**Правительство Российской Федерации**

**Санкт-Петербургский государственный университет**

**Р А Б О Ч А Я П Р О Г Р А М М А**

**УЧЕБНОЙ ДИСЦИПЛИНЫ**

Введение в теорию доказательств

Introduction to Proof Theory

**Язык(и) обучения**

русский

Трудоемкость в зачетных единицах: 4

Регистрационный номер рабочей программы: 066020

Санкт-Петербург

2020

**Раздел 1. Характеристики учебных занятий**

**1.1. Цели и задачи учебных занятий**

Курс посвящен основам теории доказательств. Изучаемые в курсе понятия и теоремы входят в необходимый минимум знаний из обширной области Теории Доказательств. Его явно будет недостаточно для того, чтобы, например, быстро разобраться в вопросах, которым посвящены статьи тома IV справочной книги по математической логике, однако, позволят сориентироваться во многих вопросах, которые порождают компьютерные науки.

Освоение курса также должно способствовать развитию математического эстетического чувства.

Для достижения этих целей на занятиях проводится доказательство таких фундаментальных утверждений математической теории доказательств, как теорема об устранении сечений в генценовском исчислении предикатов (классическом и интуиционистском), теорема Эрбрана и основная теорема Ограниченной Арифметики. Для ряда результатов, доказательство которых невозможно провести в рамках курса, будут даны планы их доказательств, либо только формулировки.

Курс можно разделить на две части: основы и арифметика. Ключевыми элементами первой части являются соответствие Карри-Ховарда и Основная Теорема Генцена (Hauptsatz). Конструктивное доказательство последней будет дано в максимально аккуратном виде. По поводу этой теоремы Ж-И Жирар в книге “Proofs and Types” пишет следующее:

“Gentzen's theorem, one of the most important in logic, is not very far removed

from normalisation in natural deduction, which is to a large extent inspired by it.

In a slightly modified form, it is at the root of languages such as PROLOG. In other

words, it is a result which everyone should see proved at least once.”

Вторая часть начинается с вопросов связи интуиционистской арифметики (Гейтинга) и арифметики Пеано, а завершается часть приложением изученной теории к вопросам алгоритмической сложности, т.е. Основной теоремой Ограниченной Арифметики Басса. Идейной основой этой теоремы являлась теорема Парсонса-Минца-Такеути.

В середину курса встроено введение в вопросы проверки правильности доказательств на основе системы Coq. Это позволит, в некотором смысле, увидеть явное приложение изучаемых понятий.

**1.2. Требования к подготовленности обучающегося к освоению содержания учебных занятий (пререквизиты)**

Дисциплина изучается в 5-м семестре обучения. Обучающиеся должны обладать математической культурой, обычно приобретаемой к данному этапу обучения, и изучить общий курс «Математическая логика». В частности, должны быть известны такие понятия, как секвенциальное исчисление предикатов, формальная аксиоматическая теория, арифметика Пеано, классы алгоритмической сложности P,NP.

**1.3. Перечень результатов обучения (learning outcomes)**

После освоения курса обучающиеся должны знать основные понятия, методы и подходы, применяемые в теории доказательств, указанные в разделе 2.2.

Уметь расширить и углубить свои знания по специализированной литературе (например, из списка дополнительной литературы 3.4.2), а также иметь возможность приступить к изучению современных работ, пытаться понимать их проблематику и оценивать ценность излагаемых в этих работах результатов.

Компетенции, формируемые в результате освоения основной образовательной программы

