**Санкт-Петербургский филиал федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский университет "Высшая школа экономики"»**

Факультет Санкт-Петербургская школа
физико-математических и компьютерных наук
Департамент информатики

**Рабочая программа дисциплины**
Теория информации

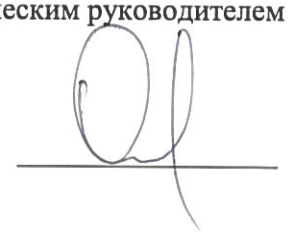
для образовательной программы «Прикладная математика и информатика»
направления подготовки 01.03.02 «Прикладная математика и информатика»
уровень бакалавриат

Разработчик: Близнец Иван Анатольевич, bliznecz@hse.ru

Утверждена Академическим руководителем образовательной программы

«31» августа 2018 г.

А.В. Омельченко



Санкт-Петербург, 2018

## 1. Область применения и нормативные ссылки

Настоящая программа учебной дисциплины устанавливает требования к образовательным результатам студента и определяет содержание и виды учебных занятий и отчетности.

Программа предназначена для преподавателей, ведущих дисциплину «Теория информации», учебных ассистентов и студентов направления 01.03.02 «Прикладная математика и информатика» подготовки бакалавра, обучающихся по бакалаврской программе «Прикладная математика и информатика» и изучающих дисциплину «Теория информации».

Рабочая программа дисциплины разработана в соответствии с:

- Образовательным стандартом НИУ ВШЭ по направлению подготовки 01.03.02 «Прикладная математика и информатика» (уровень бакалавриата), утвержденным ученым советом Национального исследовательского университета «Высшая школа экономики», протокол от 03.03.2017 №02.
- Основной профессиональной образовательной программой «Прикладная математика и информатика» направления подготовки 01.03.02 «Прикладная математика и информатика»;
- Объединенным учебным планом университета по образовательной программе «Прикладная математика и информатика», утвержденным в 2018 г.

## 2. Цели освоения дисциплины

Целями освоения дисциплины «Теория информации» являются формирование у студентов теоретических знаний и практических навыков по основам теории множеств, теории графов, комбинаторного анализа как основного математического аппарата для построения моделей дискретных структур, освоение методов математического моделирования и анализа таких структур.

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

В результате изучения дисциплины обучающийся должен:

**знать:**

- определение количества информации по Хартли и основные свойства,
- определение энтропии Шеннона и основные её свойства,
- основные определения из коммуникационной сложности,
- определение колмоговской сложности и основные её свойства.

**уметь:**

- оценивать количество информации по Хартли;
- применять свойства и соотношения на энтропию Шеннона для оценки энтропии различных случайных величин;
- применять свойства и соотношения на колмогоровскую сложность для оценки колмогоровской сложности;
- доказывать оценки на коммуникационную сложность;

**владеть:**

- основными методами работы с энтропией Шеннона и оценками на колмогоровскую сложность;
- основами техниками доказательства оценок на коммуникационную сложность.

В результате освоения дисциплины студент осваивает следующие компетенции:

| Компетенция | Код по стандарту НИУ ВШЭ | Уровень формирования компетенции | Дескрипторы – основные признаки освоения (показатели достижения результата) | Формы и методы обучения, способствующие формированию и развитию компетенции | Форма контроля уровня сформированности компетенции |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| Способен работать с информацией: находить, оценивать и использовать информацию из различных источников, необходимую для решения научных и профессиональных задач (в том числе на основе системного подхода) | УК-5 | РБ<br>СД<br>МЦ | Знает различные методы представления теории информации.<br>Умеет оценивать количество информации и давать оценку сложности.<br>Владеет навыками работы с энтропией и сложностью. | Лекции, подготовка к практическим занятиям, работа на практических занятиях, самостоятельная работа | Домашнее задание, письменный экзамен |
| Способен применять и модифицировать математические модели для решения задач в области профессиональной деятельности | ОПК-3 | РБ<br>СД<br>МЦ | Знает понятие сложности и энтропии.<br>Находит коммуникационную и формульную сложность булевых функций.<br>Владеет навыками применения Колмогоровской сложности. | Лекции, подготовка к практическим занятиям, работа на практических занятиях, самостоятельная работа | Домашнее задание, письменный экзамен |
| Способен вести письменную и устную коммуникацию на русском и иностранном языках в рамках профессионального и научного общения | ОПК-5 | РБ<br>СД<br>МЦ | Знает основную терминологию, применяемую в области теории информации.<br>Умеет грамотно строить письменную и устную коммуникацию в рамках образовательного процесса.<br>Владеет навыками участия в научных дискуссиях на заданную тему. | Лекции, подготовка к практическим занятиям, работа на практических занятиях, самостоятельная работа | Домашнее задание, письменный экзамен |
| Способен грамотно и аргументировано публично представлять результаты своей научной и профессиональной деятельности, в т.ч. используя современные средства ИКТ | ПК-5 | РБ<br>СД<br>МЦ | Демонстрирует умение подготовки презентаций по заданной теме.<br>Умеет аргументированно выражать свою точку зрения.<br>Владеет навыками публичного выступления по вопросам теории информации. | Лекции, подготовка к практическим занятиям, работа на практических занятиях, самостоятельная работа | Домашнее задание, письменный экзамен |

