

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Волгоградский государственный технический университет»



УТВЕРЖДАЮ

Первый проректор

С. В. Кузьмин

« 25 » декабря 2024 г.

ПРОГРАММА

вступительного экзамена в аспирантуру по группе научных специальностей
1.2. Компьютерные науки и информатика

Волгоград 2024

Раздел 1 . Математическое моделирование, численные методы и комплексы программ

1. Элементы теории множеств. Понятие множества, операции над множествами. Конечные и бесконечные множества. Бинарные отношения. Понятие мощности множества. Эквивалентность множеств Упорядоченность. Аксиомы выбора. Нечеткие множества. Основные операции. Нечеткая логика.

2. Математическое программирование: основы теории и численные методы. Методы безусловной минимизации: метод наискорейшего спуска, метод сопряженных градиентов. Линейное программирование. Типовые задачи линейного программирования. Целочисленное программирование. Метод отсекающих плоскостей и метод ветвей и границ в целочисленном программировании.

3. Элементы теории вероятностей и случайных процессов. Пространство элементарных событий. Случайные величины и функции распределения. Независимость событий и случайных величин. Испытания Бернулли. Числовые характеристики случайных величин. Закон больших чисел. Центральная предельная теорема. Теорема Пуассона. Дискретные цепи Маркова и их классификация.

4. Понятие о системном подходе. Выделение системы из среды. Понятие целостности. Системные понятия: вход, выход, обратная связь, ограничения. Описание систем. Общая схема системного подхода. Построение моделей. Критерии и альтернативы. Методы моделирования в системном анализе. Оптимизационные и имитационные модели. Детерминированные и стохастические модели. Языки моделирования.

5. Многокритериальная оптимизация. Виды оценок и шкал. Построение множества эффективных вариантов. Важность критериев. Компенсация критериев по относительной важности критериев. Свертка критериев. Векторная оптимизация. Гарантированные результаты. Условия парето-оптимальности. Приближенное построение паретовской границы.

6. Оценки, статистические решения, проверка гипотез. Оценки параметров статистических объектов, линейная регрессия. Метод наименьших квадратов.

7. Постановки задач оптимального управления для непрерывных и дискретных систем. Динамическое программирование. Принцип оптимальности Беллмана. Уравнение Беллмана для непрерывных и дискретных задач оптимального управления. Принцип максимума Л.С. Понтрягина для непрерывных и дискретных управляемых систем.

Рекомендуемая литература:

1. Самарский А.А., Михайлов А.П. Математическое моделирование. М.: Физматлит, 1997.

2. Математическое моделирование / Под ред. А.Н. Тихонова, В.А. Садовниченко и др. М.: Изд-во МГУ, 1993.

3. Вентцель Е.С. Исследование операций. М.: Сов. радио, 1972.

4. Нечеткие множества в моделях управления и искусственного интеллекта/ Под ред. Д.А. Поспелова. М.: Наука, Физматлит, 1986.
5. Моисеев Н.Н. Элементы теории оптимальных систем. М.: Наука, 1975.
6. Моисеев Н.Н., Иванилов Ю.П., Столяров. Методы оптимизации. М.: Наука, 1978.
7. Бусленко Н.П. Моделирование сложных систем. М.: Наука, 1978.
8. Пытьев, Ю. А. Математические методы интерпретации эксперимента / Ю. А. Пытьев. – М.: Высш. шк., 1989. – 351 с.

