МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»

Кафедра «Управление и защита информации»

АННОТАЦИЯ К РАБОЧЕЙ ПРОГРАММЕ ДИСЦИПЛИНЫ

«Применение систем искусственного интеллекта для решения задач компьютерной безопасности»

Специальность:	10.05.01 – Компьютерная безопасность
Специализация:	Информационная безопасность объектов информатизации на базе компьютерных систем
Квалификация выпускника:	Специалист по защите информации
Форма обучения:	очная
Год начала подготовки	2020

1. Цели освоения учебной дисциплины

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. Место учебной дисциплины в структуре ОП ВО

Учебная дисциплина "Применение систем искусственного интеллекта для решения задач компьютерной безопасности" относится к блоку 1 "Дисциплины (модули)" и входит в его базовую часть.

3. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций:

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

4. Общая трудоемкость дисциплины составляет

3 зачетные единицы (108 ак. ч.).

5. Образовательные технологии

Преподавание дисциплины «Применение систем искусственного интеллекта для решения задач компьютерной безопасности» осуществляется в форме лекций и практических занятий.Лекции проводятся в традиционной классно-урочной организационной форме, по типу управления познавательной деятельностью являются традиционными классически-лекционными (объяснительно-иллюстративные), и проводятся с использованием интерактивных (диалоговых) технологий, в том числе мультимедиа.Практические занятия организованы с использованием технологий развивающего обучения. Часть практического курса выполняется в виде традиционных практических занятий (объяснительно-иллюстративное решение задач), проводится с использованием интерактивных (диалоговые) технологий, в том числе электронный практикум (решение проблемных поставленных задач с помощью современной вычислительной техники и исследование моделей); технологий, основанных на коллективных способах обучения, а также использованием компьютерной тестирующей системы. Самостоятельная работа студента организована с использованием традиционных видов работы и интерактивных технологий. К традиционным видам работы относятся отработка лекционного материала и отработка отдельных тем по учебным пособиям. К интерактивным (диалоговым) технологиям относится отработка отдельных тем по электронным пособиям, подготовка к промежуточным контролям в интерактивном режиме, интерактивные консультации в режиме реального времени по специальным разделам и технологиям, основанным на коллективных способах самостоятельной работы студентов.Оценка полученных знаний, умений и навыков основана на модульно-рейтинговой технологии. Весь курс разбит на 5 разделов, представляющих собой логически завершенный объём учебной информации. Фонды оценочных средств освоенных компетенций включают как вопросы теоретического характера для оценки знаний, так и задания практического содержания (решение конкретных задач, работа с данными) для оценки умений и навыков. Теоретические знания проверяются путём

применения таких организационных форм, как индивидуальные и групповые опросы, решение тестов с использованием компьютеров или на бумажных носителях. .

6. Содержание дисциплины (модуля), структурированное по темам (разделам)

РАЗДЕЛ 1
Введение

Тема: 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.

Тема: 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 программи-рования. Визуализация. М- файлы – назначение, создание, использование. Векторизация.

РАЗДЕЛ 2
Линейная регрессия одной переменной

Тема: Постановка задачи линейной регрессии.
. Функция гипотезы. Метод наименьших квадратов и его геометрический смысл.

Тема: Метод градиентного спуска
Графическая интерпретация метода градиентного спуска. Применение метода градиент-ного спуска для решения задач линейной регрессии одной переменной.

РАЗДЕЛ 3
Многомерная линейная регрессия

Тема: Понятие признака
Множественность признаков. Нормировка признаков, геометрический смысл.

Тема: Методы решения задачи многомерной линеной регрессии
Метод градиентного спуска для многомерной линейной регрессии. Полиномиальная регрессия. Аналитическое решение задачи многомерной линейной регрессии. Проблема необратимости матрицы.

Тема: Методы решения задачи многомерной линеной регрессии
Устный опрос, защита индивидуальных заданий, тестирование

РАЗДЕЛ 4
Логистическая регрессия

Тема: Постановка задачи классификации
Оценивание апостериорных вероятностей классов с помощью сигмоидной функции активации. Разделяющая гиперповерхность.

Тема: Методы решения задачи классификации
Логарифмическая функция потерь. Применение градиентного спуска и других методов оптимизации . Многоклассовая классификация – «один против всех».

Тема: Регуляризация
Проблема переобучения. Редукция весов. Регуляризованная линейная регрессия. Регуляризованная логистическая регрессия

Тема: Регуляризация
Устный опрос, защита индивидуальных заданий, тестирование

РАЗДЕЛ 5
Введение в нейронные сети

Тема: Что такое нейронные сети
Биологический нейрон и мозг. Архитектура нейронных сетей. Примеры прикладных задач.

Тема: Персептрон
Функции активации персептрона. Обучение персептрона. Понятие линейной разделимости. Многоклассовая классификация.

Зачет