|  |  |
| --- | --- |
| Код компетенции | Наименование и (или) описание компетенции |
| ОПК-1 | Способен применять фундаментальные знания, полученные в области математических и (или) естественных наук, и использовать их в профессиональной деятельности |
| ОПК-3 | Способен применять современные информационные технологии, в том числе отечественные, при создании программных продуктов и программных комплексов различного назначения |
| ОПК-4 | Способен участвовать в разработке технической документации программных продуктов и программных комплексов |
| ПКА-1 | Способен демонстрировать базовые знания математических и естественных наук, программирования и информационных технологий |
| ПКП-1 | Способность проводить под научным руководством исследование на основе существующих методов в конкретной области профессиональной деятельности |
| ПКП-2 | Способен решать задачи в области развития науки, техники и технологии с учетом нормативного правового регулирования в сфере интеллектуальной собственности |
| ПКП-4 | Способен применять современные информационные технологии при проектировании, реализации, оценке качества и анализа эффективности программного обеспечения для решения задач в различных предметных областях |
| ПКП-5 | Способен использовать основные методы и средства автоматизации проектирования, реализации, испытаний и оценки качества при создании конкурентоспособного программного продукта и программных комплексов, а также способен использовать методы и средства автоматизации, связанные с сопровождением, администрированием и модернизацией программных продуктов и программных комплексов |
| ПКП-6 | Способен использовать знания направлений развития компьютеров с традиционной (нетрадиционной) архитектурой; современных системных программных средств: операционных систем, операционных и сетевых оболочек, сервисных программ; тенденции развития функций и архитектур проблемно-ориентированных программных систем и комплексов в профессиональной деятельности |
| ПКП-8 | Способен использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования |
| УКБ-3 | Способен понимать сущность и значение информации в развитии общества, использовать основные методы получения и работы с информацией с учетом современных технологий цифровой экономики и информационной безопасности |

**1.4. Перечень и объём активных и интерактивных форм учебных занятий**

Аудиторная учебная работа: лекции – 2 ч в неделю.  
Самостоятельная работа:   
а) под руководством преподавателя: нет;  
б) в присутствии преподавателя: нет;  
в) без участия преподавателя: индивидуальная работа с литературой из списка 3.4, или предложенной преподавателем, или самостоятельно выбранной обучающимся в целях удовлетворения личных познавательных потребностей.

**Раздел 2. Организация, структура и содержание учебных занятий**

**2.1. Организация учебных занятий**

**2.1.1 Основной курс**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Трудоёмкость, объёмы учебной работы и наполняемость групп обучающихся | | | | | | | | | | | | | | | | | | |
| Код модуля в составе дисциплины,  практики и т.п. | Контактная работа обучающихся с преподавателем | | | | | | | | | | | | Самостоятельная работа | | | | Объём активных и интерактивных  форм учебных занятий | Трудоёмкость |
| лекции | семинары | консультации | практические  занятия | лабораторныеработы | контрольныеработы | коллоквиумы | текущий контроль | промежуточная  аттестация | итоговая аттестация | под руководством преподавателя | в присутствии  преподавателя | сам. раб. с использованием  методических материалов | текущий контроль (сам.раб.) | промежуточная аттестация (сам.раб.) | итоговая аттестация  (сам.раб.) |
| ОСНОВНАЯ ТРАЕКТОРИЯ | | | | | | | | | | | | | | | | | | |
| Форма обучения: очная | | | | | | | | | | | | | | | | | | |
| Семестр 5 | 32 |  | 2 |  |  |  |  |  | 2 |  |  |  | 72 |  | 36 |  | 4 | 4 |
|  | 1-25 |  | 1-25 |  |  |  |  |  | 1-25 |  |  |  | 1-1 |  | 1-1 |  |  |  |
| ИТОГО | 32 |  | 2 |  |  |  |  |  | 2 |  |  |  | 72 |  | 36 |  |  | 4 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Виды, формы и сроки текущего контроля успеваемости и промежуточной аттестации | | | | | | |
| Код модуля в составе дисциплины, практики и т.п. | Формы текущего контроля успеваемости | | Виды промежуточной аттестации | | Виды итоговой аттестации  (только для программ итоговой аттестации и дополнительных образовательных программ) | |
| Формы | Сроки | Виды | Сроки | Виды | Сроки |
| ОСНОВНАЯ ТРАЕКТОРИЯ | | | | | | |
| Форма обучения: очная | | | | | | |
| Семестр 5 |  |  | экзамен, устно, традиционная форма | по графику промежуточной аттестации |  |  |

