МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
высшего образования - программы специалитета
по специальности
10.05.01 Компьютерная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Применение систем искусственного интеллекта для решения задач компьютерной безопасности

Специальность: 10.05.01 Компьютерная безопасность

Специализация: Информационная безопасность объектов информатизации на базе компьютерных систем

Форма обучения: Очная

1. Общие сведения о дисциплине (модуле).

Цель: Изучение теоретических основ и приобретение практических навыков использования технологий искусственного интеллекта для автоматизации процессов обнаружения, предупреждения и нейтрализации угроз безопасности информации в компьютерных системах и сетях.

Задачи:

- Анализ современных угроз компьютерной безопасности и обоснование необходимости применения интеллектуальных методов для их нейтрализации.
- Изучение математического аппарата и алгоритмического обеспечения систем ИИ, используемых в защищенных системах.
- Освоение методик проектирования и настройки интеллектуальных детекторов атак и анализаторов защищенности.
- Формирование навыков экспериментального исследования эффективности систем ИИ в задачах обеспечения компьютерной безопасности.

2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

ПК-6 - Способен проводить оценку эффективности реализации систем защиты информации и действующих политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации;

ПК-9 - Способен участвовать в управлении информационной безопасностью компьютерной системы, разрабатывать предложения по ее совершенствованию.

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Знать:

- нормативно-правовые документы в области информационной и компьютерной безопасности
- современное программно-аппаратное обеспечение
- системы антивирусной защиты
- средства криптографической защиты информации

Уметь:

- проводить оценку эффективности реализации систем защиты информации и политик безопасности в компьютерных системах, включая защищенные операционные системы, системы управления базами данных, компьютерные сети, системы антивирусной защиты, средства криптографической защиты информации
- участвовать в управлении информационной безопасностью компьютерной системы, разрабатывать предложения по ее совершенствованию

Владеть:

- навыками анализа информационной безопасностью компьютерной системы

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 3 з.е. (108 академических часа(ов).

3.2. Объем дисциплины (модуля) в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Тип учебных занятий	Количество часов	
	Всего	Семестр №5
Контактная работа при проведении учебных занятий (всего):	80	80
В том числе:		
Занятия лекционного типа	32	32
Занятия семинарского типа	48	48

3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 28 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или)

лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

4. Содержание дисциплины (модуля).

4.1. Занятия лекционного типа.

№ п/п	Тематика лекционных занятий / краткое содержание
1	Введение Рассматриваемые вопросы: - Понятие искусственного интеллекта. - Примеры прикладных задач. - Типы задач искусственного интеллекта -регрессия, прогнозирование, классификация, кластеризация. - Основные понятия – объекты и признаки, функция потерь и функционал качества. - Виды обучения – обучение с учителем, обучение без учителя. - Матричные операции и работа с пакетом Matlab. - Матрицы и вектора. - Сложение и скалярное умножение. - Умножение матрицы на вектор. - Умножение матриц, свойства. - Обратная и транспонированная матрица. - Реализация скалярных и матричных операций в пакете Matlab. - Элементы программирования. - Визуализация. - М- файлы – назначение, создание, использование. - Векторизация.
2	Линейная регрессия одной переменной Рассматриваемые вопросы: - Постановка задачи линейной регрессии. - Функция гипотезы. - Метод наименьших квадратов и его геометрический смысл. - Метод градиентного спуска. - Графическая интерпретация метода градиентного спуска. - Применение метода градиентного спуска для решения задач линейной регрессии одной переменной.
3	Многомерная линейная регрессия Рассматриваемые вопросы: - Понятие признака. - Множественность признаков. - Нормировка признаков, геометрический смысл. - Методы решения задачи многомерной линеной регрессии. - Метод градиентного спуска для многомерной линейной регрессии. - Полиномиальная регрессия. - Аналитическое решение задачи многомерной линейной регрессии. - Проблема необратимости матрицы.
4	Логистическая регрессия Рассматриваемые вопросы: - Постановка задачи классификации.

№ п/п	Тематика лекционных занятий / краткое содержание
	- Оценивание апостериорных вероятностей классов с помощью сигмоидной функции активации. - Разделяющая гиперповерхность. - Методы решения задачи классификации. - Логарифмическая функция потерь. - Применение градиентного спуска и других методов оптимизации. - Многоклассовая классификация – «один против всех». - Регуляризация. - Проблема переобучения. - Редукция весов. - Регуляризованная линейная регрессия. - Регуляризованная логистическая регрессия.
5	Введение в нейронные сети Рассматриваемые вопросы: - Что такое нейронные сети. - Биологический нейрон и мозг. - Архитектура нейронных сетей. - Примеры прикладных задач. - Персептрон. - Функции активации персептрона. - Обучение персептрона. - Понятие линейной разделимости. - Многоклассовая классификация.

