МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«_8_» _08_____ 2023 г.

Математические проблемы обеспечения информационной безопасности

Методические указания по организации самостоятельной работы по дисциплине «Математические проблемы обеспечения информационной безопасности» для студентов направления подготовки 10.04.01 «Информационная безопасность»

Курск 2023

УДК 004.773.5

Составители: Кулешова Е.А.

Рецензент

Кандидат технических наук, доцент кафедры
вычислительной техники А.В. Киселев

Математические проблемы обеспечения информационной безопасности: методические указания для самостоятельной работы / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 13 с.: Библиогр.: с. 13.

Содержат сведения по вопросам самостоятельной работы на протяжении изучения дисциплины. Указывается порядок выполнения самостоятельных работ, содержание работ.

Предназначены для студентов направления подготовки 10.04.01 «Информационная безопасность».

Текст печатается в авторской редакции
Подписано в печать . Формат 60х84 1/16.
Усл. печ.л. . Уч. –изд.л. .Тираж 50 экз. Заказ .
Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Введение

Дисциплина "Прикладные математические задачи информационной безопасности" является важным курсом для тех, кто стремится понять и применить математические алгоритмы и методы в области обеспечения безопасности информации. В данном обзоре я рассмотрю основные разделы этой дисциплины: Введение, Искусственные нейронные сети, Алгоритмы обучения нейронных сетей, Многослойные сети с обратным распространением информации и Нейронные сети в защите информации.

Введение

В начале курса студенты ознакамливаются с основными понятиями информационной безопасности и ее значением в современном мире. Они получают представление о различных угрозах информационной безопасности, а также о принципах защиты информации. Важным аспектом этого раздела является введение в математические инструменты и методы, которые будут использоваться в дальнейшем.

Искусственные нейронные сети

Раздел "Искусственные нейронные сети" фокусируется на основных принципах и структурах искусственных нейронных сетей. Студенты изучают архитектуру, составляющие и возможности нейронных сетей. Они также получают практический опыт в создании простых нейронных сетей, используя соответствующие программные инструменты и библиотеки. В контексте информационной безопасности, искусственные нейронные сети могут применяться для обнаружения и предотвращения атак на системы, анализа угроз и классификации данных.

Алгоритмы обучения нейронных сетей

В этом разделе студенты изучают различные алгоритмы обучения нейронных сетей. Они узнают о принципах обратного распространения ошибки, градиентного спуска и других методах, используемых для обучения нейронных сетей. Студенты также изучают проблему переобучения и методы регуляризации. Эти знания позволяют им эффективно обучать нейронные сети для решения задач информационной безопасности, таких как обнаружение аномалий или атак.

Многослойные сети с обратным распространением информации

Многослойные сети с обратным распространением информации являются одним из наиболее распространенных типов нейронных сетей. В этом разделе студенты углубляются в теорию и практику создания многослойных сетей, используя обратное распространение информации для обучения. Они изучают различные архитектуры, функции активации и методы оптимизации, применяемые в этом контексте. Многослойные сети могут быть использованы для решения сложных задач информационной безопасности, таких как распознавание образов или шифрование данных.

Нейронные сети в защите информации

Последний раздел дисциплины посвящен применению нейронных сетей в защите информации. Студенты узнают о различных методах использования нейронных сетей для обнаружения вредоносных программ, анализа сетевой активности, аутентификации пользователей и других аспектов информационной безопасности. Они также изучают современные техники и подходы к применению нейронных сетей для защиты информации от новых и продвинутых угроз.