Раздел 2. Искусственный интеллект и машинное обучение

1. Естественные-научные основы и методы искусственного интеллекта. Методы и алгоритмы моделирования мыслительных процессов: рассуждений, аргументации, распознавания и классификации, формирования понятий.
2. Этические проблемы, связанные с созданием и внедрением ИИ-систем, ожидаемые социальные и экономические последствия.
3. Численные методы оптимизации: методы Ньютона и секущей, методы покоординатного и градиентного спуска. Улучшение сходимости градиентных методов.
4. Понятие искусственной нейронной сети. Типы нейронных сетей. Понятие стохастического градиента для обучения нейронной сети. Архитектуры ИНС и гиперпараметры.
5. Многослойный перцептрон. Сверточные нейронные сети. Средства реализации в высокоуровневых языках программирования.
6. Генеративные методы машинного обучения. Генеративно-состязательные сети. Вариационные автокодировщики. Байесовские сети. Принципы работы, оценка качества. Примеры и средства реализации.
7. Определение вероятности. Вероятностная модель и вероятностное пространство. Вероятность случайного события и методы ее статистического оценивания по выборке.
8. Понятие регрессии. Типы регрессии. Методы численного решения задач регрессии. Способы задания целевой функции в задаче регрессии. Метод наименьших квадратов. Методы машинного обучения для решения задач регрессии. Средства реализации в высокоуровневых языках программирования.
9. Случайные процессы и временные ряды. Понятие стационарности. Ковариационная (корреляционная функция). Теорема Карунена-Лоэва. Спектральная плотность случайных процессов.
10. Графы. Основные понятия: ориентированность графа, степени вершины, связность, цепи и циклы (Эйлеров, Гамильтонов). Способы представления графа: матрицы и списки инцидентности и смежности. Важные частные случаи: деревья, направленные ациклические графы, двудольные графы.
11. Алгоритмы на графах. Алгоритмы обхода (поиска на) графах. Обнаружение кратчайшего пути и минимального цикла в графе. Построение остовного дерева.
12. Построение списка решений и дерева решений. Редукция деревьев решений. Понятие бэггинга и бустинга для деревьев решений. Случайный лес и способы его построения. Средства реализации в высокоуровневых языках программирования.
13. Основные понятия машинного обучения. Отличие машинного обучения от статистики. Обучение с учителем и без учителя. Методы и средства формирования массивов данных и прецедентов, включая «большие данные».

14. Многоагентные системы и распределенный ИИ. Средства и примеры реализации.
15. Обучение с подкреплением. Модели агентов и отклика среды. Задачи, решаемые обучением с подкреплением. Средства реализации в высокоуровневых языках программирования. Примеры реализации.
16. Цикл обучения. Понятия обучающей и тестовой выборки. Отложенная выборка. Кросс-валидация. Понятия недообучения и переобучения.
17. Метрики качества алгоритмов машинного обучения. Оценка качества и эффективности алгоритмических и программных решений для систем искусственного интеллекта и машинного обучения. Методики сравнения и выбора алгоритмических и программных решений при многих критериях.
18. Понятия классификации и кластеризации. Метрические, иерархические, вероятностные методы классификации и кластеризации. Оценка качества классификации и кластеризации. Средства реализации в высокоуровневых языках программирования.
19. Методы снижения размерности данных. Метод главных компонент. Корреляционный и факторный анализ. Нелинейные методы снижения размерности. Средства реализации в высокоуровневых языках программирования.
20. Принцип повышения размерности пространства. Метод опорных векторов. Понятие и свойства ядра. Метод Kernel-Trick. Средства реализации в высокоуровневых языках программирования.
21. Способы представления знаний. Модели графов знаний. Полнота графов знаний. Методы прямого и обратного вывода по графам знаний. Онтологическая модель и средства ее реализации.
22. Экспертные методы в принятии решений. Принятие решений при многих критериях. Множество Парето. Экспертные системы поддержки принятия решений.
23. Методы машинного обучения для анализа текстовой информации. Методы генерации текстов. Чат-боты. Большие языковые модели. Средства реализации в высокоуровневых языках программирования.
24. Управление с использованием систем искусственного интеллекта и методов машинного обучения, в том числе управление роботами, автомобилями, БПА.
25. Методы и средства реализации систем компьютерного зрения.

