \wedge ... \wedge \alpha_n, \overline{\beta}$ невыполнимо, следует, что $\alpha_1, \alpha_2, ... \alpha_n \models \beta$	5.3. Рассказать алгоритм элиминации кванторов произвольной формулы интерпретации (алгебраической системы) $\langle ¤, =, < \rangle$. 5.4. Приведите пример элиминации кванторов для $\langle ¤, =, < \rangle$.
6.1. Дать определение истинностное значение формулы $\$x_1 P(x_1, x_2)$ языка 1 порядка в интерпретации на оценке. 6.2. Задан некоторый язык 1 порядка с константами a и b, с одноместными предикатными символами P. Пусть задана интерпретация, с областью интерпретации $M = \{a, b\}$ и интерпретация предикатов: $P(a) = 1, P(b) = 0$. Найдите истинностное значение формулы в данной интерпретации: $\$xP(x) Ъ "xP(x)$ будет ли данная формула выполнимой?	6.3. Известно, что формула $"x\, a(x)$ общезначима. Будет ли общезначимой формула $a(x)$. Докажите. 6.4. Дать определение (записать в символической форме), что значит, формула является логическим следствием множества формул языка 1 порядка. Доказать, что из $\alpha_1, \alpha_2, ... \alpha_n \models \beta$ следует $\alpha_1 \wedge \alpha_2 \wedge ... \wedge \alpha_n \models \beta$.
7.1.Дайте определение истинностного значения формулы $"x_1 P(x_1, x_2)$ языка 1 порядка в интерпретации на оценке. 7.2. Пусть задан некоторый язык 1 порядка с константами a и b, с одноместными предикатными символами P и Q. Пусть задана интерпретация, с областью интерпретации $M = \{a, b\}$ и интерпретация предикатов: $P(a) = 1, P(b) = 1, Q(a) = 1, Q(b) = 0$. Найдите истинностное значение формулы в данной интерпретации: $\$x" y(P(x) Щ Q(y))$	7.3. Какая аксиоматическая теория называется исчислением предикатов? Сформулируйте теорему Гёделя о полноте для исчисления предикатов. 7.4. Дать определение (записать в символической форме), что значит множество формул является выполнимым , невыполнимым. Доказать, что из $\alpha_1 \wedge \alpha_2 \wedge ... \wedge \alpha_n \models \beta$ следует, что множество формул $\alpha_1 \wedge \alpha_2 \wedge ... \wedge \alpha_n, \overline{\beta}$ невыполнимо.
8.1. Дайте определение: значение терма t в интерпретации на оценке. 8.2. Что значит терм свободен в формуле для переменной ? Будет ли терм $t = f(x, y)$ свободен для переменной z в формулах $\forall y P(z, y) \to P(x, z)$ $\forall y P(x, y) \to P(x, z)$ $\forall z \exists y P(z, y) \to P(x, z)$	8.3. Дать определение общезначимой формулы. Доказать, что из $\alpha_1 \wedge \alpha_2 \wedge ... \wedge \alpha_n, \overline{\beta}$ невыполнимо следует, что $\alpha_1 \wedge \alpha_2 \wedge ... \wedge \alpha_n \to \beta$ общезначима. 8.4. Рассказать алгоритм доказательства общезначимости методом резолюций.
9.1.Дайте определение: истинностное значение формулы в интерпретации на оценке. 9.2. Будет ли формула $\exists x \forall y P(x, y) \to \forall y \exists x P(x, y)$ общезначимой ? Докажите.	9.3. Рассказать алгоритм доказательства логического следования методом резолюций. 9.4. Приведите пример доказательства логического следования методом резолюций.
10.1. Дать определение эквивалентных (равносильных) формул языка 1 порядка. 10.2. Какие из следующих формул не являются равносильными $\forall x A(x) \wedge \forall x B(x) \equiv \forall x (A(x) \wedge B(x))$ $\exists x (A(x) \wedge B(x)) \equiv \exists x A(x) \wedge \exists x B(x)$ $\forall x \exists y P(x, y) \equiv \exists y \forall x P(x, y)$ Докажите.	10.3. Дать определение пренексной (предварённой) нормальной формы формулы языка 1 порядка. 10.4. Рассказать алгоритм доказательства общезначимости методом резолюций.

11.1. Дать определение опровержимой формулы языка 1 порядка. 11.2. Задан некоторый язык 1 порядка с константами a и b, с одноместными предикатными символами P и Q. Пусть задана интерпретация, с областью интерпретации $M = \{a,b\}$ и интерпретация предикатов: $P(a) = 1, P(b) = 1, Q(a) = 1, Q(b) = 0$. Найдите истинностное значение формулы в данной интерпретации: $"x(P(x) \amp Q(x))$. Будет ли формула опровержимой?	11.3. Рассказать алгоритм элиминации кванторов произвольной формулы интерпретации (алгебраической системы) $\langle \breve{y}, =, <, S \rangle$. Приведите пример. 11.4. Докажите по определению равносильность $\overline{"xA(x)} \equiv \$x\overline{A(x)}$

Список определений.

