Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)

Институт прикладной математики и компьютерных наук

УТВЕРЖДЕНО:
Директор
А. В. Замятин

Рабочая программа дисциплины

Нейронные сети

по направлению подготовки / специальности

10.05.01 Компьютерная безопасность

Направленность (профиль) подготовки/ специализация:
Анализ безопасности компьютерных систем

Форма обучения
Очная

Квалификация
Специалист по защите информации

Год приема
2024

СОГЛАСОВАНО:
Руководитель ОП
В.Н. Тренькаев

Председатель УМК
С.П. Сущенко

Томск – 2024

1. Цель и планируемые результаты освоения дисциплины

Целью освоения дисциплины является формирование следующих компетенций:

ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства.

ОПК-2 Способен применять программные средства системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности.

ОПК-3 Способен на основании совокупности математических методов разрабатывать, обосновывать и реализовывать процедуры решения задач профессиональной деятельности.

ПК-2 Способен разрабатывать требования к программно-аппаратным средствам защиты информации компьютерных систем и сетей.

Результатами освоения дисциплины являются следующие индикаторы достижения компетенций:

ИОПК-1.1 Учитывает современные тенденции развития информационных технологий в своей профессиональной деятельности

ИОПК-2.3 Формулирует предложения по применению программных средств системного и прикладного назначений, в том числе отечественного производства, используемых для решения задач профессиональной деятельности

ИОПК-3.2 Осуществляет применение основных понятий, фактов, концепций, принципов математики и информатики для решения задач профессиональной деятельности

ИОПК-3.3 Выявляет научную сущность проблем, возникающих в ходе профессиональной деятельности, и применяет соответствующий математический аппарат для их формализации, анализа и выработки решения

ИПК-2.2 Разрабатывает математические модели, реализуемые в средствах защиты информации

ИПК-2.3 Проводит исследования с целью нахождения наиболее целесообразных практических решений по обеспечению защиты информации

2. Задачи освоения дисциплины

– Освоить аппарат построения интеллектуальных систем на базе искусственных нейронных сетей.

– Научиться применять понятийный аппарат интеллектуальных систем с использованием инструментария библиотек Python, R, публичных облачных сервисов, оценивать эффективность их работы и внедрять в приложения для решения практических задач профессиональной деятельности.

3. Место дисциплины в структуре образовательной программы

Дисциплина относится к Блоку 1 «Дисциплины (модули)».

Дисциплина относится к части образовательной программы, формируемой участниками образовательных отношений, предлагается обучающимся на выбор. Дисциплина входит в «Модуль «Введение в искусственный интеллект».

4. Семестр(ы) освоения и форма(ы) промежуточной аттестации по дисциплине

Седьмой семестр, экзамен

5. Входные требования для освоения дисциплины

Для успешного освоения дисциплины требуются компетенции, сформированные в ходе освоения образовательных программ предшествующего уровня образования.

Для успешного освоения дисциплины требуются результаты обучения по следующим дисциплинам: «Статистические методы машинного обучения», «Введение в интеллектуальный анализ данных».

6. Язык реализации

Русский

7. Объем дисциплины

Общая трудоемкость дисциплины составляет 4 з.е., 144 часов, из которых:
-лекции: 32 ч.
-практические занятия: 16 ч.
в том числе практическая подготовка: 16 ч.
Объем самостоятельной работы студента определен учебным планом.

8. Содержание дисциплины, структурированное по темам

Тема 1. Основы нейрокомпьютерных вычислений.

Основные положения нейросетевых вычислений. Основы проектирования нейросетевых архитектур.

Тема 2. Нейронные сети встречного распространения.

Настройка архитектуры и алгоритмы настройки нейронных сетей встречного распространения. Построение нейросетевого регрессора.

Тема 3. Алгоритмы оптимизации в обучении нейросетевых моделей.

Оптимизаторы обучения нейронных сетей. Исследование архитектур и оптимизаторов нейронной сети – классификатора для повышения её эффективной работы.

Тема 4. Рекуррентные нейронные сети.

Нейронные сети с обратными связями. Настройка рекуррентной нейросети для исследования сигналов

Тема 5. Сверточные нейронные сети.

Сверточные нейронные сети и автоэнкодеры. Исследование изображений сверточными нейронными сетями.

Тема 6. Обучение без учителя и обучение с подкреплением в нейросетевых моделях.

Нейронные сети, обучающиеся без учителя и с подкреплением. Выделение групп объектов с помощью самоорганизующихся нейронных сетей.

Тема 7. Визуализация и объяснимость нейронных сетей.

Визуализация и объяснимость нейросетевых моделей. Визуализация структуры и процесса активации нейронной сети.

Тема 8. Память нейросетевых моделей.

Хранение ассоциаций и управление памятью в нейросетевых моделях. Построение адаптивных нейронных сетей.

9. Текущий контроль по дисциплине

Текущий контроль по дисциплине проводится путем контроля посещаемости, проведения контрольных работ, тестов по лекционному материалу, проверки выполнения практических заданий, и фиксируется в форме контрольной точки не менее одного раза в семестр.

Практическая подготовка оценивается по результатам выполненных практических работ.

Оценочные материалы текущего контроля размещены на сайте ТГУ в разделе «Информация об образовательной программе» - https://www.tsu.ru/sveden/education/eduop/.

10. Порядок проведения и критерии оценивания промежуточной аттестации

Экзамен в седьмом семестре проводится в письменной форме по билетам. Экзаменационный билет состоит из трех частей. Продолжительность экзамена 1,5 часа.