Раздел 3. Кибербезопасность

1. Информация, сообщение, информационные системы и процессы как объекты информационной безопасности. Основные свойства информации. Мера количества информации. Энтропия. Модели стоимости информации.
2. Случайные события. Полная группа событий. Зависимые и независимые случайные события. Вероятность случайного события. Условная вероятность. Формула полной вероятности. Теорема Байеса.
3. Случайные величины и их характеристики: функция распределения, моменты, характеристические функции. Дискретные и непрерывные случайные величины. Биномиальный закон распределения. Нормальный закон распределения. Центральная предельная теорема Ляпунова.
4. Псевдослучайные последовательности: области применения в задачах обеспечения информационной безопасности; методы получения; способы оценки качества.
5. Основные задачи математической статистики: точечная оценка, построение доверительного интервала, различение статистических гипотез.
6. Основы теории чисел. Понятие группы, кольца, поля.
7. Криптографические методы защиты информации. Основные постулаты криптографии. Исторические шифры.
8. Криптоаналитика. Теоретическая, практическая и временная стойкость системы криптографической защиты. Современные поточные и блочные алгоритмы шифрования. Обоснование надежности криптографической защиты.
9. Методы и протоколы защиты информации от несанкционированного использования и копирования.
10. Классификация вредоносных программ. Классические определения четырех основных типов вредоносных программ. Методы борьбы с вредоносными программами.
11. Системы симметричного шифрования. Вопросы генерации и распределения ключей.
12. Системы асимметричного шифрования, открытый ключ, электронная подпись. Атака «человек посередине».
13. Современная криптография с открытым ключом: основные идеи, концепция. Криптосистемы RSA, El Gamal, рюкзака.
14. Электронная цифровая подпись: основные идеи, концепции, Подпись RSA, El Gamal. Отрицаемая и неотрицаемая подпись.
15. Криптографические протоколы. Протоколы аутентификации без разглашением, протокол подбрасывания монетки.
16. Протоколы аутентификации без разглашения.
17. Стеганография. Основные свойства, подходы к реализации, использование алгоритмов LSB и психовизуальных/психоакустических эффектов. Атаки на стеганографические методы. Понятие цифрового водяного знака.
18. Использование хэш-функций. Одноразовые подписи на цепочках Лампорта и на дереве Меркле.
19. Технология блокчейн. Принцип работы. Публичный и приватный блокчейн.
20. Постквантовая криптография как отдельный раздел криптографии. Основные концепции и идеи.

21. Проблемы безопасности сетевых технологий. Сетевая модель OSI/ISO. Уровни модели OSI.
22. Риск информационной безопасности: понятие; задача управления рисками; методологические основы и инструментальные средства оценки рисков информационной безопасности, остаточные риски.
23. Состязательное и вредоносное машинное обучение. Методы противодействия атакам на нейросети и машинное обучение.
24. Основные угрозы безопасности веб-ресурсов. OWASP Top 10: описание и механизмы защиты.
25. Методы и методики тестирования на проникновение; Основы деятельности SOC в организации. Понятия Red team, Blue team, Purple team; MITRE ATT&CK Framework.

2. Литература, рекомендуемая для подготовки к вступительному экзамену

1. Остроух, А. В. Системы искусственного интеллекта: монография / А. В. Остроух, Н. Е. Суркова. - Санкт-Петербург: Лань, 2019. - 228 с. - ISBN 978-5-8114-3427-5. - Текст: электронный // Лань: электронно-библиотечная система. - URL: <https://e.lanbook.com/book/113401> - Режим доступа: для авториз. пользователей.
2. Душкин, Р. В. Искусственный интеллект / Р. В. Душкин. - Москва: ДМК Пресс, 2019. - 280 с. - ISBN 978-5-97060-787-9. - Текст: электронный // Лань: электронно-библиотечная система. - URL: <https://e.lanbook.com/book/131703>. - Режим доступа: для авториз. пользователей.
3. Блюмин, А. М. Проектирование систем интеллектуального обслуживания: учебник / А. М. Блюмин. - Москва: Дашков и К, 2018. - 346 с. - ISBN 978-5-394-02936-3. - Текст: электронный // Лань: электронно-библиотечная система. - URL: <https://e.lanbook.com/book/110759> - Режим доступа: для авториз. пользователей.
4. И. С. Николаев, О. В. Митренина, Т. М. Ландо. Прикладная и компьютерная лингвистика. М.: Издательская группа URSS, 2017. Текст : электронный // Лань : электронно-библиотечная система. - URL: <https://e.lanbook.com/book/75506> (дата обращения: 31.03.202) <http://urss.ru/cgi-bin/db.pl?blang=ru&id=213156&lang=Ru&page=Book>
5. Николенко С. И. , Кадури А., Архангельская Е. В., Глубокое обучение. Погружение в мир нейронных сетей / Питер, 2018 / ISBN: 978-5-496-02536-2
6. Рейнхард К., Компьютерное зрение. Теория и алгоритмы. / пер. Слинкин А. А., / МК-Пресс, 2019 / ISBN: 978-5-97060-702-2
7. Селянкин В.В., Компьютерное зрение. Анализ и обработка изображений. Учебное пособие ЭБС Лань, 2019, ISBN 978-5-8114-3368-1
8. Шапиро Л., Стокман Дж., Компьютерное зрение / Лаборатория знаний, 2020 / ISBN 978-5-00101-696-0
9. Хултен, Д. Разработка интеллектуальных систем: руководство / Д. Хултен ; перевод с английского В. С. Яценкова. - Москва: ДМК Пресс, 2019. - 284 с. - ISBN 978-5-97060-760-2. - Текст: электронный // Лань: электронно-