**2.2. Структура и содержание учебных занятий**

Период обучения (модуль): Семестр 5

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование темы (раздела, части) | Вид учебных занятий | Количество часов |
| I. | Возникновение теории доказательств: логицизм, формализм, интуиционизм, конструктивизм. | Лекции | 2 |
| практические занятия | 0 |
| по методическим материалам | 0 |
| II. | Натуральные выводы. Типизированное λ-исчисление. Соответствие Карри-Ховарда. Теорема о нормализуемости. | Лекции | 6 |
| практические занятия | 0 |
| по методическим материалам | 14 |
| III. | Основные понятия системы Coq. | Лекции | 4 |
| практические занятия | 0 |
| по методическим материалам | 16 |
| IV. | Классическое секвенциальное исчисление LK и интуиционистское LJ. Hauptsatz. Оценки удлинений доказательств при устранении сечений. | Лекции | 4 |
| практические занятия | 0 |
| по методическим материалам | 8 |
| V. | Следствия Hauptsatz. Теорема Эрбрана, интерполяционная теорема Крейга, теорема Бета. | Лекции | 4 |
| практические занятия | 0 |
| по методическим материалам | 8 |
| VI. | Арифметика Гейтинга. Негативный перевод Гёделя-Генцена. Принцип Маркова. | Лекции | 4 |
| практические занятия | 0 |
| по методическим материалам | 10 |
| VII. | Теорема Парсонса-Минца-Такеути. | Лекции | 4 |
| практические занятия | 0 |
| по методическим материалам | 8 |
| VIII. | Основная теорема Ограниченной Арифметики Басса. | Лекции | 4 |
| практические занятия | 0 |
| по методическим материалам | 8 |
| IX. | Промежуточная аттестация | Консультация | 2 |
| Промежуточная аттестация (экзамен) | 2 |

Изучаемые в курсе понятия и теоремы входят в необходимый минимум знаний из обширной области Теории Доказательств. Ввиду фундаментальности материала, существует ряд изложений каждого из разделов курса. Сделаем несколько ссылок на литературу, указанную в разделе 3.4.2.

В максимально сжатом виде содержание основных вопросов курса можно найти в обзоре “Basic Proof Theory” S.S. Wainer и L.A.Wallen из зборника “Proof Theory: A selection of papers from the Leeds Proof Theory Programme 1990”. Остальные работы этого сборника носят весьма специальный характер.

Раздел I может быть опущен и оставлен обучающимся для факультативного ознакомления, например, с главами IX,X,XI книги М. Клайна “Математика. Утрата определённости”. В более сухой манере история возникновения вопросов теории доказательств можно найти в главе 1 книги A.S. Troelstra и D. van Dalen “Constructivism in Mathematics. An introduction”.

Раздел II в лаконичной форме изложен Ж.-И. Жираром в книге “Proofs and Types” в начальных главах 2-4. Более детальное изложение дано в разделах 1.1 и 1.2 книги “Proofs and Computations” H. Schwichtenberg и S.S. Wainer.

Быстрое знакомство с Coq доступно с помощью брошюры В.Н. Крупского, С.Л. Кузнецова “Практикум по математической логике. COQ.” На противоположном полюсе по степени охвата материала находится книга Ива Берто и Пьера Кастерана “Le Coq’ Art”, которая может играть роль справочника.

Разделы IV и V можно обнаружить в любой книге по Теории Доказательств, например, в Главе 1 “Теории Доказательств” Г. Такеути, Главе 2 “An introduction to Proof Theory” C. Басса или Главах 2 и 4 книги Ж.-И. Жирара “Proof theory and logical complexity”.

Введение в вопросы интуиционистской арифметики дано в книге А.Г. Драгалина “Математический Интуиционизм. Введение в теорию доказательств” (глава 2) и уже упомянутой выше книги А. С. Трулстры и Д. ван Далена (глава 3).

Теореме Парсонса-Минца-Такеути и Основной Теореме Ограниченной Арифметики посвящена вторая глава книги “Handbook of Proof Theory”, вышедшей под редакцией С. Басса. Глава называется “Proof theory of arithmetic”. Классическим изложением ограниченной арифметики Басса является его диссертация 1986 года “Bounded Arithmetic”.

