МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Воронежский государственный технический университет»

УТВЕРЖДАЮ

Декан факультета ФИТКБ

_____ /Гусев П.Ю./

28.02.2023 г.

.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Обеспечение безопасности автоматизированных систем на основе методов искусственного интеллекта»

Специальность 10.05.03 Информационная безопасность автоматизированных систем

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

Автор программы _____ /Разинкин К.А./

Заведующий кафедрой Систем информационной безопасности _____

Руководитель ОПОП _____ /Остапенко А.Г./

Воронеж 2023

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

1.1. Цели дисциплины формирование представления о современном состоянии теории и практики построения интеллектуальных систем, в том числе в контексте обеспечения безопасности компьютерных систем и сетей систем на основе методов искусственного интеллекта.

1.2. Задачи освоения 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, в том числе защите систем ИИ от адверсариальных атак на основе методов состязательного машинного обучения.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Обеспечение безопасности автоматизированных систем на основе методов искусственного интеллекта» относится к дисциплинам блока ФТД.

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Обеспечение безопасности автоматизированных систем на основе методов искусственного интеллекта» направлен на формирование следующих компетенций:

ПК-7.1 - Способен обосновывать необходимость защиты информации в автоматизированной системе на основе рисковой методологии, а также применять методы и инструментальные средства анализа данных и искусственного интеллекта при управлении защитой информации в автоматизированной системе

Компетенция	Результаты обучения, характеризующие сформированность компетенции
ПК-7.1	знать теоретические основы применения методов искусственного интеллекта в задачах обеспечения безопасности компьютерных систем и сетей
	уметь разрабатывает комплекс правил, процедур, приемов и методов, средств обеспечения защиты информации, в том числе с использованием современных методов и программного инструментария искусственного интеллекта
	владеть инструментальными средствами реализущими подходы к классификации и прогнозированию угроз безопасности информации, а так же оцениванию последствий от реализации угроз безопасности информации в КС и автоматизированных системах

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины «Обеспечение безопасности автоматизированных систем на основе методов искусственного интеллекта» составляет 2 з.е.

Распределение трудоемкости дисциплины по видам занятий

очная форма обучения

Виды учебной работы	Всего часов	Семестры
		10
Аудиторные занятия (всего)	54	54
В том числе:		
Лекции	36	36
Практические занятия (ПЗ)	18	18
Самостоятельная работа	18	18
Виды промежуточной аттестации - зачет	+	+
Общая трудоемкость: академические часы зач.ед.	 72 2	 72 2

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Содержание разделов дисциплины и распределение трудоемкости по видам занятий

очная форма обучения

№ п/п	Наименование темы	Содержание раздела	Лекц	Прак зан.	СРС	Всего, час
1	*Введение в искусственный интеллект*	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.	6	2	2	10
2	*Введение в технологии BIG DATA*	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.	6	2	2	10

		Практическое применение технологий больших данных на примерах.				
3	*Машинное обучение*	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	6	2	2	10
4	*Подходы к представлению знаний*	Логическая модель. Продукционная модель. Фреймы. Семантические сети. Нечёткие системы и нечёткий вывод	6	4	4	14
5	*Мультиагентные системы*	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 МАС.	6	4	4	14
6	*Применение ИИ в задачах обеспечения*	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	6	4	4	14

		(DLP). Обнаружения и блокирования сетевых атак на веб-приложение (WAF). Поведенческий анализ действий пользователей (UEBA). Адаптивная аутентификация. Адверсариальные атаки и состязательное машинное обучение				
		Итого	**36**	**18**	**18**	**72**

5.2 Перечень лабораторных работ

Не предусмотрено учебным планом

6. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ ПРОЕКТОВ (РАБОТ) И КОНТРОЛЬНЫХ РАБОТ

В соответствии с учебным планом освоение дисциплины не предусматривает выполнение курсового проекта (работы) или контрольной работы.

7. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

7.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

7.1.1 Этап текущего контроля

Результаты текущего контроля знаний и межсессионной аттестации оцениваются по следующей системе:

«аттестован»; «не аттестован».

