

МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра нелинейной динамики

УТВЕРЖДАЮ

Декан математического факультета



Нестеров П.Н.

21 мая 2024 г.

Рабочая программа дисциплины

Вероятностные алгоритмы

Направление подготовки (специальности)
10.05.01 Компьютерная безопасность

Направленность (профиль)
«Математические методы защиты информации»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 26 апреля 2024 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2024 г.

1. Цели освоения дисциплины

Цель дисциплины - формирование у студентов способности применять основные методы теории вероятностей и математической статистики при решении задач в их будущей профессиональной деятельности (научно-исследовательской, проектной, контрольно-аналитической). Задачи дисциплины - дать обучаемым необходимые знания по алгоритмам, основанным на вероятностных методах; способствовать развитию у обучаемых строгого математического и творческого мышления.

2. Место дисциплины в структуре образовательной программы

Данная дисциплина относится к вариативной части образовательной программы и является дисциплиной по выбору.

Для освоения дисциплины, требуются знания по основным математическим дисциплинам: математическому анализу, теории вероятностей и др.

Знания и умения, приобретаемые обучаемыми по дисциплине «Вероятностные алгоритмы», могут быть использованы при разработке курсовых и дипломных работ, в научно-исследовательской работе.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	Перечень планируемых результатов обучения
Общепрофессиональные компетенции	
ОПК-2 Обладает способностью корректно применять при решении профессиональных задач аппарат математического анализа, геометрии, алгебры, дискретной математики, математической логики, теории алгоритмов, теории вероятностей, математической статистики, теории информации, теоретико-числовых методов	Знать: - основные понятия теории графов; Уметь: - строить теоретико-вероятностные и статистические модели задач и явлений практического характера по специальности; Владеть: - навыками научного исследования с применением вероятностно-статистических методов
Профессиональные компетенции	
ПК-4 Обладает способностью проводить анализ и участвовать в разработке математических моделей безопасности компьютерных систем	Знать: - основные методы проверки статистических гипотез; Уметь: - анализировать конкретные прикладные задачи на предмет возможности применения теоретико-вероятностных и статистических методов для их решения; - применять стандартные вероятностные и статистические методы к решению типовых теоретико-вероятностных и статистических задач; Владеть: - навыками поиска научной информации в библиотеках

	и интернете; - опытом работы с реферативной, справочной, периодической и монографической литературой с целью получения новых знаний; - навыками использования библиотек прикладных программ для решения прикладных вероятностных и статистических задач с использованием компьютера.
--	--

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет **3** зачетных единиц, **108** акад. часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости Форма промежуточной аттестации (по семестрам)
			Контактная работа					самостоятельная работа	
			лекции	практические	лабораторные	консультации	аттестационные испытания		
1	Вводная лекция. Основные понятия теории вероятностей. Случайные величины, распределение вероятностей, числовые характеристики.	7	2	1				5	
2	Выработка равномерного распределения случайных чисел. Универсальные тесты для анализа случайных последовательностей.	7	6	3		1		8	
3	Статистическое моделирование случайных последовательностей с заданным законом распределения.	7	6	3		1		7	Самостоятельная работа 1
4	Случайная выборка и перемешивание. Порождение комбинаторных объектов.	7	6	3		1		8	
5	Вероятностные методы в теоретико-числовых задачах и задачах на графах для получения эффективных алгоритмов. Проверка равенства матриц и сравнение строк. Простота числа. Оценки для чисел Рамсея R	7	6	3		1		12	Самостоятельная работа 2

	(k, k). Задача о турнирах, доминирующем множестве. Реберная связность. Гамильтоновы пути. Разбиения графов. Раскраски графов. Независимые множества. Минимальные разрезы.							
6	Метод условных вероятностей. Вероятностные алгоритмы в криптографии. Асимптотические методы и оценки	7	6	3		1		10
							0,3	4,7
	ИТОГО		32	16		5	0,3	54,7
								зачёт

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Вводная лекция – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

Академическая лекция с элементами лекции-беседы – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Элементы лекции-беседы обеспечивают контакт преподавателя с аудиторией, что позволяет привлекать внимание студентов к наиболее важным темам дисциплины, активно вовлекать их в учебный процесс, контролировать темп изложения учебного материала в зависимости от уровня его восприятия.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков по закреплению полученных на лекции знаний.