**Раздел 3. Обеспечение учебных занятий**

**3.1. Методическое обеспечение**

**3.1.1 Методические указания по освоению дисциплины**

Обучение проводится последовательно путем чтения лекций с закреплением полученных знаний в ходе самостоятельной работы. На лекциях излагаются лишь основные, имеющие принципиальное значение и наиболее трудные для понимания и усвоения вопросы. Для некоторых утверждений и следствий из основных теорем могут быть даны лишь наброски доказательств, детальная проработка которых должна быть проделана обучающимися самостоятельно и, желательно, без обращения к учебным пособиям, статьям и прочим источникам. Помимо устранения пробелов в доказательствах, важную роль, начиная с середины курса, играет активное освоение системы проверки доказательств Coq. Типовые упражнения можно найти в руководствах, указанных в разделе 2.2.

**3.1.2 Методическое обеспечение самостоятельной работы**

При выполнении самостоятельной работы обучающиеся имеют возможность пользоваться специализированными источниками, приведенными в разделе 3.4 и Интернет-ресурсами.

**3.1.3 Методика проведения текущего контроля успеваемости и промежуточной аттестации и критерии оценивания**

Показателем, характеризующим текущую учебную работу, является решение “длинных упражнений” по устранению пробелов в доказательствах, построение несложных доказательств в системе Coq, активность на лекционных занятиях, заключающаяся в уточняющих вопросах, отслеживании деталей доказательств утверждений, нахождении возможных неточностей в доказательствах.

Результаты текущего контроля оцениваются преподавателем. На последнем занятии по каждой из двух частей курса (I-V и VI-VIII) преподаватель объявляет обучающимся итоговые результаты активности. На основании данных результатов, преподаватель может предложить освободить от ответа на вопрос билета, соответствующий этому разделу. Освобождение вступает в силу, если среди присутствующих на этих занятиях обучающихся будет не более одного голоса «против». Таким образом, на экзамене нужно будет либо ответить только на один вопрос (сделано 60% работы), либо, для получения оценки «отлично», необходимо решить задачу (80%).

К экзамену допускаются все, записанные на курс обучающиеся. Промежуточная аттестация состоит из следующих этапов. Если обучающийся не принимал активного участия в работе на занятиях, то до получения экзаменационного билета ему необходимо ответить на 5-6 вопросов на знание определений и формулировок (каждый вопрос 0-10) баллов). При успешном ответе на вопросы (экзамен сдан на 50%), обучающийся может либо сразу получить оценку «удовлетворительно», либо взять билет с двумя вопросами: один по части основ (разделы I-V) и один по арифметике (разделы VI-VIII). Для получения оценки «хорошо» необходимо подробно ответить на экзаменационные вопросы. Два вопроса в сумме дают 30 баллов, один может оказаться проще (10 баллов), второй сложнее (20 баллов). Сложность вопроса указывается в билете. Для получения оценки «отлично» требуется (после успешного ответа на теоретические вопросы) решить предложенную задачу. Задача оценивается 0-20 баллов.

|  |  |  |  |
| --- | --- | --- | --- |
| Итоговый процент  выполнения, % | Оценка СПбГУ при  проведении зачёта | Оценка  ECTS | Оценка СПбГУ при  проведении экзамена |
| 90-100 | зачтено | A | отлично |
| 80-89 | зачтено | B | хорошо |
| 70-79 | зачтено | C | хорошо |
| 60-69 | зачтено | D | удовлетворительно |
| 50-59 | зачтено | E | удовлетворительно |
| менее 50 | не зачтено | F | неудовлетворительно |

**3.1.4 Методические материалы для проведения текущего контроля успеваемости и промежуточной аттестации (контрольно-измерительные материалы, оценочные средства)**

**Компетенции, впервые формируемые дисциплиной:**

ПКП-2 — способен решать задачи в области развития науки, техники и технологии с учетом нормативного правового регулирования в сфере интеллектуальной собственности.

**Компетенции, развиваемые дисциплиной:**

ОПК-1 — способен применять фундаментальные знания, полученные в области математических и (или) естественных наук, и использовать их в профессиональной деятельности.

ОПК-3 — способен применять современные информационные технологии, в том числе отечественные, при создании программных продуктов и программных комплексов различного назначения.

ОПК-4 — способен участвовать в разработке технической документации программных продуктов и программных комплексов.

