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

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ

Декан математического факультета

_____ Нестеров П.Н.

20 июня 2023 г.

Рабочая программа дисциплины

Датчики случайных чисел

Направление подготовки (специальности)
10.04.01 Информационная безопасность

Направленность (профиль)
«Управление информационной безопасностью»

Форма обучения очная

Программа рассмотрена
на заседании кафедры
от 14 апреля 2023 г., протокол № 8

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

Ярославль

1. Цели освоения дисциплины

Целью освоения дисциплины «Датчики случайных чисел» является приобретение обучающимися теоретических и практических знаний в области моделирования случайных величин, помимо криптографии, находящей свое применение в теории массового обслуживания, финансовой математике, в многочисленных задачах физической и химической кинетики, математической физике, математической биологии и других научных направлениях.

2. Место дисциплины в структуре образовательной программы

Данная дисциплина является факультативной дисциплиной. (ФТД.01)

Для освоения данной дисциплины обучающиеся должны владеть аппаратом основных математических дисциплин и дисциплин, связанных с разработкой программного обеспечения.

Для успешного освоения дисциплины «Датчики случайных чисел» обучающиеся на момент начала изучения дисциплины должны быть знакомы со следующими дисциплинами:

«Математический анализ»;
«Теория вероятностей и математическая статистика»;
«Дискретная математика»;
«Информатика»;
«Языки программирования»;
«Методы программирования».

Полученные в курсе «Датчики случайных чисел» знания полезны для изучения дисциплины «Разработка безопасного программного обеспечения».

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
Профессиональные компетенции		
ПК-1 Способен разрабатывать математические модели систем обеспечения информационной безопасности, математически доказывать их соответствие выбранным политикам безопасности	**И-ПК-1_1** Знает основные математические модели систем обеспечения информационной безопасности и математические методы обеспечения информационной безопасности	Знать: - стандартные алгоритмы моделирования дискретного распределения, равномерного дискретного распределения, моделирования случайного вектора и их модификации Уметь: - модифицировать указанные алгоритмы при моделировании определенных распределений, при заданных параметрах в целях повышения скорости работы; - доказывать утверждения и теоремы, изученные в рамках дисциплины, а также их следствия
	И-ПК-1_2 Владеет навыками разработки и реализации алгоритмов решения типовых профессиональных задачна языках высокого уровня	Владеть: - навыками разработки программного обеспечения, реализующего алгоритмы моделирования дискретного распределения, равномерного дискретного распределения, моделирования случайного вектора и их модификации, алгоритмы моделирования полиномиальных и кусочно-полиномиальных плотностей

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 2 зачетных единиц, 72 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						
			лекции	практические	лабораторные	консультации	аттестационные испытания	самостоятельная работа	
1	Генераторы стандартных	2		2				4	

	случайных чисел								
2	Моделирование дискретного распределения (стандартный алгоритм)	2		2		1		8	Задания для самостоятельной работы
3	Специальные алгоритмы моделирования дискретного распределения	2		2				8	Задания для самостоятельной работы
4	Стандартный алгоритм моделирования непрерывной случайной величины	2		2		1		8	
5	Стандартный алгоритм моделирования случайного вектора	2		3				8	Задания для самостоятельной работы
6	Методы суперпозиции и исключения	2		4				8	
							0,3	10,7	Зачет
	ИТОГО			**15**		**2**	**0,3**	**54,7**	

Содержание дисциплины

Тема 1. Генераторы стандартных случайных чисел.

Основные свойства стандартного случайного числа. Два типа генераторов стандартных случайных чисел. Свойства преобразования β = {Ma}. Свойства мультикативного метода вычетов. Тестирование и модификация генераторов случайных и псевдослучайных чисел. Использование датчиков псевдослучайных чисел в параллельных вычислениях.

Тема 2. Моделирование дискретного распределения (стандартный алгоритм).

Стандартный алгоритм. Трудоемкость стандартного алгоритма. Случаи малого и бесконечного числа значений.

Тема 3. Специальные алгоритмы моделирования дискретного распределения.

Моделирование равномерного дискретного распределения. Приведение вероятностей к общему знаменателю. Перераспределение вероятностей (метод Уолкера). Квантильный метод. Бинарный поиск. Метод «мажорантной частоты». Специальные методы моделирования геометрического распределения. Специальные методы моделирования биномиального распределения. Специальные методы моделирования распределения Пуассона.

Тема 4. Стандартный алгоритм моделирования непрерывной случайной величины.

Метод обратной функции распределения. Обобщение метода обратной функции распределения. Составные плотности. Теорема о замене случайных переменных. Конструирование плотностей элементарных распределений.

Тема 5. Стандартный алгоритм моделирования случайного вектора.

