Методические рекомендации и план проведения занятия

А.Е. Сулавко, П.С. Ложников

Защищенное исполнение искусственного интеллекта

Методические рекомендации и план проведения занятия по дисциплине «**Защищенное исполнение искусственного интеллекта**»

к лекции № 1 «**Введение**»

\_\_\_\_\_ учебная группа "\_\_\_\_\_"\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_ г. аудитория №\_\_\_\_

Учебное время **– 2 часа**

1. **Вид занятия:** Лекция.
2. **ТЕМА:** Введение в курс «**Защищенное исполнение искусственного интеллекта**».
3. **Тема занятия:** Ознакомление с темами занятий в рамках учебного плана. Введение в ИИ. Защищенное исполнение моделей ИИ. Виды состязательных атак.

**Целевая установка:** ознакомить студентов с предметом, объёмом и содержанием учебной дисциплины. Провести краткое введение в курс.

1. **Основные вопросы занятия и планируемое время**

Вводная часть 5 мин.

Объявление темы, цели и порядка проведения занятия

Выдача раздаточных материалов (электронные материалы, ссылки)

Основная часть 80 мин.

Заключительная часть 5 мин.

1. **Перечень применяемых наглядных пособий и технических средств**

ПЭВМ, проектор, экран.

Опорный конспект.

**Литература для самостоятельной подготовки**

Необходимая литература для качественного изучения и освоения материалов данной дисциплины представлена в рабочей программе дисциплины «**Защищенное исполнение искусственного интеллекта**».

**Методические приемы**

1. Использование комплекта слайдов по теме занятия.
2. Использование раздаточного материала: электронные материалы, ссылки.
3. Использование примеров из профильных учебных дисциплин.
4. Проведение систематического текущего контроля обучающихся: опрос по пройдённому материалу.

**Контрольные вопросы по пройденному материалу и теме занятия**

**(с учетом применения соответствующих ТСО)**

**Задание на самостоятельную работу**

Введение в ИИ. Защищенное исполнение моделей ИИ. Изучить виды состязательных атак.

План составил

к.т.н., доцент

А.Е. Сулавко

"\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2022 г.

Методические рекомендации и план проведения занятия по дисциплине **«Защищенное исполнение искусственного интеллекта»**

к лекции № 2 **«Защищенное исполнение нейросетевых алгоритмов на базе линейных нейронов»**

\_\_\_\_\_ учебная группа "\_\_\_\_\_"\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_ г. аудитория №\_\_\_\_

Учебное время **– 2 часа**

1. **Вид занятия:** Лекция.
2. **ТЕМА: Защищенное исполнение нейросетевых алгоритмов на базе линейных нейронов**.
3. **Тема занятия:** Атака извлечения знаний на примере нейросетевых преобразователей биометрия­-код (НПБК). Энтропия выходов НПБК. Концепция защищенных нейросетевых контейнеров (ЗНК). Реализация НПБК и ЗНК.

**Целевая установка:** Ознакомить студентов с понятиями НПБК и ЗНК (защищенными нейросетевыми контейнерами), их концепцией.

1. **Основные вопросы занятия и планируемое время**

Вводная часть 5 мин.

Объявление темы, цели и порядка проведения занятия

Выдача раздаточных материалов (электронные материалы, ссылки)

Основная часть 80 мин.

Заключительная часть 5 мин.

1. **Перечень применяемых наглядных пособий и технических средств**

ПЭВМ, проектор, экран.

Опорный конспект.

**Литература для самостоятельной подготовки**

Необходимая литература для качественного изучения и освоения материалов данной дисциплины представлена в рабочей программе дисциплины «Защищенное исполнение искусственного интеллекта».

**Методические приемы**

1. Использование комплекта слайдов по теме занятия.
2. Использование раздаточного материала: электронные материалы, ссылки.
3. Использование примеров из профильных учебных дисциплин.
4. Проведение систематического текущего контроля обучающихся: опрос по пройдённому материалу.

**Контрольные вопросы по пройденному материалу и теме занятия**

**(с учетом применения соответствующих ТСО)**

**Задание на самостоятельную работу**

Изучить ГОСТ Р 52633.5. Рассмотреть защищенное исполнение нейросетевых алгоритмов на базе линейных нейронов.