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Аттестован	Не аттестован
ПК-7.1	знать теоретические основы применения методов искусственного интеллекта в задачах обеспечения безопасности компьютерных систем и сетей	знание теоретических основ применения методов искусственного интеллекта в задачах обеспечения безопасности компьютерных систем и сетей	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	уметь разрабатывает комплекс правил, процедур, приемов и методов, средств обеспечения защиты информации, в том числе с использованием современных методов и программного инструментария искусственного интеллекта	умение разрабатывать комплекс правил, процедур, приемов и методов, средств обеспечения защиты информации, в том числе с использованием современных методов и программного инструментария искусственного интеллекта	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	владеть инструментальными средствами реализущими	владение инструментальными средствами реализущими	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих про-

	подходы к классификации и прогнозированию угроз безопасности информации, а так же оцениванию последствий от реализации угроз безопасности информации в КС и автоматизированных системах	подходы к классификации и прогнозированию угроз безопасности информации, а так же оцениванию последствий от реализации угроз безопасности информации в КС и автоматизированных системах		граммах

7.1.2 Этап промежуточного контроля знаний

Результаты промежуточного контроля знаний оцениваются в 10 семестре для очной формы обучения по двухбалльной системе:

«зачтено»

«не зачтено»

Компетенция	Результаты обучения, характеризующие сформированность компетенции	Критерии оценивания	Зачтено	Не зачтено
ПК-7.1	знать теоретические основы применения методов искусственного интеллекта в задачах обеспечения безопасности компьютерных систем и сетей	Тест	Выполнение теста на 70-100%	Выполнение менее 70%
	уметь разрабатывает комплекс правил, процедур, приемов и методов, средств обеспечения защиты информации, в том числе с использованием современных методов и программного инструментария искусственного интеллекта	Решение стандартных практических задач	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены
	владеть инструментальными средствами реализущими подходы к классификации и прогнозированию угроз безопасности информации, а так же оцениванию последствий от реализации угроз безопасности информации в КС и авто-	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачи не решены

	матизированных системах			

7.2 Примерный перечень оценочных средств (типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности)

7.2.1 Примерный перечень заданий для подготовки к тестированию

1.Какой метод искусственного интеллекта может быть использован для обнаружения аномального поведения в сетевом трафике?

a)Метод глубокого обучения нейронных сетей.+

b)Метод шифрования данных.

c)Метод машинного обучения на основе правил.+

2.Какой метод искусственного интеллекта может быть использован для автоматического обнаружения и классификации вредоносных программ?

a)Метод кластеризации данных.

b)Метод анализа эмоциональной тональности текстов.

c)Метод машинного обучения на основе алгоритма случайного леса+

3.Какой метод искусственного интеллекта может быть использован для предсказания вероятности возникновения угроз информационной безопасности?

a)Метод регрессии.+

b)Метод сжатия данных.

c)Метод генетических алгоритмов.

4.Какой метод искусственного интеллекта может быть использован для защиты от спама и фишинга?

a)Метод случайного блуждания.

b)Метод байесовской фильтрации.+

c)Метод оптимизации функций.

5.Какой метод искусственного интеллекта может быть использован для обнаружения и анализа уязвимостей в приложениях?

a)Метод генетического программирования.+

b)Метод преобразования Фурье.

c)Метод рекомендательных систем.

6.Какой метод искусственного интеллекта может быть использован для автоматического разбора и анализа больших объемов текстовых данных?

a)Метод нейронных сетей с долгой краткосрочной памятью (LSTM).+

b)Метод динамического программирования.

c)Метод градиентного спуска.

7.Какой метод искусственного интеллекта может быть использован для автоматического распознавания образов на изображениях?

a)Метод сверточных нейронных сетей.+

b)Метод статистической классификации.

c)Метод группировки данных.

8.Какой метод искусственного интеллекта может быть использован для защиты от атак переполнения буфера?

a)Метод проверки формальных спецификаций.+

b)Метод ансамбля моделей.

c)Метод трансформации данных.

9.Какой метод искусственного интеллекта может быть использован для анализа и обработки больших объемов данных в реальном времени?

a)Метод стриминговой обработки данных.+

b)Метод графовых баз данных.

c)Метод анализа временных рядов.

10.Какой метод искусственного интеллекта может быть использован для автоматического обнаружения и предотвращения атак на сетевую инфраструктуру?

a)Метод усиленного обучения.+

b)Метод опорных векторов.

c)Метод случайного поиска.

