Федеральное государственное бюджетное образовательное учреждение
высшего образования
Московский государственный университет имени М.В. Ломоносова
Факультет вычислительной математики и кибернетики

УТВЕРЖДАЮ
декан факультета вычисли-
тельной математики и кибернетики

_____/И.А. Соколов /
«14» октября 2021г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Прикладная теория типов»

Уровень высшего образования:

магистратура

Направление подготовки / специальность:

01.04.02 "Прикладная математика и информатика" (3++)

Направленность (профиль) ОПОП:

Искусственный интеллект в кибербезопасности

Форма обучения:

очная

Рабочая программа рассмотрена и утверждена
на заседании Ученого совета факультета ВМК
(протокол №7, от 29 сентября 2021 года)

Москва 2021

Рабочая программа дисциплины (модуля) разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) для реализуемых основных профессиональных образовательных программ высшего образования по направлению подготовки 01.04.02 "Прикладная математика и информатика" утвержденного Приказом Министерства образования и науки РФ от 10 января 2018 г. N 13.

1. Место дисциплины (модуля) в структуре ОПОП ВО:
Дисциплина (модуль) относится к части дисциплин основной профессиональной образовательной программы, формируемых участниками образовательных отношений.

2. Входные требования для освоения дисциплины (модуля), предварительные условия:
учащиеся должны владеть знаниями по математическому анализу, линейной алгебре и теории вероятностей в объеме, соответствующем программе обучения основных образовательных программ бакалавриата по укрупненным группам направлений и специальностей 01.00.00 «Математика и механика», 02.00.00 «Компьютерные и информационные науки».

3. Результаты обучения по дисциплине (модулю), соотнесенные с требуемыми компетенциями выпускников.

Планируемые результаты обучения по дисциплине (модулю)		
Содержание и код компетенции.	**Индикатор (показатель) достижения компетенции**	**Планируемые результаты обучения по дисциплине, сопряженные с индикаторами достижения компетенций**
ОПК-1. Способен решать актуальные задачи фундаментальной и прикладной математики	ОПК-1.1. Обладает фундаментальными знаниями, полученными в области математики и информатики. ОПК-1.2. Умеет решать актуальные задачи фундаментальной и прикладной математики в профессиональной деятельности ОПК-1.3. Имеет практический опыт решения актуальных задач фундаментальной и прикладной математики в профессиональной деятельности	ОПК-1.1. З-3 ЗНАТЬ: современные методы доказательства корректности программ и практического применения теории типов для уменьшения количества уязвимостей в исходном коде. ОПК-1.2. У-3 УМЕТЬ: применять на практике современные методы верификации ПО. ОПК-1.3. ВЛАДЕТЬ: современным инструментарием для верификации ПО.
ОПК-2. Способен совершенствовать и реализовывать новые математические методы решения прикладных задач	ОПК-2.3 Имеет опыт реализации архитектуры системы искусственного интеллекта математические методы и системы программирования для разработки и реализации алгоритмов.	ОПК-2.3 З-3 ЗНАТЬ: современные подходы к верификации ПО, их достоинства и недостатки. ОПК-2.3 У-3 УМЕТЬ: применять подходы к уменьшению количества уязвимостей в исходном коде на основе систем типов.
ОПК-3. Способен разрабатывать математические модели и проводить их анализ при ре-	ОПК-3.1. Знает возможности современных инструментальных средств и систем про-	ОПК-3.1 З-3 ЗНАТЬ: возможности современных подходов к верификации ПО.

шении задач в области профессиональной деятельности	граммирования в области профессиональной деятельности. ОПК-3.2. Умеет проводить сравнительный анализ и осуществлять выбор инструментальных средств для решения задач в области профессиональной деятельности.	ОПК-3.2 У-3 УМЕТЬ: выбрать и применить нужный подход для уменьшения вероятности наличия уязвимостей в исходном коде.

4. Объем дисциплины (модуля) составляет 3 з.е., в том числе 72 академических часа, отведенных на контактную работу обучающихся с преподавателем, 36 академических часов на самостоятельную работу обучающихся.