ПКА-1 — способен демонстрировать базовые знания математических и естественных наук, программирования и информационных технологий.

ПКП-1 — способность проводить под научным руководством исследование на основе существующих методов в конкретной области профессиональной деятельности.

ПКП-4 — способен применять современные информационные технологии при проектировании, реализации, оценке качества и анализа эффективности программного обеспечения для решения задач в различных предметных областях.

ПКП-5 — способен использовать основные методы и средства автоматизации проектирования, реализации, испытаний и оценки качества при создании конкурентоспособного программного продукта и программных комплексов, а также способен использовать методы и средства автоматизации, связанные с сопровождением, администрированием и модернизацией программных продуктов и программных комплексов.

ПКП-6 — способен использовать знания направлений развития компьютеров с традиционной (нетрадиционной) архитектурой; современных системных программных средств: операционных систем, операционных и сетевых оболочек, сервисных программ; тенденции развития функций и архитектур проблемно-ориентированных программных систем и комплексов в профессиональной деятельности.

ПКП-8 — способен использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования.

УКБ-3 — способен понимать сущность и значение информации в развитии общества, использовать основные методы получения и работы с информацией с учетом современных технологий цифровой экономики и информационной безопасности.

**Компетенции, полностью сформированные по результатам освоения дисциплины:**

Нет.

Для каждой компетенции применяется линейная шкала оценивания, определяемая долей успешно выполненных заданий, проверяющих данную компетенцию

На первом занятии преподаватель доводит до обучающихся информацию о сроках проведения экзамена и условиях аттестации.

Список основных вопросов зависит от того, насколько детально и широко рассматривается каждый из восьми разделов курса. В курсе имеется несколько “больших” теорем, которые в списке экзаменационных вопросов должны быть разбиты на несколько, в соответствии с этапами доказательства. Например, для главы VIII можно выделить следующие основные этапы:

1. Полиномиальная иерархия. Формулировка теоремы Кобхема. Иерархия ограниченных формул. Формулировка теоремы Кента-Ходжсона.
2. Ограниченные арифметики Басса и .
3. -выразимые (в теории *T*) функции и -выразимые (в теории *T*) отношения.
4. Расширение и выразимыми в этих теориях функциями и отношениями.
5. Кодирование конечных последовательностей. Первая часть Основной теоремы Ограниченной Арифметики.
6. Ограниченное секвенциальное исчисление *LKB*. Устранимость сечений в *LKB*.
7. Вторая часть Основной теоремы Ограниченной Арифметики.

*Проверяемые компетенции: ПКП-2, ОПК-1, ОПК-3, ОПК-4, ПКА-1, ПКП-1, ПКП-4, ПКП-5, ПКП-6, ПКП-8, УКБ-3*

*Сформированность компетенций считается пропорционально доле успешных ответов на вопросы и выполненности заданий.*

**3.1.5 Методические материалы для оценки обучающимися содержания и качества учебного процесса**

Для оценки обучающимися содержания и качества учебного процесса применяется анкетирование в соответствии с методикой и графиком, утвержденными в установленном порядке.

**3.2. Кадровое обеспечение**

**3.2.1 Образование и (или) квалификация штатных преподавателей и иных лиц, допущенных к проведению учебных занятий**

К преподаванию дисциплины могут быть допущены преподаватели, имеющие диплом о высшем образовании или учёную степень, соответствующие профилю преподаваемой дисциплины.

**3.2.2 Обеспечение учебно-вспомогательным и (или) иным персоналом**

Не требуется.

**3.3. Материально-техническое обеспечение**

**3.3.1 Характеристики аудиторий (помещений, мест) для проведения занятий**

Учебные аудитории для проведения учебных занятий, оснащенные стандартным оборудованием, используемым для обучения в СПбГУ в соответствии с требованиями материально-технического обеспечения.

**3.3.2 Характеристики аудиторного оборудования, в том числе неспециализированного компьютерного оборудования и программного обеспечения общего пользования**

Стандартное оборудование, используемое для обучения в СПбГУ.

MS Windows, MS Office, Mozilla FireFox, Google Chrome, Acrobat Reader DC, WinZip, Антивирус Касперского.