7.2.2 Примерный перечень заданий для решения стандартных задач

1. Самым известным среди эволюционных алгоритмов является ...

генетический алгоритм

метод группового учета аргументов

алгоритм поиска глобального экстремума

алгоритм конкурирующих точек

2. Какой генетический оператор наиболее важный:

мутация

кроссовер

инверсия

3. Что является ключевой эвристикой всех эволюционных методов?

перебор всех объектов

отбор наилучших объектов

отсечение ложных объектов

4. Сколько может иметь поддеревьев каждый из узлов бинарного дерева?

1

2 +

3

4

5. Любой элемент в правой части бинарного дерева должен быть …. корня

меньше

больше

равен

не имеет значения

6. Любой элемент в левой части бинарного дерева должен быть …. корня

меньше

больше

равен

не имеет значения

7. Физический принцип действия (ФПД) - это ориентированный граф, вершинами которого являются физические объекты B, а ребрами входные A и выходные C потоки?

да +

нет

8. На какой модели базируется описание технической функции?

на модели "черный ящик"

на структурированной модели

на организационной модели

9. Сколько уровней описания имеет ФТЭ?

1

2

3 +

4

10. На первом уровне описания ФТЭ приводится следующая информация:

стандартная карта описания ФТЭ

самое короткое качественное описание ФТЭ

более подробное описание ФТЭ

7.2.3 Примерный перечень заданий для решения прикладных задач

Задача 1. Разработка алгоритма машинного обучения для обнаружения вредоносных программ в компьютерных системах.

Эталонный ответ:

```
import pandas as pd
from sklearn.model_selection import train_test_split
from sklearn.ensemble import RandomForestClassifier

# Загрузка данных
data = pd.read_csv('malware_dataset.csv')

# Разделение данных на обучающую и тестовую выборки
X = data.drop('label', axis=1)
y = data['label']
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2, random_state=42)

# Обучение модели случайного леса
model = RandomForestClassifier()
model.fit(X_train, y_train)

# Оценка точности модели
accuracy = model.score(X_test, y_test)
print("Точность модели:", accuracy)
```

Задача 2. Создание системы мониторинга сетевого трафика для обнаружения атак на компьютерные сети.

Эталонный ответ:

```
import scapy.all as scapy

# Функция для обработки пакетов
def process_packet(packet):
    # Реализуйте здесь логику обработки пакетов и обнаружения атак

# Захват пакетов
scapy.sniff(iface='eth0', prn=process_packet)
```

Задача 3. Разработка алгоритма генетического программирования для оптимизации параметров безопасности компьютерных систем.

Эталонный ответ:

```
import random

# Функция для оценки приспособленности
def fitness_function(solution):
    # Реализуйте здесь логику оценки приспособленности решения

# Генерация начальной популяции
population = [random.randint(0, 1) for _ in range(10)]

# Оптимизация параметров с помощью генетического программирования
for _ in range(100):
    # Реализуйте здесь логику генетического программирования

# Вывод оптимального решения
print("Оптимальное решение:", population[0])
```

Задача 4. Создание системы автоматического анализа логов для обнаружения необычной активности в компьютерных системах.

Эталонный ответ:

```
import pandas as pd

# Загрузка логов
logs = pd.read_csv('system_logs.csv')

# Анализ логов и обнаружение необычной активности
# Реализуйте здесь логику анализа логов и обнаружения необычной активности
```

Задача 5. Разработка алгоритма машинного обучения для предсказания уязвимостей в компьютерных системах и сетях.

Эталонный ответ:

```
import pandas as pd
from sklearn.model_selection import train_test_split
from sklearn.linear_model import LogisticRegression

# Загрузка данных
data = pd.read_csv('vulnerability_dataset.csv')

# Разделение данных на обучающую и тестовую выборки
X = data.drop('vulnerable', axis=1)
y = data['vulnerable']
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2, random_state=42)

# Обучение модели логистической регрессии
model = LogisticRegression()
model.fit(X_train, y_train)

# Оценка точности модели
accuracy = model.score(X_test, y_test)
print("Точность модели:", accuracy)
```

Задача 6. Создание системы автоматического обнаружения и реагирования на атаки типа DDoS.