Содержание самостоятельной работы

	Тема СРС	Задание
1	Введение	Сделайте сводную таблицу, в которой перечислите математические инструменты защиты информации и способы их реализации: 1. Исследуйте и составьте список математических инструментов для защиты информации: • Криптография: Использование математических алгоритмов для шифрования и дешифрования информации. • Коды контроля целостности: Математические методы для обнаружения изменений или повреждений данных. • Теория информации: Математический фреймворк для определения, измерения и передачи информации без потери. • Математические модели доступа: Модели, основанные на математических принципах, которые определяют разрешенные варианты доступа к информации. • Методы сжатия данных: Математические алгоритмы для сокращения размера данных с минимальной потерей информации. • Машинное обучение в области кибербезопасности: Использование математических моделей и алгоритмов машинного обучения для обнаружения и предотвращения кибератак. 2. Для каждого инструмента опишите способы их реализации: • Криптография: Использование алгоритмов, таких как AES, RSA или ECC, для шифрования и дешифрования данных с использованием математических операций. • Коды контроля целостности: Реализация контрольных сумм, цифровых подписей или хэш-функций для обеспечения целостности данных. • Теория информации: Применение методов сжатия данных, кодирования и оптимизации для эффективной передачи информации с минимальными потерями. • Математические модели доступа: Реализация математических моделей, таких как модель

		безопасности Белла-ЛаПадулы или матричные модели доступа, для определения политик доступа и управления привилегиями. • Методы сжатия данных: Использование алгоритмов сжатия, например, Lempel-Ziv-Welch (LZW) или Deflate, для сокращения размера данных без искажения информации. • Машинное обучение в области кибербезопасности: Применение математических моделей машинного обучения, таких как нейронные сети, метод опорных векторов (SVM) или решающие деревья, для обнаружения аномалий и классификации киберугроз. 3. Составьте сводную таблицу, перечисляющую каждый математический инструмент и способы их реализации. Для каждого инструмента укажите также краткое описание и примеры его применения.
2	Искусственные нейронные сети	Исследование и создание нейронной сети для распознавания изображений рукописных цифр. 1. Изучите основы и принципы работы искусственных нейронных сетей. 2. Используя язык программирования по вашему выбору (например, Python), реализуйте нейронную сеть с использованием библиотеки для глубокого обучения, такой как TensorFlow или PyTorch. 3. Подготовьте тренировочный набор данных, включающий изображения рукописных цифр. 4. Обучите нейронную сеть на тренировочном наборе данных и настройте ее параметры для достижения высокой точности распознавания. 5. Оцените производительность обученной нейронной сети, используя тестовый набор данных, который не использовался при тренировке. 6. Дайте краткое описание процесса и результатов вашей работы, включая решение каких-либо проблем или вызовов, с которыми вы столкнулись.
3	Алгоритмы обучения нейронных сетей	1. Изучите алгоритм обратного распространения ошибки (Backpropagation) и его реализацию. 2. Исследуйте алгоритм градиентного спуска (Gradient Descent) и его различные вариации, такие как стохастический градиентный спуск (Stochastic Gradient Descent) и мини-пакетный градиентный спуск (Mini-batch Gradient Descent). 3. Опишите алгоритмы оптимизации, используемые

		для улучшения процесса обучения нейронных сетей, такие как методы адаптивного шага обучения (Adaptive Learning Rate). 4. Изучите алгоритмы регуляризации, такие как L1 и L2 регуляризация, и объясните их влияние на процесс обучения и предотвращение переобучения (Overfitting). 5. Исследуйте алгоритмы оптимизации гиперпараметров нейронных сетей, например, с использованием перекрестной проверки (Cross-Validation) и сетки гиперпараметров (Hyperparameter Grid Search). 6. Реализуйте примеры с использованием выбранных алгоритмов обучения нейронных сетей на практике, используя одну из популярных библиотек машинного обучения, таких как TensorFlow или PyTorch. 7. Проанализируйте результаты экспериментов, проведенных в пункте 6, и сделайте выводы о влиянии различных алгоритмов обучения на эффективность и точность нейронных сетей.
4	Многослойные сети с обратным распространением информации	1. Изучите алгоритм обратного распространения ошибки (Backpropagation) в многослойных нейронных сетях и понимание работы градиентного спуска. 2. Создайте небольшой набор данных, состоящий из двух классов. Например, можно сгенерировать два облака точек, распределенных вокруг различных центров. 3. Реализуйте многослойную нейронную сеть с обратным распространением информации на выбранном вами языке программирования. В качестве активационной функции используйте, например, сигмоиду или ReLU. 4. Обучите нейронную сеть на вашем наборе данных, используя алгоритм обратного распространения ошибки. Подберите оптимальные гиперпараметры (например, скорость обучения и количество эпох) для достижения наилучшей производительности. 5. Оцените производительность обученной нейронной сети, используя метрики, такие как точность (accuracy), precision, recall или F1-меру. Сравните результаты с другими классификационными моделями, такими как метод опорных векторов или деревья решений.

