

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по выполнению практических работ

по дисциплине

«АТАКИ НА СИСТЕМЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА»

для студентов направления подготовки 02.04.01 Математика и компьютерные
науки

профиль "Искусственный интеллект в кибербезопасности"

**Ставрополь
2026**

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	3
СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ ЗАНЯТИЙ	5
Практическая работа №1. Постановка проблемы доверия искусственному интеллекту. Обсуждение индивидуальных заданий	5
Практическая работа №2. Управление рисками искусственного интеллекта	5
Практическая работа №3. Реализация объяснимого искусственного интеллекта и метрики объяснимости.	6
Практическая работа №4. Оценка робастности модели искусственного интеллекта	6
Практическая работа №5. Реализация функциональной безопасности искусственного интеллекта	7
Практическая работа №6. Противодействие компьютерным атакам на искусственный интеллект.	7
Практическая работа №7. Защита данных, используемых в системе искусственного интеллекта на этапах хранения, обучения и использования.	8
Практическая работа №8. Обнаружение аномалий	8
1.	11
2.	12
3.	13
4.	13
5. Порядок выполнения самостоятельной работы студентом	15
5.1. Методические рекомендации по работе с учебной литературой	15
5.5. Методические рекомендации по созданию проекта (докладов, рефератов, эссе, научных статей и т.д.)	19
6.	18

ВВЕДЕНИЕ

Цель и задачи освоения дисциплины

Целью освоения дисциплины «Атаки на системы искусственного интеллекта» является формирование у будущего специалиста по направлению подготовки 02.04.01 Математика и компьютерные науки профиль «Искусственный интеллект в кибербезопасности» навыков и знаний в области выявления и анализа уязвимостей систем искусственного интеллекта (ИИ) и машинного обучения. Это включает в себя:

- Понимание основных методов атак на модели ИИ, таких как враждебные атаки и атаки на данные.
- Формирование практических навыков по разработке и реализации защитных мер против этих атак.
- Развитие способности анализировать и предотвращать потенциальные угрозы безопасности в системах ИИ.

Перечень осваиваемых компетенций:

Код	Формулировка
ПК-9	С помощью современных пакетов прикладных программ моделирования, исследует вновь создаваемые математические модели

Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы высшего образования

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций, индикаторов
ПК-9 С помощью современных пакетов прикладных программ моделирования, исследует вновь создаваемые математические модели	ИД-1 с помощью современных пакетов прикладных программ моделирования, исследует вновь создаваемые математические модели	знает как использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования.
ПК-9 С помощью	ИД-2 использует современные методы разработки алгоритмов	умеет использовать

современных пакетов прикладных программ моделирования, исследует вновь создаваемые математические модели	математических моделей	современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования
ПК-9 С помощью современных пакетов прикладных программ моделирования, исследует вновь создаваемые математические модели	ИД-3 использует современные языки программирования для реализации конкретных алгоритмов и математических моделей.	владеет навыками как использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования

СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Содержание отчетов

- Титульный лист
- Цель работы
- Формулировка задания
- Краткое описание выполнения основных этапов работы
- Выводы по работе

Практические работы

Практическая работа №1. Постановка проблемы доверия искусственному интеллекту. Обсуждение индивидуальных заданий

Цель работы: изучение компонентов и свойств доверенного искусственного интеллекта, уровней доверия с опорой на теоретический лекционный материал.

Задание:

Провести анализ индивидуального домашнего задания (ИДЗ), декомпозицию задач и построить план выполнения ИДЗ.

Контрольные вопросы:

1. Почему важно доверять системам искусственного интеллекта?
2. Приведите примеры ответственных задач обработки данных.
3. Сколько уровней доверия принято выделять на данный момент?
4. Перечислите основные компоненты доверенного искусственного интеллекта.
5. Какие вам известны аппаратные платформы для доверенного ИИ?

Практическая работа №2. Управление рисками искусственного интеллекта

Цель работы: изучение процесса управления рисками на основе информации из теоретического материала для конкретной модели искусственного интеллекта.

Задание:

Провести идентификацию, оценку рисков для конкретной модели искусственного интеллекта, выполнить анализ результатов оценки и описать необходимые шаги по их обработке.