## 4. Место дисциплины в структуре образовательной программы

Для образовательной программы «Прикладная математика и информатика» направления подготовки 01.03.02 «Прикладная математика и информатика» настоящая дисциплина относится к дисциплинам по выбору базовой профильной части блока дисциплин.

Для освоения дисциплины необходимы компетенции, полученные в ходе изучения дисциплин:

- Дискретная математика;
- Алгоритмы и структуры данных;
- Теория алгоритмов.

Основные положения данной дисциплины используются для освоения следующих дисциплин:

- Криптографичесие протоколы

## 5. Тематический план учебной дисциплины

Курс рассчитан на 66 часов аудиторной нагрузки, из них 33 часа лекций и 33 часа практических занятий, общим объемом 3 зачетных единицы (114 часов).

| № | Название раздела | Всего часов | Аудиторные часы | | | Самостоя - тельная работа |
|---|---|---|---|---|---|---|
| | | | Лекции | Семинары | Практи-ческие занятия | |
| 1. | Информация по Хартли. Энтропия Шеннона. | 38 | 11 | - | 11 | 16 |
| 2. | Кодирование. Теория информации в криптографии. | 38 | 11 | - | 11 | 16 |
| 3. | Коммуникационная сложность и формульная сложность булевых функций. Колмогоровская сложность. Применение Колмогоровской сложности. | 38 | 11 | - | 11 | 16 |
| Итого | | 114 | 33 | - | 33 | 48 |

## 6. Содержание дисциплины

| Раздел 1. Информация по Хартли. Энтропия Шеннона. | |
|---|---|
| Тема 1 | Информация по Хартли.<br>– Мотивация и определение.<br>– Информация в проекциях.<br>– Игра в 10 вопросов.<br>– Цена информации.<br>– Упорядочение камней по весу.<br>– Поиск фальшивой монетки (разные вариации).<br>– Логика знаний. |
| Тема 2 | Энтропия Шеннона.<br>– Мотивация и определение.<br>– Свойства энтропии.<br>– Энтропия пары.<br>– Условная энтропия.<br>– Свойства условной энтропии.<br>– Взаимная информация.<br>– Свойства взаимной информации.<br>– Применение энтропии к задаче о поиске фальшивой монетки.<br>– Энтропийные профили для одного, двух и трёх распределений.<br>– Неравенства о тройке распределений (два). |