Консультации – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

В процессе осуществления образовательного процесса по дисциплине используются:
для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- программы Microsoft Office;
- издательская система LaTeX;
- Adobe Acrobat Reader;
- MikTeX (свободно распространяемое ПО);
- Network 15 Mathematica 11 Increment Standard Bundled List Price with Service.

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)

В процессе осуществления образовательного процесса по дисциплине используются:

- Автоматизированная библиотечно-информационная система «БУКИ-NEXT»

http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php

- Электронно-библиотечная система «Юрайт» <https://urait.ru>

- Электронно-библиотечная система «Консультант Студента»

<https://www.studentlibrary.ru/>

- Электронно-библиотечная система «Лань» <http://e.lanbook.com/>

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины

а) основная литература

1. Задачи и упражнения по математической логике, дискретным функциям и теории алгоритмов: учеб. пособие для вузов. / М. М. Глухов, О. А. Козлитин, В. А. Шапошников, А. Б. Шишков; УМО по образованию в обл. информационной безопасности - СПб.: Лань, 2008. - 111 с.
2. И. В. Хрущева, В. И. Щербаков, Д. С. Леванова. Основы математической статистики и теории случайных процессов: учебное пособие — Санкт-Петербург: Лань, 2021. — <https://reader.lanbook.com/book/167790>
3. Г. А. Михайлов, А. В. Войтишек. Статистическое моделирование. Методы Монте-Карло: учебное пособие для вузов — Москва: Издательство Юрайт, 2022. <https://urait.ru/viewer/statisticheskoe-modelirovanie-metody-monte-karlo-494032>
4. Каштанов, В. А. Случайные процессы : учебник и практикум для вузов / В. А. Каштанов, Н. Ю. Энатская. — Москва : Издательство Юрайт, 2023. — 156 с. — (Высшее образование). — ISBN 978-5-534-04482-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/513724>

б) дополнительная литература

1. Ю. В. Русин Алгоритмы статистического моделирования вероятностных распределений - Ярославль, ЯрГУ, 2006.
<http://www.lib.uniyar.ac.ru/edocs/iuni/20060235.pdf>
2. Ермаков С. М. Курс статистического моделирования: Учеб.пособие для вузов. / С.М.Ермаков,Г.А.Михайлов.М-во высш.и сред.спец.образования СССР - М.: Наука, 1976. - 168с.
3. Алон, Н. Вероятностный метод : учебное пособие / Н. Алон, Дж. Спенсер; пер. 2-го англ. изд. - 4-е изд. - Москва : Лаборатория знаний, 2020. - 323 с. Систем. требования: Adobe Reader XI ; экран 10". - ISBN 978-5-00101-672-4. - Текст : электронный // ЭБС "Консультант студента" : [сайт]. - URL : <https://www.studentlibrary.ru/book/ISBN9785001016724.html>

4. Д. Кнут, Искусство программирования, том 2. Получисленные алгоритмы — М.: Издательский дом «Вильямс», 2000.
5. Ермаков С. М. Метод Монте-Карло и смежные вопросы. - М.: Наука, 1975.
6. Соболев И. М. Метод Монте-Карло. / И. М. Соболев - 2-е изд., испр. - М.: Наука, 1972. - 64 с.
7. Феллер В. Введение в теорию вероятностей и ее приложения: В 2-х томах. Т.1. - М.: Мир, 1984.
8. Феллер В. Введение в теорию вероятностей и ее приложения: В 2-х томах. Т.2. - М.: Мир, 1984.

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа и практических занятий (семинаров);
- учебные аудитории для проведения групповых и индивидуальных консультаций,
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания технических средств обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду организации.