Контрольные вопросы:

1. Какие вам известны принципы управления рисками согласно ИСО 31000:2018?

2. Перечислите, что должна включать в себя приверженность риск-менеджменту?
3. В зависимости от чего при определении рисков систем искусственного интеллекта следует учитывать различные источники рисков?
4. Что такое автономность искусственного интеллекта?
5. Что определяет степень прозрачности принятия решений?

Практическая работа №3. Реализация объяснимого искусственного интеллекта и метрики объяснимости.

Цель работы: получение навыков проектирования объяснимого искусственного интеллекта с использованием методов и подходов к реализации объяснимого ИИ (деревья решений, GA2M, TCAV, LIME, SHAP и другое) и получения метрик объяснимости.

Задание:

Выбрать метод или подход к оценке объяснимости. Провести проектирование модели искусственного интеллекта по индивидуальному заданию. Выполнить оценку объяснимости модели ИИ, рассчитать метрики объяснимости согласно выбранному подходу. Проанализировать результат.

Контрольные вопросы:

6. Дайте определение объяснимости согласно ГОСТ Р 59276-2020.
7. Какие составляющие включает в себя объяснимость искусственного интеллекта?
8. Какие выделяют методы отбора признаков?
9. Какие методы и подходы к реализации объяснимого искусственного интеллекта и оценке метрик объяснимости на данный момент известны?
10. Назовите несколько программных продуктов для создания объяснимого или повышения объяснимости искусственного интеллекта.

Практическая работа №4. Оценка робастности модели искусственного интеллекта

Цель работы: получение навыков оценки робастности модели искусственного интеллекта с применением методов оценки робастности с опорой на теоретический лекционный материал.

Задание:

Выполнить оценки метрик робастности модели искусственного интеллекта, построенной по индивидуальному заданию.

Контрольные вопросы:

1. Дайте определение понятию робастность.

2. В чем заключается главный принцип робастности в случае системы искусственного интеллекта?
3. Какие группы методов выделяют среди методов оценки робастности нейронных сетей?
4. Опишите типичный алгоритм для оценки робастности нейронных сетей.
5. Каким образом решают проблему недостаточной обучающей способности нейронных сетей?

Практическая работа №5. Реализация функциональной безопасности искусственного интеллекта

Цель работы: получение навыков управления безопасностью системы искусственного интеллекта.

Задание:

Выбрать для исследования систему искусственного интеллекта. Изучить состав технологических элементов системы. Описать методы, используемые для реализации функциональной безопасности в выбранной системе искусственного интеллекта. Привести описание с помощью чего реализован каждый технологический элемент. Выполнить анализ выбранного технологического элемента с точки зрения функциональной безопасности.

Контрольные вопросы:

1. Что понимают под функциональной безопасностью искусственного интеллекта?
2. На что направлена функциональная безопасность? Посредством чего достигается эта цель?
3. Опишите трехкомпонентную структуру системы искусственного интеллекта.
4. Какие технологические элементы на основе функциональных уровней экосистемы ИИ содержит процесс создания и выполнения модели искусственного интеллекта?
5. Приведите примеры языка или инструмента реализации каждого технологического элемента.

Практическая работа №6. Противодействие компьютерным атакам на искусственный интеллект.

Цель работы: получение навыков защиты от компьютерных атак на системы искусственного интеллекта.

Задание:

Выбрать определенный класс компьютерных атак на искусственный интеллект. Провести эксперимент по моделированию атаки на модель искусственного интеллекта. Выбрать метод противодействия атаке, опираясь на теоретический материал, реализовать выбранный метод для модели. Провести эксперимент по моделированию атаки на защищенную модель искусственного интеллекта.

Контрольные вопросы:

1. Какие принято выделять классы характерных атак на искусственный интеллект?
2. Сколько существует разновидностей атак? Назовите их.
3. Какие типы атак выделяют в зависимости от направления вектора атаки?
4. В какой ситуации атаки, направленные на извлечение входных данных, являются актуальными?
5. Дайте определение понятию состязательной атаки на искусственный интеллект? Что понимают под термином зондирование моделей?

Практическая работа №7. Защита данных, используемых в системе искусственного интеллекта на этапах хранения, обучения и использования.

