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

Кафедра нелинейной динамики

УТВЕРЖДАЮ
Декан математического факультета

Нестеров П.Н.
20 июня 2023 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 12 апреля 2023 г., протокол № 8

Программа одобрена НМК
математического факультета
протокол № 9 от 3 мая 2023 г.

Ярославль

**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**

Дисциплина «ВЕРОЯТНОСТНЫЕ АЛГОРИТМЫ» 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)** | **Индикатор достижения компетенции (код и формулировка)** | **Перечень планируемых результатов обучения** |
|---|---|---|
| **Общепрофессиональные компетенции** | | |
| ОПК-3<br>Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности;<br>математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности; | И-ОПК-3_1<br>Способен использовать в профессиональной деятельности аппарат и методы теории вероятности и математической статистики | ***знать:***<br>−основные понятия теории графов;<br>−вероятностные методы решения задач;<br>−основные методы проверки статистических гипотез;<br>**уметь**:<br>−анализировать конкретные прикладные задачи на предмет возможности применения теоретико-вероятностных и статистических методов для их решения;<br>**владеть**:<br>-навыками поиска научной информации в библиотеках и интернете;<br>−опытом работы с реферативной, справочной, периодической и монографической литературой с целью получения новых знаний; |

| | | |
|---|---|---|
| | И-ОПК-3_2<br>Осуществляет постановку задачи, выбирает способ ее решения | **уметь**:<br>−строить теоретико-вероятностные и статистические модели задач и явлений практического характера по специальности;<br>**владеть:**<br>- навыками научного исследования с применением вероятностно-статистических методов; |
| | И-ОПК-3_3<br>Применяет математический аппарат для решения прикладных и теоретических задач | **уметь**:<br>−применять стандартные вероятностные и статистические методы к решению типовых теоретико-вероятностных и статистических задач;<br>**владеть:**<br>−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<br><br>Форма промежуточной аттестации *(по семестрам)*<br><br>Формы ЭО и ДОТ *(при наличии)* |
|---|---|---|---|---|---|---|---|---|---|
| | | | Контактная работа | | | | | самостоятельная работа | |
| | | | лекции | практические | лабораторные | консультации | аттестационные испытания | | |
| 1 | Вводная лекция. Основные понятия теории вероятностей. Случайные величины, распределение вероятностей, числовые характеристики. | 8 | 2 | 1 | | | | 5 | |
| 2 | Выработка равномерного распределения случайных чисел. Универсальные тесты | 8 | 6 | 3 | | | | 8 | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | для анализа случайных последовательностей. | | | | | | | | |
| 3 | Статистическое моделирование случайных последовательностей с заданным законом распределения. | 8 | 6 | 3 | | 2 | | 7 | Самостоятельная работа 1 |
| 4 | Случайная выборка и перемешивание. Порождение комбинаторных объектов. | 8 | 6 | 3 | | | | 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 (k, k). Задача о турнирах, доминирующем множестве. Реберная связность. Гамильтоновы пути. Разбиения графов. Раскраски графов. Независимые множества. Минимальные разрезы. | 8 | 6 | 3 | | 2 | | 12 | Самостоятельная работа 2 |
| 6 | Метод условных вероятностей.<br>Вероятностные алгоритмы в криптографии. Асимптотические методы и оценки | 8 | 6 | 3 | | | | 10 | |
| | | | | | | 1 | 0,3 | 4,7 | зачёт |
| | **ИТОГО** | | 32 | 16 | | 5 | 0,3 | 54,7 | |

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

Основной образовательной (дидактической) технологией освоения дисциплины предполагается современное традиционное обучение, состоящее из непосредственного (очного) взаимодействия преподавателя и обучающихся на аудиторных занятиях в форме классических традиционных лекций и практических занятий в составе учебных групп, а также из самостоятельной работы обучаемых. При этом не исключается использование в учебном процессе современных компьютерных технологий (слайд-лекции, элементы дистанционного обучения и т.д.).

При выполнении обучаемыми долгосрочного домашнего задания целесообразно сделать основной упор на освоение и применение компьютерных методов. Для этого следует предложить обучаемым самостоятельно (или в рамках дисциплины по выбору) освоить в достаточной степени и затем использовать при решении домашнего задания пакет прикладных математических программ MATHEMATICA и статистический пакет STATISTICA (или SPSS).