Автор(ы):

Доцент, к.ф.-м.н

Д. В. Гринёв

Приложение № 1 к рабочей программе дисциплины «Вероятностные алгоритмы»

Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине

1. Типовые контрольные задания и иные материалы, используемые в процессе текущего контроля успеваемости

Рекомендуемый перечень тем задач индивидуальных заданий для самостоятельных работ

В качестве самостоятельной работы предлагается составить алгоритм и программу для решения индивидуального задания или подготовить выступление перед учебной группой с изложением предложенной преподавателем или самим студентом темы на практическом занятии:

1. Разыграть равномерно распределенную случайную величину конгруэнтным и квадратичным методами для N чисел (значение всех необходимых параметров задаются). Вычислить основные характеристики полученных последовательностей и сравнить их с теоретическими значениями.
2. Применить к последовательности из п. 1 критерий Пирсона сделать вывод о том какая последовательность ближе к равномерному распределению.
3. Применить к последовательности из п. 1 критерий Колмогорова сделать вывод о том какая последовательность ближе к равномерному распределению.
4. Разыграть случайную величину, распределенную по заданному закону используя метод обратных функций. Равномерно распределенную последовательность получить конгруэнтным и квадратичным методами для N чисел. Вычислить основные характеристики полученных последовательностей и сравнить их с теоретическими значениями.
5. Применить к последовательности из п. 1 критерий Пирсона сделать вывод о том какая последовательность ближе к заданному распределению
6. Применить к последовательности из п. 1 критерий Колмогорова сделать вывод о том какая последовательность ближе к заданному распределению.
7. Выработка равномерного распределения случайных чисел.
8. Универсальные тесты для анализа случайных последовательностей.
9. Теоретические тесты.
10. Числовые распределения.
11. Случайная выборка и перемешивание.
12. Порождение комбинаторных объектов.
13. Вероятностные алгоритмы на графах.
14. Вероятностные теоретико-числовые алгоритмы.
15. Сравнение эвристических алгоритмов.
16. Имитационное моделирование.
17. Вероятностные алгоритмы в криптографии.
18. Асимптотические методы и оценки.

2. Список вопросов и (или) заданий для проведения промежуточной аттестации

1. Выработка равномерного распределения случайных чисел.
2. Универсальные тесты для анализа случайных последовательностей.

3. Теоретические тесты.
4. Числовые распределения.
5. Случайная выборка и перемешивание.
6. Порождение комбинаторных объектов.
7. Вероятностные алгоритмы на графах.
8. Вероятностные теоретико-числовые алгоритмы.
9. Сравнение эвристических алгоритмов.
10. Имитационное моделирование.
11. Вероятностные алгоритмы в криптографии.
12. Асимптотические методы и оценки.

Приложение № 2 к рабочей программе дисциплины «Вероятностные алгоритмы»

Методические указания для студентов по освоению дисциплины

Основной формой изложения учебного являются лекции, причем в форме лекции-беседы или мастер-класса. По большинству тем предусмотрены домашние работы, на которых происходит закрепление лекционного материала путем применения его к конкретным задачам и отработка навыков работы по применению различных конструкций языка и структур данных.

Для успешного освоения дисциплины очень важно решение задач, требующих разработки алгоритма и написания программы, как в аудитории, так и самостоятельно в качестве домашних заданий. Примеры решения задач разбираются на лекциях и практических занятиях, при необходимости по наиболее трудным темам проводятся дополнительные консультации. Для решения всех задач необходимо знать и понимать лекционный материал. Поэтому в процессе изучения дисциплины рекомендуется регулярное повторение пройденного лекционного материала. Материал, законспектированный на лекциях, необходимо дома еще раз прорабатывать и при необходимости дополнять информацией, полученной на консультациях, практических занятиях или из учебной литературы.

Большое внимание должно быть уделено выполнению домашней работы. В качестве заданий для самостоятельной работы дома студентам предлагаются задачи, аналогичные разобранным на лекциях и практических занятиях или немного более сложные, которые являются результатом объединения нескольких базовых задач.

Для проверки и контроля усвоения материала в течение обучения при сдаче самостоятельных работ преподаватель задает вопросы, позволяющие выяснить понимание материала. Также проводятся консультации (при необходимости) по разбору заданий для самостоятельной работы, которые вызвали затруднения.

В конце семестра студенты сдают зачет.