Цель работы: получить навыки по защите данных в системе искусственного интеллекта

Задание: Выбрать конкретный вид атаки на данные на одном из этапов их обработки. Студент должен проанализировать материалы лекций, основную и дополнительную литературу, интернет источники, составить перечень способов защиты от атаки на данные, указав ссылки на источники с обоснованием эффективности способов защиты.

Контрольные вопросы:

1. Назовите два основных способа предотвращения атаки манипуляции с входными данными.
2. В каком случае атаки типа "ключ под ковриком" и атаки "на решающий бит" станут неосуществимы уже на уровне концепции построения ИИ?
3. Перечислите преимущества федеративного обучения?
4. Какие выделяют причины необходимости применения гомоморфного шифрования при разработке систем искусственного интеллекта?
5. Что является целью определения показателей конфиденциальности?
6. Перечислите несколько программных продуктов, где реализованы методы по защите конфиденциальности и целостности данных ИИ.

Практическая работа №8-9. Обнаружение аномалий

Цель работы: получение навыков по обнаружению аномалий искусственного интеллекта.

Задание:

Согласовать с преподавателем выбор типа аномалии. Студент должен проанализировать материалы лекций, основную и дополнительную литературу, интернет источники, привести подход к обнаружению выбранной аномалии и реализовать его для модели ИИ самостоятельно либо с помощью готового программного продукта. Выполнить эксперимент по моделированию обнаружения аномалий.

Контрольные вопросы:

1. Приведите определение дрейфа данных. С чем часто связан дрейф данных? Приведите пример такой ситуации.
2. Дайте определение понятию дрейф концепции. Каким примером можно описать дрейф концепции?
3. Когда утечка данных может стать актуальной угрозой для искусственного интеллекта? Приведите способы защиты от утечки данных.
4. Что должно рассматриваться для разработки приложений мониторинга ИИ?
5. Приведите примеры программных продуктов для обнаружения аномалий в данных.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

для обучающихся по организации и проведению самостоятельной работы

по дисциплине «АТАКИ НА СИСТЕМЫ ИСКУССТВЕННОГО
ИНТЕЛЛЕКТА»

для студентов направления подготовки

направленность (профиль):

Ставрополь

2026

1. Общие положения

Самостоятельная работа – планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студентов). Владиславу Вячеславовичу

Самостоятельная работа студентов (СРС) в ВУЗе является важным видом учебной и научной деятельности студента. Самостоятельная работа студентов играет значительную роль в рейтинговой технологии обучения.

К основным видам самостоятельной работы студентов относятся:

- формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);
- написание докладов;
- подготовка к семинарам, практическим и лабораторным работам, их оформление;
- составление аннотированного списка статей из соответствующих журналов по отраслям знаний (педагогических, психологических, методических и др.);
- выполнение учебно-исследовательских работ, проектная деятельность;
- подготовка практических разработок и рекомендаций по решению проблемной ситуации;
- выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и т.д.;
- компьютерный текущий самоконтроль и контроль успеваемости на базе электронных обучающих и аттестующих тестов;
- выполнение курсовых работ (проектов) в рамках дисциплин;

- выполнение выпускной квалификационной работы и др.

Методика организации самостоятельной работы студентов зависит от структуры, характера и особенностей изучаемой дисциплины, объема часов на ее изучение, вида заданий для самостоятельной работы студентов, индивидуальных качеств студентов и условий учебной деятельности.

Процесс организации самостоятельной работы студентов включает в себя следующие этапы:

- подготовительный (определение целей, составление программы, подготовка методического обеспечения, подготовка оборудования);
- основной (реализация программы, использование приемов поиска информации, усвоения, переработки, применения, передачи знаний, фиксирование результатов, самоорганизация процесса работы);
- заключительный (оценка значимости и анализ результатов, их систематизация, оценка эффективности программы и приемов работы, выводы о направлениях оптимизации труда).

Самостоятельная работа по дисциплине «Информационные технологии командной работы и проектной деятельности» направлена на формирование следующих **компетенций**:

Код	Формулировка
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений
УК-3	Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде

2. Цель и задачи самостоятельной работы

Ведущая цель организации и осуществления СРС совпадает с целью обучения студента – формирование набора общенаучных, профессиональных и универсальных компетенций будущего бакалавра.