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	Знакомство с пакетом MATLAB Изучение интерфейса. Выполнение базовых матричных операций: сложение, умножение, транспонирование.
2	Визуализация данных в MATLAB Построение графиков функций, диаграмм рассеяния. Импорт и первичный анализ данных.
3	Разработка системы прогнозирования (МНК). Реализация метода наименьших квадратов для линейной регрессии одной переменной.
4	Разработка системы прогнозирования (градиентный спуск). Реализация линейной регрессии с использованием метода градиентного спуска. Сравнение с МНК.
5	Визуализация работы градиентного спуска. Построение графиков траектории спуска и поверхности функции потерь.
6	Многомерная линейная регрессия. Реализация прогнозирования на основе нескольких признаков. Подготовка данных.
7	Нормировка признаков. Исследование влияния масштабирования признаков на скорость сходимости градиентного спуска.
8	Полиномиальная регрессия. Построение модели, учитывающей нелинейные зависимости между признаками и целевой переменной.
9	Аналитическое решение многомерной регрессии. Решение задачи регрессии с помощью нормального уравнения (Normal Equation).

№ п/п	Наименование лабораторных работ / краткое содержание
10	Логистическая регрессия. Бинарная классификация. Построение классификатора для разделения данных на два класса с использованием сигмоидной функции.
11	Визуализация границы принятия решений. Построение разделяющей гиперплоскости для логистической регрессии.
12	Функции потерь для классификации. Изучение логарифмической функции потерь (log-loss). Сравнение с квадратичной ошибкой.
13	Проблема переобучения. Демонстрация эффекта переобучения на примере полиномиальной модели.
14	Регуляризация. Применение L2-регуляризации для борьбы с переобучением в линейной регрессии.
15	Регуляризованная логистическая регрессия. Реализация классификатора с регуляризацией для улучшения обобщающей способности.
16	Многоклассовая классификация (One-vs-All). Реализация метода "один против всех" для задачи классификации на несколько классов.
17	Введение в нейронные сети. Модель персептрона. Программная реализация простейшего персептрона и его обучение.
18	Исследование функций активации. Сравнение сигмоиды, гиперболического тангенса и ReLU. Визуализация их графиков и производных.
19	Проблема линейной разделимости. Реализация логического элемента XOR и демонстрация ограничений однослойного персептрона.
20	Многослойный персептрон. Построение простой двухслойной нейронной сети для решения задачи XOR.
21	Применение ИИ для детектирования аномалий. Построение модели (One-Class SVM или на основе логистической регрессии) для поиска выбросов в сетевом трафике.
22	Кластеризация данных. Реализация алгоритма k-средних (k-means) для группировки данных о событиях безопасности.
23	Оценка качества моделей. Расчет метрик классификации: accuracy, precision, recall, F1-measure. Построение ROC-кривой.
24	Итоговая работа. Разработка интеллектуального модуля. Сквозное проектирование: от предобработки данных до обучения и оценки модели для задачи компьютерной безопасности.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Изучение дополнительной литературы.
2	Подготовка к лабораторным работам.
3	Подготовка к промежуточной аттестации.
4	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых проектов

Курсовые работы (проекты) не предусмотрены

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа
1	Нейронные сети в Matlab Маслова А.А. Учебное пособие Балтийский государственный технический университет «Военмех» имени Д.Ф. Устинова, - 165 с. - ISBN 978-5-906920-72-0 , 2017	https://reader.lanbook.com/book/121856#3
2	Нейронные сети и генетический алгоритм Шматов Г. П. Учебное пособие Тверской государственный технический университет, - 200 с. - ISBN 978-5-7995-1007-7 , 2019	https://reader.lanbook.com/book/171312
3	Модели и методы искусственного интеллекта Пенькова Т.Г., Вайнштейн Ю.В. Учебное пособие Красноярск: Сиб. федер. ун-т, - 116 с. - ISBN 978-5-57638-4043-8 , 2019	https://reader.lanbook.com/book/157579#3

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

Официальный сайт РУТ (МИИТ) (https://www.miit.ru/).

Научно-техническая библиотека РУТ (МИИТ) (http:/library.miit.ru).

Образовательная платформа «Юрайт» (https://urait.ru/).

Общие информационные, справочные и поисковые системы «Консультант Плюс», «Гарант».

Электронно-библиотечная система издательства «Лань» (http://e.lanbook.com/).

Электронно-библиотечная система ibooks.ru (http://ibooks.ru/).

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

Microsoft Internet Explorer (или другой браузер).

Операционная система Microsoft Windows.

Microsoft Office

Пакет прикладных программ MATLAB

Пакет прикладных программ MATCad
Adobe Reader

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

Учебные аудитории для проведения учебных занятий, оснащенные компьютерной техникой и наборами демонстрационного оборудования.

9. Форма промежуточной аттестации:

Зачет в 5 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

доцент, к.н. кафедры «Управление и защита информации» Н.Н. Зольникова

Согласовано:

Заведующий кафедрой УиЗИ Л.А. Баранов

Председатель учебно-методической комиссии С.В. Володин