Представление плотности распределения случайного вектора в виде произведения условных плотностей. Стандартный алгоритм. Случай независимых компонент. Векторы с марковским свойством. Моделирование случайного вектора с заданными одномерным распределением и корреляционной матрицей (метод повторения).

Тема 6. Методы суперпозиции и исключения.

Метод интегральной суперпозиции. Метод дискретной суперпозиции. Модифицированный метод суперпозиции. Метод суперпозиции для составных плотностей. Общие принципы построения и трудоемкость методов исключения. Мажорантный метод исключения. Специальные методы построения мажорант. Двусторонний метод исключения. Моделирование усеченных распределений.

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:

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

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

В процессе осуществления образовательного процесса 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;

при проведении практических занятий используется программное обеспечение

- MicrosoftVisualStudio.

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

Для поиска учебной литературы библиотеки ЯрГУ используется автоматизированная библиотечно-информационная система «БУКИ-NEXT»
http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php.

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

а) основная литература

1. Михайлов, Г. А. Статистическое моделирование. Методы монте-карло : учебное пособие для бакалавриата и магистратуры / Г. А. Михайлов, А. В. Войтишек. — М. : Издательство Юрайт, 2018. — 371 с. — (Серия : Бакалавр и магистр. Академический курс). — ISBN 978-5-534-06881-8. https://biblio-online.ru/book/8365BAAE-9AD1-41C9-B9AB-FE76294A1034/statisticheskoe-modelirovanie-metody-monte-karlo.

2. Глухов, М.М. Математическая логика. Дискретные функции. Теория алгоритмов [Электронный ресурс] : учебное пособие / М.М. Глухов, А.Б. Шишков. — Электрон. дан. — Санкт-Петербург : Лань, 2012. — 416 с. — Режим доступа: https://e.lanbook.com/book/4041.

б) дополнительнаялитература

1. *Goldreich O.* Foundations of Cryptography Basic Tools / O. Goldreich – 2004, 372 с.

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 практических занятий, оснащенные средствами вычислительной техники, с установленным программным обеспечением MicrosoftVisualStudio;
- учебные аудитории для проведения групповых и индивидуальных консультаций;
- учебные аудитории для проведения текущего контроля;
- 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 к электронной информационно-образовательной среде ЯрГУ.

Автор(ы):

Доцент кафедры КБиММОИ, канд. физ.-мат. наук Д.М. Мурин

Приложение № 1 к рабочей программе дисциплины
«Датчики случайных чисел»

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

Задания для самостоятельной работы

Варианты заданий по теме № 2: «Моделирование дискретного распределения (стандартный алгоритм)».

1. Написать программное обеспечение, реализующее стандартный алгоритм получения случайной величины ξ с конечным числом значений $x_1, x_2, \ldots, x_N$ и распределением вероятностей $\Pr(\xi = x_i) = p_i,\ i = \overline{1,N};\ \ p_i > 0,\ i = \overline{1,N};\ \sum_{i=1}^{N} p_i = 1$. Провести проверку статистических характеристик вырабатываемой программным обеспечением последовательности.
2. Написать программное обеспечение, реализующее стандартный алгоритм получения случайной величины η с конечным числом значений $x_1 = 1, x_2 = 2, \ldots, x_N = N$ и распределением вероятностей $\Pr(\eta = i) = p_i,\ i = \overline{1,N};\ \ p_i > 0,\ i = \overline{1,N};\ \sum_{i=1}^{N} p_i = 1$. Провести проверку статистических характеристик вырабатываемой программным обеспечением последовательности.
3. Написать программное обеспечение, реализующее стандартный алгоритм получения случайной величины ξ с конечным числом значений x_1, x_2 и распределением вероятностей $\Pr(\xi = x_1) = p_1, \Pr(\xi = x_2) = p_2;\ \ p_i > 0,\ i = \overline{1,2};\ p_1 + p_2 = 1$. Провести проверку статистических характеристик вырабатываемой программным обеспечением последовательности.
4. Написать программное обеспечение, реализующее стандартный алгоритм получения случайной величины ξ с бесконечным числом значений $x_1, x_2, \ldots, x_N, \ldots$ и распределением вероятностей $\Pr(\xi = x_i) = p_i,\ i = 1, 2, \ldots;\ \ p_i > 0,\ i = 1, 2, \ldots;\ \sum_{i=1}^{\infty} p_i = 1$. Провести проверку статистических характеристик вырабатываемой программным обеспечением последовательности.

Варианты заданий по теме № 3: «Специальные алгоритмы моделирования дискретного распределения».

1. Написать программное обеспечение, реализующее стандартный алгоритм получения случайной величины ξ с конечным числом значений $x_1, x_2, \ldots, x_N$ и дискретным равномерным распределением вероятностей $\Pr(\xi = x_i) = \dfrac{1}{N},\ i = \overline{1,N}$. Провести проверку статистических характеристик вырабатываемой программным обеспечением последовательности.