План составил

к.т.н., доцент

А.Е. Сулавко

"\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2022 г.

Методические рекомендации и план проведения занятия по дисциплине «**Защищенное исполнение искусственного интеллекта**»

к лекции № 3 **«Защищенное исполнение нейросетевых алгоритмов на базе квадратичных нейронов»**

\_\_\_\_\_ учебная группа "\_\_\_\_\_"\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_ г. аудитория №\_\_\_\_

Учебное время **– 2 часа**

1. **Вид занятия:** Лекция.
2. **ТЕМА:** Защищенное исполнение нейросетевых алгоритмов на базе квадратичных нейронов.
3. **Тема занятия:** Плоское пространство признаков и мера Минковского. Спрямляющее пространство признаков. Проклятье размерности. Cети радиально-­базисных функций. Защищенное исполнение сетей квадратичных нейронов.

**Целевая установка:** ознакомить студентов с концепцией построения пространства признаков, проблемой проклятья размерности, сетями радиально-базисных функций. Сформировать представление о защищенном исполнении сетей квадратичных нейронов.

1. **Основные вопросы занятия и планируемое время**

Вводная часть 5 мин.

Объявление темы, цели и порядка проведения занятия

Выдача раздаточных материалов (электронные материалы, ссылки)

Основная часть 80 мин.

Заключительная часть 5 мин.

1. **Перечень применяемых наглядных пособий и технических средств**

ПЭВМ, проектор, экран.

Опорный конспект.

**Литература для самостоятельной подготовки**

Необходимая литература для качественного изучения и освоения материалов данной дисциплины представлена в рабочей программе дисциплины «Защищенное исполнение искусственного интеллекта».

**Методические приемы**

1. Использование комплекта слайдов по теме занятия.
2. Использование раздаточного материала: электронные материалы, ссылки.
3. Использование примеров из профильных учебных дисциплин.
4. Проведение систематического текущего контроля обучающихся: опрос по пройдённому материалу.

**Контрольные вопросы по пройденному материалу и теме занятия**

**(с учетом применения соответствующих ТСО)**

**Задание на самостоятельную работу**

Изучить защищенное исполнение сетей квадратичных нейронов.

План составил

к.т.н., доцент

А.Е. Сулавко

"\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2022 г.

Методические рекомендации и план проведения занятия по дисциплине **«Защищенное исполнение искусственного интеллекта»**

к лекции № 4 **«Защищенное исполнение нейросетевых алгоритмов на базе корреляционных нейронов»**

\_\_\_\_\_ учебная группа "\_\_\_\_\_"\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_ г. аудитория №\_\_\_\_

Учебное время **– 4 часа**

1. **Вид занятия:** Лекция.
2. **ТЕМА:** Защищенное исполнение нейросетевых алгоритмов на базе корреляционных нейронов.
3. **Тема занятия:** Мера Байеса­-Минковского. Точечная оценка корреляции. Мета-­пространство признаков Байеса-­Минковского. Модели преобразователей образов в код на базе сетей корреляционных нейронов.

**Целевая установка:** ознакомить студентов понятием точечной оценки корреляции, а также с мерой и мета-пространством Байеса-Минковского. Сформировать представление о моделях преобразователей образов в код на базе сетей корреляционных нейронов.

1. **Основные вопросы занятия и планируемое время**

Вводная часть 5 мин.

Объявление темы, цели и порядка проведения занятия

Выдача раздаточных материалов (электронные материалы, ссылки)

Основная часть 200 мин.

Заключительная часть 5 мин.

1. **Перечень применяемых наглядных пособий и технических средств**

ПЭВМ, проектор, экран.

Опорный конспект.

**Литература для самостоятельной подготовки**

Необходимая литература для качественного изучения и освоения материалов данной дисциплины представлена в рабочей программе дисциплины «Защищенное исполнение искусственного интеллекта».

**Методические приемы**

1. Использование комплекта слайдов по теме занятия.
2. Использование раздаточного материала: электронные материалы, ссылки.
3. Использование примеров из профильных учебных дисциплин.
4. Проведение систематического текущего контроля обучающихся: опрос по пройдённому материалу.

**Контрольные вопросы по пройденному материалу и теме занятия**

**(с учетом применения соответствующих ТСО)**

**Задание на самостоятельную работу**

Изучить защищенное исполнение сетей корреляционных нейронов.