Оценочные материалы для проведения промежуточной аттестации размещены на сайте ТГУ в разделе «Информация об образовательной программе» - https://www.tsu.ru/sveden/education/eduop/.

11. Учебно-методическое обеспечение

а) Электронный учебный курс по дисциплине в LMS IDO
- https://lms.tsu.ru/course/view.php?id=35025

б) Оценочные материалы текущего контроля и промежуточной аттестации по дисциплине.

12. Перечень учебной литературы и ресурсов сети Интернет

а) основная литература:

– Christopher M. Bishop, Hugh Bishop. Deep Learning. Foundations and Concepts. Springer. – 2024. ISBN 978-3-031-45467-7. https://doi.org/10.1007/978-3-031-45468-4 – 649 p.

– Suman Kalyan Adari, Sridhar Alla. Beginning Anomaly Detection Using Python-Based Deep Learning: Implement Anomaly Detection Applications with Keras and PyTorch, Second Edition. Apress. – 2024. ISBN-13 (pbk): 979-8-8688-0007-8. https://doi.org/10.1007/979-8-8688-0008-5 – 529 p.

– Ivan Gridin. Automated Deep Learning Using Neural Network Intelligence: Develop and Design PyTorch and TensorFlow Models Using Python. Apress. – 2022. ISBN-13 (pbk): 978-1-4842-8148-2. https://doi.org/10.1007/978-1-4842-8149-9 – 384 p.

– Шолле Франсуа. Глубокое обучение на Python. 2-е межд. издание. — СПб.: Питер, 2023. — 576 с.: ил. — (Серия «Библиотека программиста»). ISBN 978-5-4461-1909-7

– Ферлитш Э. Шаблоны и практика глубокого обучения / пер. с англ. А. В. Логунова. – М.: ДМК Пресс, 2022. – 538 с.: ил. ISBN 978-5-93700-113-9

б) дополнительная литература:

– Douglas J. Santry. Demystifying Deep Learning. An Introduction to the Mathematics of Neural Networks. The Institute of Electrical and Electronics Engineers, Inc. IEEE Press Wiley – 2024. Hardback ISBN: 9781394205608 – 247 p.

– Ivan Vasilev. Python Deep Learning. Packt Publishing. – 2023. ISBN 978-1-83763-850-5 – 345 p.

– Simon J.D. Prince. Understanding Deep Learning. The MIT Press, https://mitpress.mit.edu. – 2024. – 527 p.

– Daniel A.Roberts, Sho Yaida, Boris Hanin. The Principles of Deep Learning Theory. Cambridge University Press. – 2022. ISBN 9781316519332. DOI: 10.1017/9781009023405. – 460 p.

– Стивенс Эли, Антига Лука, Виман Томас. PyTorch. Освещая глубокое обучение. — СПб.: Питер, 2022. — 576 с.: ил. —(Серия «Библиотека программиста»). ISBN 978-5-4461-1945-5

– Тушан Ганегедара. Обработка естественного языка с TensorFlow / пер. с анг. В. С. Яценкова. – М.:ДМК Пресс, 2020. – 382 с.: ил. ISBN 978-5-97060-756-5

в) ресурсы сети Интернет:

– The AI community building the future. The platform where the machine learning community collaborates on models, datasets, and applications. – https://huggingface.co/

– OpenAI. – https://openai.com/

– Tensorflow. An end-to-end platform for machine learning. – https://www.tensorflow.org/

– PyTorch documentation. – https://pytorch.org/

– IBM. What is deep learning? – https://www.ibm.com/topics/deep-learning

13. Перечень информационных технологий

а) лицензионное и свободно распространяемое программное обеспечение:

– Microsoft Office Standart 2013 Russian: пакет программ. Включает приложения: MS Office Word, MS Office Excel, MS Office PowerPoint, MS Office On-eNote, MS Office Publisher, MS Outlook, MS Office Web Apps (Word Excel MS PowerPoint Outlook);

– публично доступные облачные технологии (Google Docs, Google Colab, Яндекс диск).

- Пакет Anaconda
- Средства языков программирования и анализа данных R и Python
- Библиотеки для машинного и глубокого обучения: Scikit-learn, NumPy, Matplotlib.pyplot, Seaborn, PyTorch, Keras/TensorFlow, OpenAI Gym.

б) информационные справочные системы:

– Электронный каталог Научной библиотеки ТГУ – http://chamo.lib.tsu.ru/search/query?locale=ru&theme=system

– Электронная библиотека (репозиторий) ТГУ – http://vital.lib.tsu.ru/vital/access/manager/Index

– ЭБС Лань – http://e.lanbook.com/

– ЭБС Консультант студента – http://www.studentlibrary.ru/

– Образовательная платформа Юрайт – https://urait.ru/

– ЭБС ZNANIUM.com – https://znanium.com/

– ЭБС IPRbooks – http://www.iprbookshop.ru/

14. Материально-техническое обеспечение

Аудитории для проведения занятий лекционного типа.

Аудитории для проведения занятий семинарского типа, индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы, оснащенные компьютерной техникой и доступом к сети Интернет, в электронную информационно-образовательную среду и к информационным справочным системам.

Аудитории для проведения занятий лекционного и семинарского типа индивидуальных и групповых консультаций, текущего контроля и промежуточной аттестации в смешенном формате («Актру»).

15. Информация о разработчиках

Аксёнов Сергей Владимирович, к.т.н., кафедра теоретических основ информатики (ТОИ) Института прикладной математики и компьютерных наук (ИПМКН) Национальный исследовательский Томский государственный университет (НИ ТГУ), доцент каф. ТОИ