2. Написать программное обеспечение, реализующее метод приведения вероятностей к общему знаменателю, для моделирования дискретного равномерного распределения вероятностей. Провести проверку статистических характеристик вырабатываемой программным обеспечением последовательности.
3. Написать программное обеспечение, реализующее метод Уолкра (метод перераспределения вероятностей), для моделирования дискретного равномерного распределения вероятностей. Провести проверку статистических характеристик вырабатываемой программным обеспечением последовательности.
4. Написать программное обеспечение, реализующее квантильный метод, для моделирования дискретного равномерного распределения вероятностей. Провести проверку статистических характеристик вырабатываемой программным обеспечением последовательности.
5. Написать программное обеспечение, реализующее метод бинарного поиска. Провести проверку статистических характеристик вырабатываемой программным обеспечением последовательности.
6. Написать программное обеспечение, реализующее метод мажорантной частоты. Провести проверку статистических характеристик вырабатываемой программным обеспечением последовательности.
7. Написать программное обеспечение, реализующее метод моделирования целочисленной случайной величины, имеющей геометрическое распределение. Провести проверку статистических характеристик вырабатываемой программным обеспечением последовательности.
8. Написать программное обеспечение, реализующее метод моделирования целочисленной случайной величины, имеющей биномиальное распределение. Провести проверку статистических характеристик вырабатываемой программным обеспечением последовательности.
9. Написать программное обеспечение, реализующее метод моделирования целочисленной случайной величины, имеющей распределение Пуассона. Провести проверку статистических характеристик вырабатываемой программным обеспечением последовательности.

Варианты заданий по теме № 5: «Стандартный алгоритм моделирования случайного вектора».

1. Написать программное обеспечение, реализующее стандартный алгоритм моделирования случайного вектора малой размерности. Провести проверку статистических характеристик вырабатываемой программным обеспечением последовательности.
2. Написать программное обеспечение, реализующее стандартный алгоритм моделирования случайного вектора для случая независимых компонент. Провести проверку статистических характеристик вырабатываемой программным обеспечением последовательности.
3. Написать программное обеспечение, реализующее стандартный алгоритм моделирования случайного вектора, обладающего марковским свойством. Провести проверку статистических характеристик вырабатываемой программным обеспечением последовательности.
4. Написать программное обеспечение, реализующее стандартный алгоритм моделирования случайного вектора с заданными одномерным распределением и корреляционной матрицей (метод повторения). Провести проверку статистических характеристик вырабатываемой программным обеспечением последовательности.

Варианты заданий по теме № 6: «Метод суперпозиции».

1. Написать программное обеспечение, реализующее метод дискретной суперпозиции. Провести проверку статистических характеристик вырабатываемой программным обеспечением последовательности.
2. Написать программное обеспечение, реализующее модифицированный метод дискретной суперпозиции. Провести проверку статистических характеристик вырабатываемой программным обеспечением последовательности.

Варианты заданий по теме № 8: «Моделирование полиномиальных и кусочно-полиномиальных плотностей».

1. Написать программное обеспечение, реализующее один из изучаемых методов моделирования кусочно-постоянных плотностей. Провести проверку статистических характеристик вырабатываемой программным обеспечением последовательности.
2. Написать программное обеспечение, реализующее один из изучаемых методов моделирования кусочно-линейных плотностей. Провести проверку статистических характеристик вырабатываемой программным обеспечением последовательности.
3. Написать программное обеспечение, реализующее метод суперпозиции для моделирования полиномиальных плотностей. Провести проверку статистических характеристик вырабатываемой программным обеспечением последовательности.
4. Написать программное обеспечение, моделирующее полиномиальные плотности с использованием порядковых статистик. Провести проверку статистических характеристик вырабатываемой программным обеспечением последовательности.

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

Вопросы к зачету

1. Основные свойства стандартного случайного числа.
2. Два типа генераторов стандартных случайных чисел.
3. Свойства преобразования $\beta = \{Ma\}$.
4. Свойства мультикативного метода вычетов.
5. Тестирование и модификация генераторов случайных и псевдослучайных чисел.
6. Использование датчиков псевдослучайных чисел в параллельных вычислениях.
7. Моделирование дискретного распределения (стандартный алгоритм).
8. Трудоемкость стандартного алгоритма.
9. Случай малого числа значений.
10. Случай бесконечного числа значений.
11. Моделирование равномерного дискретного распределения.
12. Приведение вероятностей к общему знаменателю.
13. Перераспределение вероятностей (метод Уолкера).
14. Квантильный метод.
15. Бинарный поиск.
16. Метод «мажорантной частоты».
17. Специальные методы моделирования геометрического распределения.
18. Специальные методы моделирования биномиального распределения.
19. Специальные методы моделирования распределения Пуассона.