1. Предикат задан на множестве. Операции над предикатами.
2. Сигнатура, терм, формула языка первого порядка. Атомарная (элементарная) формула. Язык 1 порядка. Булева комбинация атомарных формул.
3. Свободная переменная, связанная переменная. Замкнутая формула. $\exists$ - замыкание формулы. $\forall$ - замыкание формулы.
4. Интерпретация языка 1 порядка.
5. Оценка в интерпретации.
6. Значение терма в интерпретации на оценке.
7. Истинностное значение формулы в интерпретации на оценке.
8. Формула выполнимая в интерпретации, формула выполнимая, формула опровержимая в интерпретации, формула опровержимая.
9. Формула общезначимая (тождественно истинная), формула противоречивая(тождественно ложная).
10. Равносильные (эквивалентные) формулы языка 1 порядка.
11. Пренексная (предваренная) нормальная форма формулы языка 1 порядка.
12. Сколемовская нормальная форма языка 1 порядка.
13. Формула является логическим следствием множества формул (пустого множества).
14. Множество формул языка 1 порядка является выполнимым (совместным, непротиворечивым), невыполнимым.
15. Терм свободен для переменной в формуле.
16. Литерал. Элементарный дизъюнкт. Унификация переменных дизъюнкта.
17. Говорят, что задана аксиоматическая теория языка 1 порядка.
18. Вывод формулы из множества формул в аксиоматической теории языка 1 порядка.
19. Исчисление предикатов.
20. Интерпретация языка 1 порядка с заданной сигнатурой допускает элиминацию кванторов.

Список алгоритмов

1. Доказательство логического следования методом резолюций.
2. Доказательство общезначимости методом резолюций.
3. Приведение формулы к Сколемовской нормальной форме.
4. Элиминация кванторов для $\langle \breve{y}, =, S, 0 \rangle$.
5. Элиминация кванторов для $\langle \breve{y}, =, <, S \rangle$.
6. Элиминация кванторов для $\langle ¤, =, < \rangle$.

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в электронном университете «Moodle» - https://moodle.tsu.ru/course/view.php?id=00000

б) Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине (Приложение 1).

12. Перечень учебной литературы и ресурсов сети Интернет

Основная.

1. Глухов М.М., Козлитин О.А., Шапошников В.А., Шишков А.Б. Задачи и упражнения по математической логике, дискретным функциям и теории алгоритмов. - СПб: Лань, 2021
2. Верещагин Н., Шень А.. Языки и исчисления. МЦНМО. 2017. 240 с.
3. В.А. Романович. Лекции по математической логике. 4.1,2. Томский государственный университет. 2015, 408 с.

Дополнительная.

4. Игошин В.И. Математическая логика и теория алгоритмов. Академия.- 2008, 448 с.
5. Игошин В.И. Задачи и упражнения по математической логике и теории алгоритмов.- 2007, 304 с.

в) ресурсы сети Интернет:

– http://e-science.sources.ru/ – портал естественных наук
– http://www.coursera.org/ – сайт обучающих курсов ведущих вузов мира
– https://ocw.mit.edu/index.htm – сайт открытых курсов MIT

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:

– Microsoft Office Standart 2013 Russian: пакет программ. Включает приложения: MS Office Word, MS Office Excel, MS Office PowerPoint, MS Office On-eNote, MS Office Publisher, MS Outlook, MS Office Web Apps (Word Excel MS PowerPoint Outlook);

– публично доступные облачные технологии (Google Docs, Яндекс диск и т.п.).

б) информационные справочные системы:

– Электронный каталог Научной библиотеки ТГУ – http://chamo.lib.tsu.ru/search/query?locale=ru&theme=system

– Электронная библиотека (репозиторий) ТГУ – http://vital.lib.tsu.ru/vital/access/manager/Index

– ЭБС Лань – http://e.lanbook.com/
– ЭБС Консультант студента – http://www.studentlibrary.ru/
– Образовательная платформа Юрайт – https://urait.ru/
– ЭБС ZNANIUM.com – https://znanium.com/
– ЭБС IPRbooks – http://www.iprbookshop.ru/

14. Материально-техническое обеспечение

Аудитории для проведения занятий лекционного типа.

Аудитории для проведения занятий семинарского типа, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы, оснащенные компьютерной техникой и доступом к сети Интернет, в электронную информационно-образовательную среду и к информационным справочным системам.

15. Информация о разработчиках

Галанова Наталия Юрьевна, к.ф.-м.н., доцент каф. общей математики, ММФ, ТГУ