		6. Проведите анализ результатов и осмыслите полученные выводы. Обратите внимание на эффективность и скорость обучения многослойной нейронной сети, а также на ее способность к классификации и обработке сложных данных.
5	Нейронные сети в защите информации	Напишите исследовательскую статью на тему "Применение нейронных сетей в защите информации". 1. Введение: o Расскажите о важности защиты информации и возможных угрозах, с которыми сталкиваются организации и частные лица. o Представьте концепцию нейронных сетей и их возможности в обработке сложных данных. 2. Обзор литературы: o Проанализируйте существующие исследования и публикации по применению нейронных сетей в задачах защиты информации. o Обсудите различные подходы и модели нейронных сетей, используемые для обнаружения и предотвращения атак, а также для анализа и обработки зашифрованных данных. 3. Методология: o Опишите методы и алгоритмы, используемые для построения нейронных сетей в задачах защиты информации. o Рассмотрите вопросы выбора архитектуры сети, оптимизации гиперпараметров, выбора функции активации и прочих важных аспектов. 4. Эксперименты и результаты: o Проведите эксперименты, используя выбранные методы и данные, чтобы продемонстрировать эффективность нейронных сетей в задачах защиты информации. o Оцените результаты экспериментов с использованием метрик, таких как точность, полнота и F1-мера. o Сравните результаты с другими методами защиты информации и обсудите преимущества и ограничения нейронных сетей. 5. Обсуждение и выводы: o Проанализируйте полученные результаты и сделайте выводы о применимости нейронных сетей в задачах защиты информации. o Обсудите потенциальные риски и вызовы,

		связанные с использованием нейронных сетей в защите информации. ○ Предложите возможные направления дальнейших исследований и улучшения в данной области. 6. Заключение: ○ Подведите итоги исследования и подчеркните его вклад в развитие области защиты информации с использованием нейронных сетей. 7. Список литературы: ○ Предоставьте список всех использованных источников, ссылаясь на соответствующие работы и публикации.

КОНТРОЛЬНЫЕ ВОПРОСЫ

Тема 1. Введение

1. Что такое искусственный интеллект и как он связан с нейронными сетями?
2. Какие преимущества и вызовы представляет собой использование нейронных сетей?
3. Каковы основные принципы функционирования нейронных сетей?
4. Какие области применения и потенциальные выгоды имеют нейронные сети?
5. Какова история развития искусственного интеллекта и нейронных сетей?
6. Какие факторы способствовали росту интереса к нейронным сетям в последние годы?
7. Какие были основные прорывы в исследовании искусственного интеллекта, приведшие к появлению нейронных сетей?
8. Какая роль нейронных сетей сыграла в развитии машинного обучения и глубокого обучения?
9. Какие исторические моменты в сфере искусственного интеллекта и нейронных сетей стали вехами в их развитии?
10. Какие вызовы и проблемы искусственного интеллекта и нейронных сетей были преодолены за последние годы?

Тема 2. Искусственные нейронные сети

1. Что является входом искусственного нейрона?
2. Что такое множество весовых значений нейрона?
3. Что означает величина NET?
4. Что означает величина OUT?
5. Что такое искусственный интеллект и как он связан с нейронными сетями?
6. Какие преимущества и вызовы представляет собой использование нейронных сетей?
7. Каковы основные принципы функционирования нейронных сетей?
8. Какие области применения и потенциальные выгоды имеют нейронные сети?
9. Какие компоненты составляют структуру искусственной нейронной сети?
10. Каким образом веса и смещения влияют на работу искусственной нейронной сети?

