

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

Рабочая программа дисциплины (модуля) в виде
электронного документа выгружена из единой
корпоративной информационной системы управления
университетом и соответствует оригиналу

Простая электронная подпись, выданная РУТ (МИИТ)
ID подписи: 2053
Подписал: заведующий кафедрой Баранов Леонид Аврамович
Дата: 01.06.2023

1. Общие сведения о дисциплине (модуле).

Основной целью изучения учебной дисциплины «Применение систем искусственного интеллекта для решения задач компьютерной безопасности» является формирование у обучающегося компетенций для следующих видов деятельности: проектно-конструкторской; научно-исследовательской.

Дисциплина предназначена для получения знаний для решения следующих профессиональных задач (в соответствии с видами деятельности): Проектно-конструкторская деятельность: сбор и анализ исходных данных для расчета и проектирования устройств и систем автоматизации и управления; расчет и проектирование отдельных блоков и устройств систем автоматизации и управления в соответствии с техническим заданием; разработка проектной и рабочей документации, оформление отчетов по законченным проектно-конструкторским работам; Научно-исследовательская деятельность: анализ научно-технической информации, отечественного и зарубежного опыта по тематике исследования; участие в работах по организации и проведению экспериментов на действующих объектах по заданной методике; обработка результатов экспериментальных исследований с применением современных информационных технологий и технических средств; проведение вычислительных экспериментов с использованием стандартных программных средств с целью получения математических моделей процессов и объектов автоматизации и управления; подготовка данных и составление обзоров, рефератов, отчетов, научных публикаций и докладов на научных конференциях и семинарах, участие во внедрении результатов исследований и разработок; Целями освоения учебной дисциплины (модуля) «Применение систем искусственного интеллекта для решения задач компьютерной безопасности» являются изучение алгоритмов и способов разработки современных интеллектуальных систем, подготовка к применению полученных знаний для решения различных интеллектуальных задач, таких как задачи прогнозирования, классификации объектов, распознавание звуков речи и различных символов и т. п. Дисциплина призвана дать комплекс базовых теоретических знаний в области систем искусственного интеллекта, а также привить студентам уверенные практические навыки по использованию средств вычислительной техники и программного обеспечения для решения практических инженерных задач. Воспитательной целью дисциплины является формирование у студентов научного, творческого подхода к освоению технологий, методов и средств разработки интеллектуальных систем.

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	Сем. №6
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	<p>Введение</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - 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.

№ п/п	Тематика лекционных занятий / краткое содержание
	<ul style="list-style-type: none"> - 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	<p>Линейная регрессия одной переменной</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - 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	<p>Многомерная линейная регрессия</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Понятие признака. - Множественность признаков. - Нормировка признаков, геометрический смысл. - Методы решения задачи многомерной линейной регрессии. - Метод градиентного спуска для многомерной линейной регрессии. - Полиномиальная регрессия. - Аналитическое решение задачи многомерной линейной регрессии. - Проблема необратимости матрицы.
4	<p>Логистическая регрессия</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Постановка задачи классификации. - 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	<p>Введение в нейронные сети</p> <p>Рассматриваемые вопросы:</p> <ul style="list-style-type: none"> - Что такое нейронные сети. - Биологический нейрон и мозг. - Архитектура нейронных сетей. - Примеры прикладных задач. - Персептрон. - Функции активации персептрона. - Обучение персептрона. - Понятие линейной разделимости.

№ п/п	Тематика лекционных занятий / краткое содержание
	- Многоклассовая классификация.

4.2. Занятия семинарского типа.

Лабораторные работы

№ п/п	Наименование лабораторных работ / краткое содержание
1	ЛР №1 Разработка автоматической системы прогнозирования на основе линейной регрессии одной переменной.
2	ЛР №2 Разработка автоматической системы прогнозирования на основе линейной регрессии одной переменной.
3	ЛР №3 Разработка автоматической системы прогнозирования на основе линейной регрессии одной переменной.
4	ЛР №4 Разработка автоматической системы прогнозирования на основе многомерной линейной регрессии.
5	ЛР №5 Разработка автоматической системы прогнозирования на основе многомерной линейной регрессии.
6	ЛР №6 Разработка линейного классификатора на основе логистической регрессии.
7	ЛР №7 Разработка линейного классификатора на основе логистической регрессии.
8	ЛР №8 Разработка классификатора на основе логистической регрессии с использованием регуляризации.

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.
5	Подготовка к промежуточной аттестации.
6	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: распознавание, управление, принятие решений А.Б. Барский Финансы и статистика , 2007	НТБ (уч.3); НТБ (фб.); НТБ (чз.2)
2	Теория вероятностей и математическая статистика В. М. Буре, Е. М. Парилина Лань , 2013	НТБ (уч.3); НТБ (фб.); НТБ (чз.2);
3	Численные методы Н.С. Бахвалов, Н.П. Жидков, Г.М. Кобельков Бином. Лаборатория знаний , 2007	НТБ (уч.2); НТБ (уч.4)
1	Распознавание образов. Введение в методы статистического обучения А.Б. Мерков Едиториал УРСС, , 2011	Internet
2	Самообучающиеся системы С.И. Николенко, А.Л. Тулупов МЦНМО , 2009	Internet
3	MATLAB 6.5 SP1/7/7 SP1/7 SP2 + Simulink 5/6. Инструменты искусственного интеллекта и биоинформатики. В.П. Дьяконов, В.В. Круглов СОЛОН-ПРЕСС , 2009	Internet
4	Введение в искусственный интеллект Л.Н. Ясницкий Академия , 2010	Internet
5	Вычислительные методы. Теория и практика в среде MATLAB К. Плохотников Горячая Линия – Телеком , 2013	Internet
6	Задача прогнозирования (линей-ная регрессия одной и нескольких переменных). Методические указания по дисциплине «Системы искусственного интеллекта» Зольникова Н.Н., Мелёшин И.С. В печати МИИТ, , 2017	Internet

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 6 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