5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и виды учебных занятий:

Целью курса является обучение слушателей базовой теории типов и некоторых современных способов верификации компьютерных программ, для достижения чего необходимо решить следующие задачи:

1. Изучить теоретические основы исчислений лямбда высказываний, а также некоторые свойства аксиоматической теории множеств ZFC;
2. Ознакомить слушателей с основами MLTT, HoTT и кубической теории типов;
3. ознакомить слушателей с основами верификации компьютерных программ на примере Coq, Arend и Agda.

Наименование и краткое содержание разделов и тем дисциплины (модуля), **Форма промежуточной аттестации по дисциплине (модулю)**	**Всего (часы)**	В том числе	
		Контактная работа (работа во взаимодействии с преподавателем) **Виды контактной работы, часы**	**Самостоятельная работа обучающегося, часы** *(виды самостоятельной работы – эссе, реферат, контрольная работа и пр. – указываются при необходимости)*

		Занятия лекционного типа	Практические занятия	**Всего**	
Тема 1. Основы ZFC	**5**	2	2	**4**	2 Текущий контроль успеваемости: теоретическое задание № 1
Тема 2. Основы нетипизированного лямбда исчисления	**5**	2	2	**4**	2 Текущий контроль успеваемости: теоретическое задание № 2
Тема 3. Типизированное лямбда исчисление - Просто типизированное лямда исчисление - Система λ2 - Система λP - Система λω - Система CoC	**6**	6	6	**12**	6 Текущий контроль успеваемости: теоретическое задание № 3
Тема 4. Основы системы верификации Coq	**8**	8	8	**16**	6 Текущий контроль успеваемости: практическое задание № 1
Тема 5. Основы MLTT	**6**	8	8	**16**	8
Тема 6. Основы гомотопической и кубической теории типов	**12**	6	6	**12**	6
Тема 7. Основы систем верификации Arend и Agda		4	4	**8**	8 Текущий контроль успеваемости: практическое задание № 2
Промежуточная аттестация: экзамен	**36**	0	0	**0**	
Итого	**108**	**36**	**36**	**72**	**36**

6. Фонд оценочных средств (ФОС, оценочные и методические материалы) для оценивания результатов обучения по дисциплине (модулю).

6.1. Типовые контрольные задания или иные материалы для проведения текущего контроля успеваемости, критерии и шкалы оценивания

Примеры заданий для текущего контроля знаний

Задача 1 (4 балла)

Приведите полный λP вывод $S:*\vdash S\to S\to *:\square$

(a) в древовидном формате

(b) в формате флагов

Задача 2. (9 баллов)

Покажите, что следующие утверждения являются тавтологиями, приведя вывод в λP исчислении:

(a) $(A\Rightarrow B)\Rightarrow((B\Rightarrow C)\Rightarrow(A\Rightarrow C))$ (b) $((A\Rightarrow B)\Rightarrow A)\Rightarrow((A\Rightarrow B)\Rightarrow B)$

(c) $(A\Rightarrow(B\Rightarrow C))\Rightarrow((A\Rightarrow B)\Rightarrow(A\Rightarrow C))$

Задача 3. (7 баллов)

Пусть задан контекст $G\equiv S:*,P:S\to *,Q:S\to *$.

Найдите населяющие объекты $x : S.Px \to Qx \to Px$ с учётом

контекста G, для каждого из них укажите соответствующий вывод.

Задача 4. (9 баллов)

Пусть в λP задан контекст $G \equiv S : *, R : S \to S \to *, u : x, y : S.Rxy \to Ryx, u : x, y, z : S.Rxy \to Rxz \to Ryz$.