Тема 3. Алгоритмы обучения нейронных сетей

1. Сетью без обратных связей называется сеть?

2. Какие сети характеризуются отсутствием памяти?
3. Входом персептрона являются
4. Теорема о двухслойности персептрона утверждает, что?
5. Что такое искусственный интеллект и как он связан с нейронными сетями?
6. Какие преимущества и вызовы представляет собой использование нейронных сетей?
7. Каковы основные принципы функционирования нейронных сетей?
8. Какие области применения и потенциальные выгоды имеют нейронные сети?
9. Какие методы и стратегии можно применять для инициализации весов в нейронных сетях перед обучением?
10. Какие меры принимаются для предотвращения переобучения нейронных сетей?

Тема 4. Многослойные сети с обратным распространением информации

1. Какой должна быть активационная функция, для того чтобы возможно было применять алгоритм обратного распространения?
2. Обобщенным многослойным персептроном называется
3. Входным слоем обобщенного многослойного персептрона называется?
4. Скрытым слоем обобщенного многослойного персептрона называется?
5. Что такое искусственный интеллект и как он связан с нейронными сетями?
6. Какие преимущества и вызовы представляет собой использование нейронных сетей?
7. Каковы основные принципы функционирования нейронных сетей?
8. Какие области применения и потенциальные выгоды имеют нейронные сети?
9. Что такое градиентный спуск и как он применяется в обратном распространении ошибки?
10. Какие функции активации чаще всего используются в многослойных нейронных сетях и почему?

Тема 5. Нейронные сети в защите информации

1. Как называется информация, которую следует защищать (по нормативам, правилам сети, системы)?
2. Разновидностями угроз безопасности (сети, системы) являются
3. Относятся к правовым методам, обеспечивающим информационную безопасность
4. Основные источники угроз информационной безопасности

5. Что такое искусственный интеллект и как он связан с нейронными сетями?

6. Какие преимущества и вызовы представляет собой использование нейронных сетей?

7. Каковы основные принципы функционирования нейронных сетей?

8. Какие области применения и потенциальные выгоды имеют нейронные сети?

9. Какие методы аутентификации и идентификации могут быть улучшены с помощью нейронных сетей?

10. Какая роль играют нейронные сети в обнаружении аномалий и вредоносных программ в системах защиты информации?

ПЕРЕЧЕНЬ ЛИТЕРАТУРЫ И ИНФОРМАЦИОННЫХ РЕСУРСОВ

1. Осипов, Г. С. Методы искусственного интеллекта : монография / Г. С. Осипов. – Москва : Физматлит, 2011. – 296 с. – URL: https://biblioclub.ru/index.php?page=book&id=457464 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.

2. Белозерова, Г. И. Нечеткая логика и нейронные сети : учебное пособие / Г. И. Белозерова, Д. М. Скуднев, З. А. Кононова ; Липецкий государственный педагогический университет им. П. П. Семенова-Тян-Шанского. – Липецк : Липецкий государственный педагогический университет им. П.П. Семенова-Тян-Шанского, 2017. – Часть 1. – 65 с. – URL: https://biblioclub.ru/index.php?page=book&id=576909 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.

3. Сергеев, Н. Е. Системы искусственного интеллекта : учебное пособие / Н. Е. Сергеев. – Таганрог : Южный федеральный университет, 2016. – Часть 1. – 123 с. – URL: https://biblioclub.ru/index.php?page=book&id=493307 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.

4. Сохибов, Т. Т. Конструирование искусственных нейронных сетей с помощью меметических алгоритмов : научная работа / Т. Т. Сохибов ; Московский Государственный Университет имени М. В. Ломоносова, Факультет вычислительной математики и кибернетики. – Москва : б.и., 2020. – 61 с.– URL: https://biblioclub.ru/index.php?page=book&id=594428 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.