Эталонный ответ:

```
import scapy.all as scapy

# Функция для обработки пакетов
def process_packet(packet):
    # Реализуйте здесь логику обработки пакетов и обнаружения атак DDoS

# Захват пакетов
scapy.sniff(iface='eth0', prn=process_packet)
```

Задача 7. Разработка алгоритма машинного обучения для идентификации и аутентификации пользователей в компьютерных системах.

Эталонный ответ:

```
import pandas as pd
from sklearn.model_selection import train_test_split
from sklearn.svm import SVC
```

```
# Загрузка данных
data = pd.read_csv('user_authentication_dataset.csv')

# Разделение данных на обучающую и тестовую выборки
X = data.drop('authenticated', axis=1)
y = data['authenticated']
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2, ran-
dom_state=42)

# Обучение модели методом опорных векторов
model = SVC()
model.fit(X_train, y_train)

# Оценка точности модели
accuracy = model.score(X_test, y_test)
print("Точность модели:", accuracy)
```

Задача 8. Создание системы автоматического обнаружения и блокирования фишинговых атак.

Эталонный ответ:

```
import requests
# Функция для проверки URL-адреса на фишинговую активность
def check_phishing(url):
    # Реализуйте здесь логику проверки URL-адреса на фишинговую
активность

# Пример использования
url = "https://example.com"
is_phishing = check_phishing(url)
print("Фишинговая активность:", is_phishing)
```

Задача 9. Разработка алгоритма машинного обучения для обнаружения аномального поведения пользователей в компьютерных системах.

Эталонный ответ:

```
import pandas as pd
from sklearn.model_selection import train_test_split
from sklearn.ensemble import IsolationForest
# Загрузка данных
data = pd.read_csv('user_behavior_dataset.csv')

# Разделение данных на обучающую и тестовую выборки
X = data.drop('normal', axis=1)
y = data['normal']
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.2, ran-
```

dom_state=42)

```
# Обучение модели леса изолирующих деревьев
model = IsolationForest()
model.fit(X_train)

# Оценка точности модели
accuracy = model.score(X_test)
print("Точность модели:", accuracy)
```

Задача 10. Создание системы автоматического обнаружения и предотвращения утечки конфиденциальной информации из компьютерных систем.

Эталонный ответ:

```
import pandas as pd
# Функция для обнаружения утечки конфиденциальной информации
def detect_data_leak(data):
    # Реализуйте здесь логику обнаружения утечки конфиденциальной информации
# Пример использования
data = pd.read_csv('sensitive_data.csv')
leak_detected = detect_data_leak(data)
print("Утечка конфиденциальной информации:", leak_detected)
```

7.2.4 Примерный перечень вопросов для подготовки к зачету

1.Определение искусственного интеллекта. Задачи искусственного интеллекта.

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

3.Основы технологий больших данных. Особенности применения. Архитектуры организации систем Big Data. Big Data и Data Mining.

4. Технологии Больших данных. Hadoop. Инфраструктура больших данных. Настройка авторизации в озере данных Hadoop

5. Apache Hadoop. Файловая система HDFS. Защита данных HDFS. Настройка политик аудита в Hadoop

6. Модель распределённых вычислений MapReduce.

7. Apache Kafka - распределенная платформа для потоковой обработки данных

8. Обеспечение безопасности Apache Kafka в кластере Big Data. Управление доступом.

9. Настройка безопасности периметра с Apache Knox Gateway.

10. Комплексное управление безопасностью кластера Hadoop с Apache Ranger

11. Архитектура распределенного приложения Spark. Основные кон-

цепции: RDD и DAG

12. Архитектура распределенного приложения Spark. Трансформации и действия. Материализация приложения.

13. DataFrame API и Spark SQL

14. Реализация методов регрессии, классификации и кластеризации в PySpark.

15. Нейросети в PySpark

15. Задачи обучения по прецедентам. Байесовские методы классификации.

16. Метрические методы классификации: метод ближайшего соседа и его обобщения.

17. Метод стохастического градиента.

18. Логистическая регрессия.

19. Метод опорных векторов

20. Линейная регрессия. Нелинейные методы восстановления регрессии.

21. Искусственные нейронные сети. Проблема полноты. Многослойные нейронные сети.