библиотечная система. - URL: <https://e.lanbook.com/book/131705> - Режим доступа: для авториз. пользователей.

10. Боярский К.К. Введение в компьютерную лингвистику ИТМО, 2013 - URL: <https://e.lanbook.com/book/70822>

11. Лабораторный практикум по машинному обучению и анализу данных. ВолгГТУ. - Волгоград : ВолгГТУ, 2020. - 32 с.

12. Шитиков В.К., Мастицкий С.Э. Классификация, регрессия и другие алгоритмы Data Mining с использованием R. - URL: <https://ranalytics.github.io/data-mining/>

13. Прохоренок Н., OpenCV и Java. Обработка изображений и компьютерное зрение / БХВ-Петербург, 2018 / ISBN: 978-5-9775-3955-5

14. Солем Я. Э., Программирование компьютерного зрения на языке Python / ДМК Пресс 2012 / ISBN: 978-5-97060-200-3

15. Форсайт Дэвид А., П. Жан, Компьютерное зрение. Современный подход. Вильямс, 2004, ISBN:5-8459-0542-7

16. Хайкин С., Нейронные сети. Полный курс, Вильямс, 2019, ISBN:978-5-8459-2069-0

17. R. Szeliski, Computer Vision: Algorithms and Applications, 2nd ed. / [электронный ресурс] <https://szeliski.org/Book/>

18. Паласиос, Х. Unity 5.x. Программирование искусственного интеллекта в играх / Х. Паласиос ; перевод с английского Р. Н. Рагимова. - Москва: ДМК Пресс, 2017. - 272 с. - ISBN 978-5-97060-436-6. - Текст: электронный // Лань: электронно-библиотечная система. - URL: <https://e.lanbook.com/book/97348> - Режим доступа: для авториз. пользователей.

19. Москвитин, А. А. Данные, информация, знания: методология, теория, технологии: монография / А. А. Москвитин. - Санкт-Петербург: Лань, 2019. - 236 с. - ISBN 978-5-8114-3232-5. - Текст: электронный // Лань: электронно-библиотечная система. - URL: <https://e.lanbook.com/book/113937> - Режим доступа: для авториз. пользователей.

20. Гласснер, Э. Глубокое обучение без математики: Э. Гласснер; перевод с английского В. А. Яроцкого. - Москва: ДМК Пресс, [б. г.]. - Том 1: Основы - 2019. - 578 с. - ISBN 978-5-97060-701-5. - Текст: электронный // Лань: электронно-библиотечная система. - URL: <https://e.lanbook.com/book/131696> - Режим доступа: для авториз. пользователей.

21. Ростовцев, В. С. Искусственные нейронные сети : учебник / В. С. Ростовцев. - Санкт-Петербург: Лань, 2019. - 216 с. - ISBN 978-5-8114-3768-9. - Текст: электронный // Лань: электронно-библиотечная система. - URL: <https://e.lanbook.com/book/122180>. - Режим доступа: для авториз. пользователей.

