АННОТАЦИЯ

к рабочей программе дисциплины

«Обеспечение безопасности автоматизированных систем на основе методов искусственного интеллекта»

Специальность 10.05.03 Информационная безопасность автоматизированных систем

Специализация специализация N 7 "Анализ безопасности информационных систем"

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2021

Цель изучения дисциплины: формирование представления о современном состоянии теории и практики построения интеллектуальных систем, в том числе с целью обеспечения безопасности автоматизированных систем на основе методов искусственного интеллекта.

Задачи изучения дисциплины:

- формирование знаний, умений и навыков в области теории и методов исследования моделей представления, хранения и обработки знаний;
- овладения умениями и навыками программирования задач обработки знаний;
- формирование системного базового представления, первичных знаний, умений и навыков студентов по основам инженерии знаний и нейроинформатике, как двум направлениям построения интеллектуальных систем;
- формирование общих представлений о прикладных системах искусственного интеллекта.

Содержание дисциплины:

Определение искусственного интеллекта. Задачи искусственного интеллекта. История развития искусственного интеллекта как науки. Основные подходы к исследованию искусственного интеллекта. Основные направления исследований в области искусственного интеллекта.

Основы технологий больших данных. Особенности применения. Архитектуры организации систем Big Data. Big Data и Data Mining. Технологии Больших данных. Hadoop. Инфраструктура больших данных. Apache Kafka. Подход MapReduce и его программные реализации. Роль СУБД NoSQL в инфрастурктуре BigData. Apache Spark. Архитектура распределенного приложения Spark. Основные концепции Spark: RDD и DAG; основные этапы обработки данных; загрузка данных из внешнего хранилища; вычисления в Spark; Shuffle механизм; управление памятью. DataFrame API и Spark SQL. Создание, настройка и запуск Spark проекта. Практическое применение технологий больших данных на примерах.

Введение: задачи обучения по прецедентам. Примеры прикладных

задач.

Байесовские методы классификации. Вероятностная постановка задачи классификации. Непараметрическая классификация. Нормальный дискриминантный анализ.

Метрические методы классификации: метод ближайшего соседа и его обобщения.

Линейные методы классификации. Аппроксимация и регуляризация эмпирического риска. Линейная модель классификации. Метод стохастического градиента. Логистическая регрессия. Метод опорных векторов. Методы восстановления регрессии. Метод наименьших квадратов. Непараметрическая регрессия: ядерное сглаживание. Линейная регрессия. Метод главных компонент. Нелинейные методы восстановления регрессии. Метод опорных векторов в задачах регрессии. Искусственные нейронные сети. Проблема полноты. Многослойные нейронные сети. Кластеризация и визуализация. Алгоритмы кластеризации. Сети Кохонена. Многомерное шкалирование. Введение в обучение с подкреплением

Логическая модель. Продукционная модель. Фреймы. Семантические сети. Нечёткие системы и нечёткий вывод

Основы теории агентов и мультиагентных систем. Основные понятия. Современные подходы к решению распределенных задач. Примеры задач, решаемых посредством агентов. Общая классификация агентов.

Общая характеристика мультиагентных систем. Примеры построения мультиагентных систем. Коллективное поведение агентов. Модели коллективного поведения. Виды моделей. Модели кооперации агентов. Конфликты в мультиагентных системах. Основные типы конфликтов. Механизмы разрешения конфликтов. Инструментарий программирования MAC.

Обнаружение и предотвращение вторжений. Обнаружение и изучение вредоносной активности на конечных точках: подключенных к сети рабочих станциях, серверах, устройствах Интернета вещей (EDR). SIEM-системы. Предотвращение утечек информации (DLP). Обнаружения и блокирования сетевых атак на веб-приложение (WAF). Поведенческий анализ действий пользователей (UEBA). Адаптивная аутентификация.

Перечень формируемых компетенций:

ПК-7.1 - Способен применять математические модели при исследовании систем защиты информации автоматизированных систем, в том числе с использованием современных методов и программного инструментария искусственного интеллекта

Общая трудоемкость дисциплины: 2 з.е.

Форма итогового контроля по дисциплине: Зачет