План составил

к.т.н., доцент

А.Е. Сулавко

"\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2022 г.

Методические рекомендации и план проведения занятия по дисциплине **«Защищенное исполнение искусственного интеллекта»**

к лекции № 5 **«Защищенное исполнение гибридных нейросетевых алгоритмов»**

\_\_\_\_\_ учебная группа "\_\_\_\_\_"\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_ г. аудитория №\_\_\_\_

Учебное время **– 4 часа**

1. **Вид занятия:** Лекция.
2. **ТЕМА:** Защищенное исполнение гибридных нейросетевых алгоритмов.
3. **Тема занятия:** Модели гибридные нейронных сетей и их преимущества. Дрейф моделей ИИ в защищенном исполнении. Автоматическое переобучение. Вариационные автокодировщики и их применение.

**Целевая установка:** ознакомить студентов с моделями гибридных нейронных сетей. Сформировать представление о дрейфе моделей в ИИ и понятии автоматического переобучения глубокой нейронной сети. Построить модели для извлечения признаков на базе нейронных сетей.

1. **Основные вопросы занятия и планируемое время**

Вводная часть 5 мин.

Объявление темы, цели и порядка проведения занятия

Выдача раздаточных материалов (электронные материалы, ссылки)

Основная часть 200 мин.

Заключительная часть 5 мин.

1. **Перечень применяемых наглядных пособий и технических средств**

ПЭВМ, проектор, экран.

Опорный конспект.

**Литература для самостоятельной подготовки**

Необходимая литература для качественного изучения и освоения материалов данной дисциплины представлена в рабочей программе дисциплины «Защищенное исполнение искусственного интеллекта».

**Методические приемы**

1. Использование комплекта слайдов по теме занятия.
2. Использование раздаточного материала: электронные материалы, ссылки.
3. Использование примеров из профильных учебных дисциплин.
4. Проведение систематического текущего контроля обучающихся: опрос по пройдённому материалу.

**Контрольные вопросы по пройденному материалу и теме занятия**

**(с учетом применения соответствующих ТСО)**

**Задание на самостоятельную работу:**

Изучить защищенное исполнение гибридных нейросетевых алгоритмов.

План составил

к.т.н., доцент

А.Е. Сулавко

"\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2022 г.

Методические рекомендации и план проведения занятия по дисциплине **«Защищенное исполнение искусственного интеллекта»**

к лекции № 6 **«Заключение»**

\_\_\_\_\_ учебная группа "\_\_\_\_\_"\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_ г. аудитория №\_\_\_\_

Учебное время **– 3 часа**

1. **Вид занятия:** Лекция.
2. **ТЕМА:** Заключение.
3. **Тема занятия:** Итоги курса. Перспективы развития нейросетевых моделей ИИ. Защищенное исполнение нейросетевых алгоритмов.

**Целевая установка:** подвести итоги курса, рассмотреть перспективы развития нейросетевых моделей ИИ.

1. **Основные вопросы занятия и планируемое время**

Вводная часть 5 мин.

Объявление темы, цели и порядка проведения занятия

Выдача раздаточных материалов (электронные материалы, ссылки)

Основная часть 150 мин.

Заключительная часть 5 мин.

1. **Перечень применяемых наглядных пособий и технических средств**

ПЭВМ, проектор, экран.

Опорный конспект.

**Литература для самостоятельной подготовки**

Необходимая литература для качественного изучения и освоения материалов данной дисциплины представлена в рабочей программе дисциплины «Защищенное исполнение искусственного интеллекта».

**Методические приемы**

1. Использование комплекта слайдов по теме занятия.
2. Использование раздаточного материала: электронные материалы, ссылки.
3. Использование примеров из профильных учебных дисциплин.
4. Проведение систематического текущего контроля обучающихся: опрос по пройдённому материалу.

**Контрольные вопросы по пройденному материалу и теме занятия**

**(с учетом применения соответствующих ТСО)**

**Задание на самостоятельную работу**

Рассмотреть перспективы развития нейросетевых моделей ИИ и подвести итоги по изучению защищенного исполнения нейросетевых алгоритмов.

План составил

к.т.н., доцент

А.Е. Сулавко

"\_\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2022 г.