(a) покажите, что R рефлексивно на его домене с помощью конструирования населяющих тип объектов

(b) покажите, что R транзитивно на его домене с помощью конструирования населяющих тип объектов

Задача 5. (10 баллов)

Пусть S множество, Q, R отношения, заданные на $S*S$, а f, g - это функции, домен и кодомен которых S. Предположим, что $\forall x,y \in S\ Q(x,f(y)) \to Q(g(x),y)$, $\forall x,y \in S\ Q(x,f(y)) \to R(x,y)$,$\forall x\in S\ Q(x,f(f(x)))$. Докажите, что $\forall x \in S\ R(g(g(x)), g(x))$

6.2. Типовые контрольные задания или иные материалы для проведения промежуточной аттестации по дисциплине, критерии и шкалы оценивания

Вопросы к экзамену

1. Аксиоматика ZFC, задание типов, как множеств.
2. Построение нетепизированного лямбда исчисления: объединение и абстракция. Альфа замена и бэта редукция.
3. Классическая и интуиционистская логика. Комбинаторы.
4. Теорема о неподвижной точке, комбинатор неподвижной точки и его применение.
5. Кодировка Чёрча для чисел и булевой алгебры.
6. Построение λ →, представления Чёрча и Карри.
7. Основные свойства и проверка типов в λ →
8. Редукция в λ →.
9. Построение λ2 и его основные свойства.
10. Абстракция над типами и их применение.
11. Пи и сигма типы на примере λ2.
12. Построение λω и его основные свойства.
13. Логика первого порядка.
14. Основные правила вывода типов в λω: аппликация, абстракция, sort-like, var-like, правило ослабления типов.
15. Построение λP и его основные свойства.
16. Минимальная предикатная логика над λP.
17. Построение λC и его основные свойства.
18. Сравнение вывода и проверки типов в лябмда системах типов, куб Барендрегта.
19. Определения, их виды и формальное определение. Примеры задания индуктивных и рекурсивных определений.
20. Использование определений в λC.
21. n, unit и identity типы.
22. Правила анфолдинга и сигма преобразований определений. Примеры.
23. Построение λD и его основные свойства.
24. Способы вывода и основные типы определений в λD.
25. Построение систем формальной верификации на исчислении лямбда высказываний на примере Coq. Полиморфные и зависимые функции в Coq.
26. Равенство типов в Coq, Пи и Сигма типов.
27. Основные тактики вывода в Coq.
28. Зависимые типы в Coq, использование и формальные основания.
29. Зависимое совпадение типов с формальной точки зрения в Coq.
30. Построение систем формальной верификации на исчислении лямбда высказываний на примере Cgda. Полиморфные и зависимые функции в Coq.
31. Зависимые типы в Agda, использование и формальные основания.
32. Основные отличия систем формальной верификации Coq и Agda.

33. Вселенные типов. Примеры в Coq и Agda.
34. W -типы. Примеры формального описания списков и бинарных деревьев в MLTT.
35. Типы как пространства, основы гомотопической эквивалентности.
36. Унивалентность и эквивалентность типов.
37. Основы высших индуктивных типов на примере типа интервала и окружности.

Преподаватель учитывает оценку за текущий контроль (домашние задания).

$$О_{накопленная} = \frac{(Од/з1 + Од/з2 + ... + Од/з5)}{5}$$

Действует следующий способ округления накопленной оценки текущего контроля: при значениях от 0,1 до 0,4 оценка округляется в меньшую сторону, от 0,5 до 0,9 – в большую.
Результирующая оценка за дисциплину рассчитывается следующим образом:

$$О_{Результирующая} = 0{,}5\ О_{накопленная} + 0{,}5\ О_{экзамен}$$

На экзамене студенту не предоставляется возможность получить дополнительный балл для компенсации оценки за текущий контроль.