| | |
|---|---|
| Раздел 2. Кодирование. Теория информации в криптографии. | |
| Тема 1 | Кодирование.<br>– Однозначно декодируемые коды.<br>– Неравенство Крафта-Макмилана.<br>– Префиксные коды.<br>– Теоремы Шеннона об однозначно декодируемых кодах.<br>– Код Шеннона-Фано, код Хаффмана.<br>– Блоковое кодирование.<br>– Арифметическое кодирование.<br>– Теоремы Шеннона о блоковом кодировании с ошибками. |
| Тема 2 | Теория информации в криптографии.<br>– Теорема Шеннона об энтропии ключа шифрования.<br>– Схемы разделения секрета. Пороговая схема Шамира.<br>– Энтропия секрета существенного участника.<br>– Нижняя оценка 3/2 на энтропию ключа участника.<br>– Теорема Чирмаза. |
| Раздел 3. Коммуникационная сложность и формульная сложность булевых функций. Колмогоровская сложность. Применение Колмогоровской сложности. | |
| Тема 1 | Коммуникационная сложность и формульная сложность булевых функций.<br>– Верхние оценки на коммуникационную сложность функций.<br>– Нижние оценки: метод размера прямоугольников, метод трудного множества и метод ранга матрицы.<br>– Сложность EQ и GE.<br>– Теорема Карчмера-Вигдерсона.<br>– Внешнее и внутреннее информационное разглашение и их связь.<br>– Теорема о связи размера протокола и внешнего информационного разглашения.<br>– Теорема Храпченко. |
| Тема 2 | Колмогоровская сложность.<br>– Теорема о существовании оптимального способа описания.<br>– Определение колмогоровской сложности.<br>– Свойства колмогоровской сложности.<br>– Слова большой сложности.<br>– Невычислимость колмогоровской сложности.<br>– Связь колмогоровской сложности и энтропии.<br>– Условная сложность: существование оптимального способа описания, определение и свойства.<br>– Сложность пары. Теорема Колмогорова-Левина.<br>– Метод несжимаемых объектов.<br>– Теорема об иерархии языков, распознаваемых конечными автоматами с несколькими головками.<br>– Случайность по Мартину-Лёфу. Свойства.<br>– Теорема о том, что случайные последовательности случайны по Мартину-Лёфу. |
| Тема 3 | Применение Колмогоровской сложности<br>– Перенос информации по ленте.<br>– Нижняя оценка на копирование на одноленточной машине Тьюринга.<br>– Алгоритм сложения битовых чисел.<br>– Локальная лемма Ловаса.<br>– Симметричная локальная лемма Ловаса.<br>– Применение локальной леммы Ловаса к последовательностям с запрещёнными словами. |

| | |
|---|---|
| | – Эффективное доказательство леммы Ловаса, Теорема Мозера-Тардош. |

## 7. Оценочные средства

### 7.1. Формы контроля знаний студентов

| Тип контроля | Форма контроля | 3 год | Параметры |
|---|---|---|---|
| | | 3 модуль | |
| Текущий | Домашнее задание | * | Письменное домашнее задание |
| Итоговый | Письменный экзамен | * | Экзамен в письменной форме |

### 7.2. Критерии и шкалы оценки

#### 7.2.1. Текущий контроль

Текущий контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств.

**ДОМАШНЕЕ ЗАДАНИЕ**

*Домашнее задание выдается студентам в одном варианте и состоит из 8 задач. Срок выполнения домашнего задания - 2 недели. Форма представления обучающимися домашнего задания - представленные в письменном виде решения задач.*

**Пример домашнего задания №1:**

1. Пусть даны случайные величины $\alpha, \beta$ с $n$ возможными исходами. Докажите, что $|H(\alpha) - H(\beta)| \leq d \log n + h(d, 1-d)$, где $d$ обозначает статистическое расстояние между $\alpha, \beta$, а $h(d, 1-d)$ есть энтропия Шеннона случайной величины с вероятностями исходов $d$ и $1-d$.

2. Пусть энтропия случайно величины $a$ равна $n$, а взаимная информация пар $a$ и $b$, а также $a$ и $c$ больше $3n/4$. Докажите, что $I(b:c) > n/2$.

3. Случайные функции $a$ и $b$ принимают значения в 3-элементном множестве, и $a = b$ с вероятностью $2/3$. Докажите, что $H(a \mid b) \leq \frac{4}{3}$.

4. Докажите, что следующее утверждение неверно
$\exists c \; \forall x, y \;\; K(x, y) \leq K(x) + K(y \mid x) + c.$

5. Если функция KS' перечислима сверху и $|\{x | KS'(x) < n\}| \leq 2^n$ при всех $n$, то найдется такое $c$, что $KS(x) < KS'(x) + c$ для всех $x$.

6. Докажите, что для любого $m$, для всех достаточно больших $n$ найдется не менее $m$ слов $x$ длины $n$ таких, что $KS(x) \geq n$.

7. Докажите, что для префиксной колмогоровской сложности выполняется неравенство:
$KP(x, y) \leq KP(x) + KP(y) + O(1).$

8. Пусть $X, Y$ случайные величины. Пусть $Z = X + Y$.

(i) Докажите, что $H(Z \mid X) = H(Y \mid X)$. Покажите, что если $X, Y$ независимы, то $H(Y) \leq H(Z)$ и $H(X) \leq H(Z)$.

(ii) Приведите пример, таких $X, Y$, что $H(Z) < H(X)$.