22. Макшанов, А. В. Технологии интеллектуального анализа данных: учебное пособие / А. В. Макшанов, А. Е. Журавлев. - 2-е изд., стер. - Санкт-Петербург: Лань, 2019. - 212 с. - ISBN 978-5-8114-4493-9. - Текст : электронный // Лань : электронно-библиотечная система. - URL: <https://e.lanbook.com/book/120063>. - Режим доступа: для авториз. пользователей.

23. Michael Huth, Mark Ryan, Logic in Computer Science. Modelling and Reasoning about Systems, 2nd edition [Электронный ресурс]. – [2020]. – Режим

доступа: <https://www.cambridge.org/core/books/logic-in-computer-science/9022E2BE5E7C9F20D259F4A83986236C#fndtn-contents>

24. Чио, К. Машинное обучение и безопасность: руководство / К. Чио, Д. Фримэн ; перевод с английского А. В. Снастина. - Москва: ДМК Пресс, 2020. - 388 с. - ISBN 978-5-97060-713-8. - Текст: электронный // Лань: электронно-библиотечная система. - URL: <https://e.lanbook.com/book/131707>- Режим доступа: для авториз. пользователей.

25. Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. - Санкт-Петербург : Лань, 2021. - 324 с. - ISBN 978-5-8114-6738-9. - Текст : электронный // Лань : электронно-библиотечная система. - URL: <https://e.lanbook.com/book/165837> (дата обращения: 14.10.2021).

26. Защита информации в центрах обработки данных : учебное пособие / И. А. Ушаков, В. А. Десницкий, А. А. Чечулин [и др.]. - Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2019. - 92 с. - Текст : электронный // Лань : электронно-библиотечная система. - Режим доступа: <https://e.lanbook.com/book/180085> (дата обращения: 10.10.2021).

27. Лукша, М. Kubernetes в действии / М. Лукша ; перевод с английского А. В. Логунов. - Москва : ДМК Пресс, 2019. - 672 с. - ISBN 978-5-97060-657-5. - Текст : электронный // Лань : электронно-библиотечная система. - URL: <https://e.lanbook.com/book/131688> (дата обращения: 14.10.2021).

28. Журавлев, А. Е. Инфокоммуникационные системы. Аппаратное обеспечение : учебник для вузов / А. Е. Журавлев, А. В. Макшанов, А. В. Иванищев. - 2-е изд., стер. - Санкт-Петербург : Лань, 2021. - 392 с. - ISBN 978-5-8114-8514-7. - Текст : электронный // Лань : электронно-библиотечная система. - URL: <https://e.lanbook.com/book/176657> (дата обращения: 14.10.2021). - Режим доступа: для авториз. пользователей.

29. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Д. П. Зегжда, Е. Б. Александрова, М. О. Калинин [и др.]. - Москва : Научно-техническое издательство "Горячая линия-Телеком", 2021. - 560 с. - ISBN 978-5-9912-0827-7.

30. Келдыш, Н. В. Информационная безопасность. Защита информации на объектах информатизации / Н. В. Келдыш. - Москва : Общество с ограниченной ответственностью "Издательство "Мир науки", 2022. - 260 с. - ISBN 978-5-907603-01-1.

31. Швечкова, О. Г. Информационная безопасность : Стандарты и документы / О. Г. Швечкова, С. И. Бабаев. Том Часть 2. - Москва : Курс, 2021. - 144 с. - ISBN 978-5-907352-68-1.

32. Сухостат, В. В. Информационная безопасность : Учебное пособие / В. В. Сухостат. - Санкт-Петербург : Санкт-Петербургский государственный экономический университет, 2021. - 98 с. - ISBN 978-5-7310-5584-0.

33. Солодянников, А. В. Информационная безопасность автоматизированных систем / А. В. Солодянников. - Санкт-Петербург : Санкт-Петербургский государственный экономический университет, 2020. - 108 с. - ISBN 978-5-7310-5001-2.