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

23. Основы теории агентов и мультиагентных систем. Основные понятия. Современные подходы к решению распределенных задач.

24.Модели коллективного поведения. Виды моделей. Модели кооперации агентов.

25. Конфликты в мультиагентных системах. Основные типы конфликтов. Механизмы разрешения конфликтов. Инструментарий программирования МАС.

26. Обнаружение и предотвращение вторжений. Обнаружение и изучение вредоносной активности на конечных точках: подключенных к сети рабочих станциях, серверах, устройствах Интернета вещей (EDR).

27. SIEM-системы использующие технологии искусственного интеллекта.

28. Предотвращение утечек информации (DLP).

29. Обнаружения и блокирования сетевых атак на веб-приложение (WAF).

30. Поведенческий анализ действий пользователей (UEBA).

31. Адаптивная аутентификация.

32. Концепция атаки уклонением на нейросетевые модели. Существующие атаки уклонением и методы защиты моделей от атак данного типа.

33. Принципы работы FGSM, PGD, семейство атак Карлини и Вагнера, атака Brendel & Bethge, Universal Adversarial Perturbations

34. Концепция атак извлечением данных. Существующие атаки извлечением данных на модели и методы защиты моделей от атак данного типа.

35. Подходы к извлечению текстовых данных из лингвистических моделей.

36. Подходы к извлечению данных из моделей, работающих с изображениями.

37. Концепция атаки отравлением данных на нейросетевые модели. Существующие атаки отравлением данных и методы защиты моделей от атак данного типа

38. Принципы работы Adversarial Backdoor Embedding, Clean Label Feature Collision Attack, Clean-Label Backdoor Attack

39. Концепция инверсионных атак. Существующие инверсионные атаки и методы защиты моделей от атак данного типа.

40. Методы атак на основе запросов. Дифференциальные атаки. Атаки по побочным каналам.

41. Методы формальной верификации моделей машинного обучения. Верификация на основе ограничений. Абстрактная верификация.

42. Методы оценки устойчивости моделей машинного обучения к внешним воздействиям

7.2.5 Примерный перечень заданий для решения прикладных задач

Не предусмотрено учебным планом

7.2.6. Методика выставления оценки при проведении промежуточной аттестации

Зачёт проводится по билетам, каждый из которых содержит 3 вопроса и 2 задачи. Для проверки усвоения компетенции, в билет включается один из вопросов, выданных на самостоятельное изучение. Каждый правильный ответ на вопрос в билете оценивается 3 баллами, задача оценивается в 5 баллов. Максимальное количество набранных баллов - 19.

1. Отметка «Зачтено» ставится в случае, если студент набрал 10-19 баллов.

2. Отметка «Незачтено» ставится в случае, если правильные ответы только на теоретические вопросы или решены только практические задачи, или студент набрал менее 8 баллов.

7.2.7 Паспорт оценочных материалов

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции	Наименование оценочного средства
1	Введение в искусственный интеллект	ПК-7.1	Тест, защита практических работ, защита реферата
2	Введение в технологии BIG DATA	ПК-7.1	Тест, защита практических работ, защита реферата
3	Машинное обучение	ПК-7.1	Тест, защита практических работ, защита реферата
4	Подходы к представлению знаний	ПК-7.1	Тест, защита практических работ, защита ре-

			ферата
5	Мультиагентные системы	ПК-7.1	Тест, защита практических работ, защита реферата
6	Применение ИИ в задачах обеспечения	ПК-7.1	Тест, защита практических работ, защита реферата

7.3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Тестирование осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных тест-заданий на бумажном носителе. Время тестирования 30 мин. Затем осуществляется проверка теста экзаменатором и выставляется оценка согласно методики выставления оценки при проведении промежуточной аттестации.

Решение стандартных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

Решение прикладных задач осуществляется, либо при помощи компьютерной системы тестирования, либо с использованием выданных задач на бумажном носителе. Время решения задач 30 мин. Затем осуществляется проверка решения задач экзаменатором и выставляется оценка, согласно методики выставления оценки при проведении промежуточной аттестации.