(iii) Опишите условия при которых $H(Z) = H(X) + H(Y)$

**Критерии оценивания и шкала оценки домашнего задания**

| Оценка | Критерии выставления оценки |
|---|---|
| «Отлично» (8-10) | Решено задач 6 и более задач |
| «Хорошо» (6-7) | Количество решенных задач: 4 или 5 |
| «Удовлетворительно» (4-5) | Количество решенных задач: 2 или 3 |
| «Неудовлетворительно» (0-3) | Количество решенных задач: 0 или 1 |

### 7.2.2. Итоговый контроль по дисциплине

Проверка качества освоения дисциплины производится в форме письменного экзамена.

**ПИСЬМЕННЫЙ ЭКЗАМЕН**

*Письменный экзамен проводится в форме ответов на вопросы экзаменационного билета. Экзаменационный билет содержит два вопроса из перечня вопросов к экзамену. На подготовку ответа выделяется 2,5 часа.*

**Примерный перечень вопросов к экзамену:**

1. Информация по Хартли. Мотивация и определение. Информация в проекциях. Игра в 10 вопросов. Цена информации. Упорядочение камней по весу. Поиск фальшивой монетки (разные вариации). Логика знаний.
2. Энтропия Шеннона. Мотивация и определение. Свойства энтропии. Энтропия пары. Условная энтропия. Свойства условной энтропии. Взаимная информация. Свойства взаимной информации. Применение энтропии к задаче о поиске фальшивой монетки.
3. Кодирование. Однозначно декодируемые коды. Неравенство Крафта-Макмилана. Префиксные коды. Теоремы Шеннона об однозначно декодируемых кодах. Код Шеннона-Фано, код Хаффмана.
4. Блоковое кодирование с ошибками. Блоковое кодирование. Арифметическое кодирование. Теоремы Шеннона о блоковом кодировании с ошибками.
5. Свойства распределений. Энтропийные профили для одного, двух и трёх распределений. Неравенства о тройке распределений (два).
6. Криптография. Теорема Шеннона об энтропии ключа шифрования. Схемы разделения секрета. Пороговая схема Шамира. Энтропия секрета существенного участника. Нижняя оценка 3/2 на энтропию ключа участника. Теорема Чирмаза.
7. Коммуникационная сложность. Верхние оценки на коммуникационную сложность функций. Нижние оценки: метод размера прямоугольников, метод трудного множества и метод ранга матрицы. Сложность □□ и □□.
8. Связь протоколов и формул. Теорема Карчмера-Вигдерсона. Внешнее и внутреннее информационное разглашение и их связь. Теорема о связи размера протокола и внешнего информационного разглашения. Теорема Храпченко.
9. Колмогоровская сложность. Теорема о существовании оптимального способа описания.

Определение колмогоровской сложности. Свойства колмогоровской сложности. Слова большой сложности. Невычислимость колмогоровской сложности. Связь колмогоровской сложности и энтропии.

10. Условная колмогоровская сложность и сложность пары. Условная сложность: существование оптимального способа описания, определение и свойства. Сложность пары. Теорема Колмогорова-Левина.
11. Метод несжимаемых объектов. Теорема об иерархии языков, распознаваемых конечными автоматами с несколькими головками.
12. Алгоритмическая случайность. Случайность по Мартину-Лёфу. Свойства. Теорема о том, что случайные последовательности случайны по Мартину-Лёфу.
13. Применение колмогоровской сложности. Перенос информации по ленте. Нижняя оценка на копирование на одноленточной машине Тьюринга. Алгоритм сложения битовых чисел.
14. Локальная лемма Ловаса. Локальная лемма Ловаса. Симметричная локальная лемма Ловаса. Применение локальной леммы Ловаса к последовательностям с запрещёнными словами.
15. Эффективное доказательство леммы Ловаса. Теорема Мозера-Тардош.

**Критерии оценивания и шкала оценки письменного экзамена**

| Оценка | Критерии выставления оценки |
|---|---|
| «Отлично» (8-10) | Дан развернутый ответ на поставленные вопросы. Материал изложен последовательно. Имеются логичные и аргументированные выводы. |
| «Хорошо» (6-7) | Дан развернутый ответ на поставленные вопросы. Материал изложен в целом последовательно. Имеются логичные и аргументированные выводы. |
| «Удовлетворительно» (4-5) | Ответ на вопросы не является полным. Материал изложен непоследовательно. Выводы не аргументированы. |
| «Неудовлетворительно» (0-2) | Ответ на вопрос является неверным. Материал изложен непоследовательно. Отсутствуют выводы. |

### 7.3 Порядок формирования оценок по дисциплине

Результирующая оценка за дисциплину рассчитывается следующим образом:

$$О_{Результирующая} = 0{,}5\ О_{д/з} + 0{,}5\ О_{экзамен1}$$

Действует следующий способ округления: при значениях от 0,1 до 0,4 оценка округляется в меньшую сторону, от 0,5 до 0,9 – в большую.

