6 Критерии оценивания и оценочные материалы

6.1 Критерии оценивания

Для дисциплины «Атаки на нейронные сети» формой промежуточной аттестации является зачет с оценкой.

Зачет с оценкой

Оценка	Описание
Неудовлетворительно	Курс не освоен. Студент испытывает серьезные трудности при ответе на ключевые вопросы дисциплины
Удовлетворительно	Студент в целом овладел курсом, но некоторые разделы освоены на уровне определений и формулировок теорем
Хорошо	Студент овладел курсом, но в отдельных вопросах испытывает затруднения. Умеет решать задачи
Отлично	Студент демонстрирует полное овладение курсом, способен применять полученные знания при решении конкретных задач.

Особенности допуска

Для допуска к экзамену студент должен успешно выполнить и защитить ИДЗ.

6.2 Оценочные материалы для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине

Примерные вопросы к дифф.зачету

№ п/п	Описание
1	Основные архитектуры нейронных сетей.
2	Состязательное машинное обучение. Примеры атак.
3	Классификация атак на модели машинного обучения по целям, времени и имеющейся информации.
4	Атака с уклонением. Способы осуществления и примеры.
5	Способы защиты от атак с уклонением.
6	Атака с отравлением данных. Способы осуществления и примеры.
7	Способы защиты от атак с уклонением.

Весь комплект контрольно-измерительных материалов для проверки сформированности компетенции (индикатора компетенции) размещен в закрытой части по адресу, указанному в п. 5.3

6.3 График текущего контроля успеваемости

Неделя	Темы занятий	Вид контроля
5	Атаки с уклонением	
6		
7		
8		ИДЗ / ИДРГЗ / ИДРЗ
10	Атаки с отравлением данных	
11		
12		ИДЗ / ИДРГЗ / ИДРЗ