20. Метод обратной функции распределения.
21. Обобщение метода обратной функции распределения.
22. Составные плотности.
23. Теорема о замене случайных переменных. Конструирование плотностей элементарных распределений.
24. Представление плотности распределения случайного вектора в виде произведения условных плотностей.
25. Стандартный алгоритм моделирования случайного вектора.
26. Случай независимых компонент.
27. Случай векторов, обладающих марковским свойством.
28. Моделирование случайного вектора с заданными одномерным распределением и корреляционной матрицей (метод повторения).
29. Метод интегральной суперпозиции.
30. Метод дискретной суперпозиции.
31. Модифицированный метод суперпозиции.
32. Метод суперпозиции для составных плотностей.
33. Общие принципы построения и трудоемкость методов исключения.
34. Мажорантный метод исключения.

Правила выставления оценки на зачете.

В процессе зачета требуется ответить на один из приведенных выше вопросов. На подготовку к ответу дается не менее 1 академического часа.

По итогам зачета выставляется одна из оценок: «зачтено», «не зачтено».

Оценка «Зачтено» выставляется студенту, который демонстрирует владение содержанием материала и понятийным аппаратом теории псевдослучайных генераторов; умеет связывать теорию с практикой. В ответе могут допускаться отдельные неточности (несущественные ошибки), которые исправляются самим студентом после дополнительных и (или) уточняющих вопросов экзаменатора. На часть дополнительных вопросов студент может не дать ответ или дать неверный ответ.

Оценка «Не зачтено» выставляется студенту, который демонстрирует разрозненные, бессистемные знания; беспорядочно и неуверенно излагает материал; не умеет выделять главное и второстепенное, не умеет соединять теоретические положения с практикой; допускает грубые ошибки при определении понятий, вследствие непонимания их существенных и несущественных признаков и связей; дает неполные ответы, логика и последовательность изложения которых имеют существенные и принципиальные нарушения, в ответах отсутствуют выводы. Дополнительные и уточняющие вопросы экзаменатора не приводят к коррекции ответов студента. На основную часть дополнительных вопросов студент затрудняется дать ответ или дает неверные ответы.

Оценка «Не зачтено» выставляется также студенту, который взял экзаменационный билет, но отказалсядать на него ответ.

Приложение № 2 к рабочей программе дисциплины
«Датчики случайных чисел»

Методические указания для студентов по освоению дисциплины

Учебным планом на изучение дисциплины «Датчики случайных чисел» отводится один семестр. В конце семестра в качестве итогового контроля предусмотрен зачет. В процессе изучения дисциплины выполняются пять заданий для самостоятельной работы.

При изучении учебного материала по дисциплине «Датчики случайных чисел» следует обратить особое внимание на тот факт, что практические занятия обязательно должны быть подкреплены самостоятельной работой. Это связано с тем, что дисциплина «Датчики случайных чисел» является разделом прикладной математики. Математический аппарат, изучаемый в рамках дисциплины, имеет непосредственное прикладное назначение. Следовательно, для полноценного освоения изучаемого материала, обучающемуся необходимо получить самостоятельный опыт его практического применения.

Основную роль для анализа и контроля качества усвоения материала играют задания для самостоятельной работы. В качестве заданий для самостоятельной работы обучающимся предлагаются задачи по разработке программного обеспечения, которые должны позволить студенту переосмыслить изученные понятия и методы, применить их на практике. Решения заданий должны быть подготовлены, оформлены в виде программ с подробными комментариями и представлены в установленные сроки.

Для повышения качества усвоения теоретического материала, приобретенных практических навыков работы с изучаемым в рамках дисциплины математическим аппаратом проводятся консультации по разбору заданий для самостоятельной работы. Также на консультациях, возможно повторно, разъясняются вопросы, вызвавшие затруднения у обучающихся.

По окончанию семестра изучения дисциплины обучающиеся сдают зачет. Зачет принимается по билетам, каждый из которых включает в себя один теоретический вопрос. На самостоятельную подготовку к зачету выделяется 2 дня.

Опыт преподавания дисциплины «Датчики случайных чисел» говорит о высокой сложности ее самостоятельного изучения для обучающегося в первую очередь ввиду необходимости обладания, с одной стороны, достаточно глубокими знаниями теории вероятностей и математической статистики, а, с другой стороны, продвинутым уровнем освоения дисциплин, связанных с разработкой программного обеспечения. Излагаемый на материал часто является нетривиальным и требует опыта практической реализации. Поэтому посещение всех аудиторных занятий является обязательным.