8 УЧЕБНО МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ)

8.1 Перечень учебной литературы, необходимой для освоения дисциплины

Основная

1. Остроух, А. В. Системы искусственного интеллекта: монография / А. В. Остроух, Н. Е. Суркова. — 2-е изд., стер. — Санкт-Петербург: Лань, 2021. — 228 с. — ISBN 978-5-8114-8519-2. — Текст : электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/176662.

2. Гусарова, Н. Ф. Введение в теорию искусственного интеллекта : учебное пособие / Н. Ф. Гусарова. — Санкт-Петербург : НИУ ИТМО, 2018. — 62 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/136515

Дополнительная

3. Романов, П. С. Системы искусственного интеллекта. Моделирование нейронных сетей в системе MATLAB. Лабораторный практикум : учебное пособие для вузов / П. С. Романов, И. П. Романова. —

Санкт-Петербург: Лань, 2021. — 140 с. — ISBN 978-5-8114-7747-0. — Текст : электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/179031.

4. Шелухин, О. И. Обнаружение вторжений в компьютерные сети (сете-вые аномалии): учебное пособие / О. И. Шелухин, Д. Ж. Сакалема, А. С. Филинова; под редакцией О. И. Шелухина. — Москва: Горячая линия-Телеком, 2018. — 220 с. — ISBN 978-5-9912-0323-4. — Текст : электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/111119

5. Адилов, Р. М. Системы искусственного интеллекта. Модуль2. Экспертные системы: учебно-методическое пособие / Р. М. Адилов. — Пенза: ПензГТУ, 2012. — 34 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/62762

8.2 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень лицензионного программного обеспечения, ресурсов информационно-телекоммуникационной сети «Интернет», современных профессиональных баз данных и информационных справочных систем:

Список ресурсов по искусственному интеллекту
https://github.com/owainlewis/awesome-artificial-intelligence
Все об обработке и анализе данных
https://medium.com/kaggle-blog
Ресурсы по глубокому обучению
http://deeplearning.net/software_links/
Библиотеки для глубокого обучения
http://www.teglor.com/b/deep-learning-libraries-language-cm569/

Kaggle (https://www.kaggle.com/) - платформа для соревнований по анализу данных и машинному обучению. Здесь вы можете найти различные состязания, связанные с состязательным машинным обучением, и присоединиться к ним. Вы можете изучать код других участников, участвовать в дискуссиях и получать опыт, работая над реальными задачами.

OpenAI Gym (https://gym.openai.com/) - это набор инструментов для разработки и сравнения алгоритмов обучения с подкреплением. Здесь вы найдете широкий выбор сред с состязательными задачами, такими как игры на двоих или многоагентные среды. Вы можете использовать этот ресурс для изучения и экспериментирования с состязательныма-шинным обучением.

Ar (https://arxiv.org/) - архив научных статей, где исследователи публикуют свои работы. Вы можете использовать поиск на Arxiv, чтобы найти статьи и документы, связанные с состязательным машинным обучением. Здесь вы найдете последние исследования и новейшие подходы к этой области

.

9 МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Специализированная лекционная аудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой. Дисплейный класс, оснащенный компьютерными программами для проведения лабораторного практикума.

10. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

По дисциплине «Обеспечение безопасности автоматизированных систем на основе методов искусственного интеллекта» читаются лекции, проводятся практические занятия.

Основой изучения дисциплины являются лекции, на которых излагаются наиболее существенные и трудные вопросы, а также вопросы, не нашедшие отражения в учебной литературе.

Практические занятия направлены на приобретение практических навыков реализации методов машинного обучения для задач обеспечения информационной безопасности. Занятия проводятся путем решения конкретных задач в аудитории.

Вид учебных занятий	Деятельность студента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Практическое занятие	Конспектирование рекомендуемых источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы. Прослушивание аудио- и видеозаписей по заданной теме, выполнение расчетно-графических заданий, решение задач по алгоритму.
Самостоятельная работа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; выполнение домашних заданий и расчетов; работа над темами для самостоятельного изучения; участие в работе студенческих научных конференций, олимпиад; подготовка к промежуточной аттестации.
Подготовка к промежуточной аттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом три дня эффективнее всего использовать для повторения и систематизации материала.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Перечень вносимых изменений	Дата внесения изменений	Подпись заведующего кафедрой, ответственной за реализацию ОПОП