**3.3.3 Характеристики специализированного оборудования**

Не требуется.

**3.3.4 Характеристики специализированного программного обеспечения**

Не требуется.

**3.3.5 Перечень и объёмы требуемых расходных материалов**

Мел, маркеры, тряпки для стирания мела, губки для стирания маркерной записи.

**3.4. Информационное обеспечение**

**3.4.1 3.4.1 Список обязательной литературы**

1. Математическая теория логического вывода. - М.: Наука, 1967.

**3.4.2 Список дополнительной литературы**

1. Клини С.К. Математическая логика. - М.: Мир, 1973.
2. Такеути Г. Теория доказательств. М.: Мир, 1978.
3. Драгалин А. Г. Математический интуиционизм. Введение в теорию доказательств. - М.: Наука, 1979.
4. Справочная книга по математической логике, под ред. Дж. Барвайса. Том 4, "Теория доказательств". - М.: Наука, 1982.
5. Клайн М. “Математика. Утрата определённости” - М.: Мир, 1984.
6. S. Buss. Bounded Arithmetic. Bibliopolis, Naples, Italy, 1986.
7. V. Orevkov. Complexity of proofs and their transformations in axiomatic theories. Amer. Math. Soc., 1993.
8. S. Buss. An introduction to proof theory, in Handbook of Proof Theory (ed. S. Buss), North-Holland, Amsterdam, 1998, pp. 1–78.
9. S. Buss. Proof theory of arithmetic, in Handbook of Proof Theory (ed. S. Buss), North-Holland, Amsterdam, 1998, pp. 79–147.
10. J. Krajıcek. Bounded Arithmetic, Propositional Logic, and Complexity Theory // Vol. 60 of Encyclopedia of Mathematics and Its Applications, Cambridge University Press, Cambridge, 1995.
11. A. Woods. Some problems in logic and number theory, and their connections. Ph.D. Thesis, University of Manchester, 1981.
12. Jean-Yves Girard*.* Proof theory and logical complexity*.* Volume I. Studies in proof theory, no. 1. Bibliopolis, Naples 1987.
13. Troelstra A. S. & van Dalen D. Constructivism in mathematics. An introduction. Volume 1. North-Holland, Amsterdam. 1988.
14. J.Y. Girard, Y. Lafont, P. Taylor. Proofs and Types. Cambridge Tracts in Theoretical Computer Science, Cambridge University Press, Cambridge, 1989.
15. [Peter Aczel](https://philpapers.org/s/Peter%20Aczel), [Harold Simmons](https://philpapers.org/s/Harold%20Simmons) , S. S. Wainer (eds.) Proof Theory: A Selection of Papers From the Leeds Proof Theory Programme, 1990.
16. Helmut Schwichtenberg and Stanley S. Wainer. Proofs and Computations. Cambridge: Cambridge University, 2012.
17. В.Н.Крупский, С.Л.Кузнецов, “Практикум по математической логике. COQ.” 2013г. <http://www.mi-ras.ru/~sk/lehre/coq/coq_pract.pdf>
18. Yves Bertot, Pierre Casteran. Interactive Theorem Proving and Program Development. Coq’Art:The Calculus of Inductive Constructions. <https://www.labri.fr/perso/casteran/CoqArt/coqartF.pdf>

**3.4.3 Перечень иных информационных источников**

1. Сайт Научной библиотеки им. М. Горького СПбГУ: http://www.library.spbu.ru/
2. Электронный каталог Научной библиотеки им. М. Горького СПбГУ: http://www.library.spbu.ru/cgi-bin/irbis64r/cgiirbis\_64.exe?C21COM=F&I21DBN=IBIS&P21DBN=IBIS
3. Перечень электронных ресурсов, находящихся в доступе СПбГУ: http://cufts.library.spbu.ru/CRDB/SPBGU/
4. Перечень ЭБС, на платформах которых представлены российские учебники, находящиеся в доступе СПбГУ: http://cufts.library.spbu.ru/CRDB/SPBGU/browse?name=rures&resource\_type=8

**Раздел 4. Разработчики программы**

Старчак Михаил Романович, ассистент кафедры информатики, <mikhstark@gmail.com>