Представляется также полезным ориентировать обучаемых на использование в самостоятельной работе вузовских электронно-библиотечных систем учебной литературы и базы научно-технической информации ВИНИТИ РАН через сеть Интернет.

**Консультации** – групповые занятия, являющиеся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты в решении задач, которые возникают у них в процессе самостоятельной работы, обсуждаются результаты решения заданий, выполненных студентами самостоятельно.

В конце семестра предусматривается зачёт.

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

В процессе осуществления образовательного процесса используются:

-программное обеспечение для создания и демонстрации презентаций, иллюстраций и

других учебных материалов:

- Microsoft Windows (в составе Microsoft Imagine Premium Electronic Software Delivery);

- Microsoft OfficeSTD 2013;

- MikTeX (свободно распространяемое ПО).

- Network 15 Mathematica 11 Increment Standard Bundled List Price with Service.

-– для поиска учебной литературы:

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

В процессе осуществления образовательного процесса используются:

- автоматизированная библиотечная информационная система "БУКИ-NEXT" (АБИС "Буки-Next")

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

**а) основная литература**


1. Глухов, М. М. Математическая логика. Дискретные функции. Теория алгоритмов : учебное пособие / М. М. Глухов, А. Б. Шишков. — Санкт-Петербург : Лань, 2021. — 416 с. — ISBN 978-5-8114-1344-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/168441 (дата обращения: 28.01.2022).
2. Хрущева, И. В. Основы математической статистики и теории случайных процессов : учебное пособие / И. В. Хрущева, В. И. Щербаков, Д. С. Леванова. — Санкт-Петербург : Лань, 2021. — 336 с. — ISBN 978-5-8114-0914-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167790 (дата обращения: 28.01.2022)
3. Михайлов, Г. А. Статистическое моделирование. Методы Монте-Карло : учебное пособие для вузов / Г. А. Михайлов, А. В. Войтишек. — Москва : Издательство Юрайт, 2022. — 323 с. — (Высшее образование). — ISBN 978-5-534-11518-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/494032 (дата обращения: 28.01.2022).
4. Каштанов, В. А. Случайные процессы : учебник и практикум для вузов / В. А. Каштанов, Н. Ю. Энатская. — Москва : Издательство Юрайт, 2022. — 156 с. — (Высшее образование). — ISBN 978-5-534-04482-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/491656 (дата обращения: 28.01.2022).


**б) дополнительная литература**


1. Ю.В.Русин, Алгоритмы статистического моделирования вероятностных распределений, Ярославль, ЯрГУ, 2006.
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. / Н. Алон, Дж. Спенсер; пер. с англ. под ред. А. А. Сапоженко - М.: БИНОМ. Лаборатория знаний, 2007. - 320 с.
4. Д. Кнут, Искусство программирования, том 2. Получисленные алгоритмы. : Пер. с англ. — М.: Издательский дом «Вильямс», 2000.
5. Ермаков С. М. Метод Монте-Карло и смежные вопросы. / С. М.Ермаков - 2-е изд.,доп. - М.: Наука, 1975. - 471с.
6. Соболь И. М. Метод Монте-Карло. / И. М. Соболь - 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. / В.Феллер; Пер.с англ - М.: Мир, 1984. - 527с.
8. Феллер В. Введение в теорию вероятностей и ее приложения: В 2-х томах.. Т.2. / В.Феллер; Пер.с англ - М.: Мир, 1984. - 751с.


**в) ресурсы сети «Интернет» (при необходимости)**

**1.** Электронная библиотека учебных материалов ЯрГУ (http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php).

**2.** электронные каталоги Научной библиотеки ЯрГУ им. П.Г. Демидова (http://www.lib.uniyar.ac.ru/opac/bk_one_find.php)

**3.** Электронно-библиотечная система «Университетская библиотека online» (www.biblioclub.ru ).

## 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.
– компьютерный класс (лаборатория информационных технологий) для выполнения домашних заданий с использованием пакетов прикладных программ.

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

Число посадочных мест в лекционной аудитории больше либо равно списочному составу потока, а в аудитории для практических занятий (семинаров) – списочному составу группы обучающихся.

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 (**И-ОПК-3_1 - 3**):

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.

Список вопросов и (или) заданий для проведения промежуточной аттестации (**И-ОПК-3_1)**
2.

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.