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

## 8. Образовательные технологии

Основными образовательными технологиями являются: интерактивные лекции, работа в группах на практических занятиях.

## 9. Учебно-методическое и информационное обеспечение дисциплины

### 9.1 Основная литература


1. Шапцев, В. А. Теория информации. Теоретические основы создания информационного общества: учебное пособие для вузов / В. А. Шапцев, Ю. В. Бидуля. — М. : Издательство Юрайт, 2018. — 177 с.
2. Elements of Information Theory. Cover T.M., Thomas J.A. Wiley, 2006

3. Elements of Information Theory//Wireless Communications: Algorithmic Techniques. Vitetta G.M., Taylor D.P., Colavolpe G., Pancaldi F., Martin P.A. Wiley, 2013.

### 9.2 Дополнительная литература

1. Крупский, В. Н. Теория алгоритмов. Введение в сложность вычислений: учебное пособие для бакалавриата и магистратуры / В. Н. Крупский. — 2-е изд., испр. и доп. — М.: Издательство Юрайт, 2018. — 117 с.
2. Information Theory and Statistical Learning / Dehmer, Matthias; Emmert-Streib, Frank. Springer. 2009
3. Information Theory and Best Practices in the IT Industry / Mohapatra, Sanjay; Amboy. Springer. 2012

## 10. Рекомендации для самостоятельной работы студентов

Самостоятельная работа может рассматриваться как организационная форма обучения - система педагогических условий, обеспечивающих управление учебной деятельностью по освоению знаний и умений в области учебной деятельности без посторонней помощи. Студенту нужно четко понимать, что самостоятельная работа – не просто обязательное, а необходимое условие для получения знаний по дисциплине и развитию компетенций, необходимых в будущей профессиональной деятельности.

Самостоятельная работа проводится с целью:

- систематизации и закрепления полученных на лекциях теоретических знаний;
- углубления и расширения теоретических знаний;
- формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развития познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирования самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- формирования практических (общеучебных и профессиональных) умений и навыков;
- развития исследовательских умений;
- получения навыков эффективной самостоятельной профессиональной (практической и научно-теоретической) деятельности.

В учебном процессе выделяют два вида самостоятельной работы:

- аудиторная;
- внеаудиторная.

Аудиторная самостоятельная работа по дисциплине выполняется на учебных занятиях под непосредственным руководством преподавателя и по его заданию.

Внеаудиторная самостоятельная работа - планируемая учебная работа студентов, выполняемая во внеаудиторное время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

Самостоятельная работа, не предусмотренная программой учебной дисциплины, раскрывающей и конкретизирующей ее содержание, осуществляется студентом инициативно, с целью реализации собственных учебных и научных интересов.

Для более эффективного выполнения самостоятельной работы по дисциплине преподаватель рекомендует источники для работы, характеризует наиболее рациональную методику самостоятельной работы, демонстрирует ранее выполненные студентами работы и т. п.

Виды заданий для внеаудиторной самостоятельной работы, их содержание и характер могут иметь вариативный и дифференцированный характер, учитывать индивидуальные особенности студента.

Самостоятельная работа может осуществляться индивидуально или группами студентов online и на занятиях в зависимости от цели, объема, конкретной тематики самостоятельной работы,

уровня сложности.

Контроль результатов внеаудиторной самостоятельной работы осуществляется в пределах времени, отведенного на обязательные учебные занятия по дисциплине на практических занятиях.

**11. Материально-техническое обеспечение дисциплины и информационные технологии, используемые при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения информационных справочных систем (при необходимости).**

Для проведения всех занятий используется проектор и компьютер для проекции слайдов.

**12. Особенности организации обучения для лиц с ограниченными возможностями здоровья**

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться следующих варианты восприятия учебной информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

1) *для лиц с нарушениями зрения:* в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.

2) *для лиц с нарушениями слуха*: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

3) *для лиц с нарушениями опорно-двигательного аппарата*: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.