ШКАЛА И КРИТЕРИИ ОЦЕНИВАНИЯ результатов обучения (РО) по дисциплине (модулю)				
Оценка РО и соответствующие виды оценочных средств	2 (не зачтено)	3 (зачтено)	4 (зачтено)	5 (зачтено)
Знания *Зачет*	Отсутствие знаний	Фрагментарные знания	Общие, но не структурированные знания	Сформированные систематические знания
Умения *Практические задания*	Отсутствие умений	В целом успешное, но не систематическое умение	В целом успешное, но содержащее отдельные пробелы умение (допускает неточности непринципиального характера)	Успешное и систематическое умение

Навыки (владения, опыт деятельности) *Зачет, практические занятия*	Отсутствие навыков (владений, опыта)	Наличие отдельных навыков (наличие фрагментарного опыта)	В целом, сформированные навыки (владения), но используемые не в активной форме	Сформированные навыки (владения), применяемые при решении задач

7. Ресурсное обеспечение:
7.1. Перечень основной и дополнительной литературы

Основная литература

1. Ланц,Бретт Машинное обучение на R : эксперт. техники для прогност. анализа : [пер. с англ.]. / Бретт Ланц. - СПб. [и др.] : Питер, 2020. - 462, [1] с.; 24 см - (Библиотека программиста).

2. Плас,Джейк Вандер Python для сложных задач. Наука о данных и машинное обучение / Дж. Вандер Плас ; [пер. с англ. И. Пальти]. - СПб. [и др.] : Питер, 2020. - 572, [2] с.; 24 см - (Бестселлеры O'Reilly).

Дополнительная литература

1. Э. Берлекэмп. Алгебраическая теория кодирования. Москва «Мир», 1971.
2. Т. Касами, Н. Токура, Ё. Ивадари, Я. Инагаки. Теория кодирования. Москва «Мир», 1978.

7.2. Перечень лицензионного программного обеспечения, в том числе отечественного производства

При реализации дисциплины может быть использовано следующее программное обеспечение:

1. Программное обеспечение для подготовки слайдов лекций MS PowerPoint
2. Программное обеспечение для создания и просмотра pdf-документов Adobe Reader
3. Издательская система LaTeX.

7.3. Перечень профессиональных баз данных и информационных справочных систем

1. http://www.edu.ru – портал Министерства образования и науки РФ

2. http://www.ict.edu.ru – система федеральных образовательных порталов «ИКТ в образовании»
3. http://www.openet.ru - Российский портал открытого образования
4. http://www.mon.gov.ru - Министерство образования и науки Российской Федерации
5. http://www.fasi.gov.ru - Федеральное агентство по науке и инновациям

7.4. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Math-Net.Ru [Электронный ресурс] : общероссийский математический портал / Математический институт им. В. А. Стеклова РАН ; Российская академия наук, Отделение математических наук. - М. : [б. и.], 2010. - Загл. с титул. экрана. - Б. ц.
URL: http://www.mathnet.ru
2. Университетская библиотека Online [Электронный ресурс] : электронная библиотечная система / ООО "Директ-Медиа" . - М. : [б. и.], 2001. - Загл. с титул. экрана. - Б. ц. URL: www.biblioclub.ru
3. Универсальные базы данных East View [Электронный ресурс] : информационный ресурс / East View Information Services. - М. : [б. и.], 2012. - Загл. с титул. экрана. - Б. ц.
URL: www.ebiblioteka.ru
4. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс] : информационный портал / ООО "РУНЭБ" ; Санкт-Петербургский государственный университет. - М. : [б. и.], 2005. - Загл. с титул. экрана. - Б. ц.
URL: www.eLibrary.ru

7.5. Описание материально-технического обеспечения.

Факультет ВМК, ответственный за реализацию данной Программы, располагает соответствующей материально-технической базой, включая современную вычислительную технику, объединенную в локальную вычислительную сеть, имеющую выход в Интернет. Используются специализированные компьютерные классы, оснащенные современным оборудованием. Материальная база факультета соответствует действующим санитарно-техническим нормам и обеспечивает проведение всех видов занятий (лабораторной, практической, дисциплинарной и междисциплинарной подготовки) и научно-исследовательской работы обучающихся, предусмотренных учебным планом.

8. Соответствие результатов обучения по данному элементу ОПОП результатам освоения ОПОП указано в Общей характеристике ОПОП.

9. Разработчик (разработчики) программы.

Воронов Михаил Сергеевич

10. Язык преподавания - русский.