При организации СРС важным и необходимым условием становятся формирование умения самостоятельной работы для приобретения знаний, навыков и возможности организации учебной и научной деятельности. Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов

способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Задачами СРС являются:

- систематизация и закрепление полученных теоретических знаний и практических умений студентов;
- углубление и расширение теоретических знаний;
- формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развитие исследовательских умений;
- использование материала, собранного и полученного в ходе самостоятельной работы и лабораторных занятий.

3. Технологическая карта самостоятельной работы студента

Коды реализуемых компетенций	Вид деятельности студентов	Итоговый продукт самостоятельной работы	Средства и технологии оценки	Объем часов, в том числе (астр.)		
				СРС	Контактная работа с преподавателем	Всего
3 семестр						
ПК-9	Подготовка к лекциям	Конспект лекций	Собеседование	27,0	9,0	36,0
ПК-9	Подготовка к практическим занятиям	Отчет в электронном виде	Собеседование	27,0	9,0	36,0
ПК-9	Самостоятельное изучение литературы	Конспект	Собеседование	27,0	9,0	36,0
ПК-9	Самотестирование, подготовка к тестированию	Тестирование	Тестовые задания	27,0	9,0	36,0
Итого за 3 семестр				108,0	36,0	144,0
Итого				108,0	36,0	144,0

4. Контрольные точки и виды отчетности по ним

Контроль качества и сроков самостоятельной работы выполняется в соответствии с учебным графиком и оформляется в соответствии с заданием. Предусмотрена следующая рейтинговая оценка знаний

Описание шкалы оценивания

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации.

Текущий контроль

5. Порядок выполнения самостоятельной работы студентом

5.1. Методические рекомендации по работе с учебной литературой

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги.

Важно помнить, что рациональные навыки работы с книгой - это всегда большая экономия времени и сил.

Правильный подбор учебников рекомендуется преподавателем, читающим лекционный курс. Необходимая литература может быть также указана в методических разработках по данному курсу.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

При изучении любой дисциплины большую и важную роль играет самостоятельная индивидуальная работа.

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно. Нужно добиваться точного представления о том, что изучаешь. Полезно составлять опорные конспекты. При изучении материала по учебнику полезно в тетради (на специально отведенных полях) дополнять конспект лекций. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Опыт показывает, что многим студентам помогает составление листа опорных сигналов, содержащего важнейшие и наиболее часто употребляемые формулы и понятия. Такой лист помогает запомнить формулы, основные положения лекции, а также может служить постоянным справочником для студента.

Чтение научного текста является частью познавательной деятельности. Ее цель – извлечение из текста необходимой информации. От того насколько осознанна читающим собственная внутренняя установка при обращении к печатному слову (найти нужные сведения, усвоить информацию полностью или частично, критически проанализировать материал и т.п.) во многом зависит эффективность осуществляемого действия.

Выделяют **четыре основные установки в чтении научного текста:**

информационно-поисковый (задача – найти, выделить искомую информацию)

усваивающая (усилия читателя направлены на то, чтобы как можно полнее осознать и запомнить как сами сведения излагаемые автором, так и всю логику его рассуждений)

аналитико-критическая (читатель стремится критически осмыслить материал, проанализировав его, определив свое отношение к нему)

творческая (создает у читателя готовность в том или ином виде – как отправной пункт для своих рассуждений, как образ для действия по аналогии и т.п. – использовать суждения автора, ход его мыслей, результат наблюдения, разработанную методику, дополнить их, подвергнуть новой проверке).

Основные виды систематизированной записи прочитанного:

Аннотирование – предельно краткое связанное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;

Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;

Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;

Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

5.2. Методические рекомендации по составлению конспекта лекций:

1. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта.

2. Выделите главное, составьте план.

3. Кратко сформулируйте основные положения текста, отметьте аргументацию автора.

4. Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.

5. Грамотно записывайте цитаты. Цитируя, учитывайте лаконичность, значимость мысли.

В тексте конспекта желательно приводить не только тезисные положения, но и их доказательства. При оформлении конспекта необходимо стремиться к емкости каждого предложения. Мысли автора книги следует излагать кратко, заботясь о стиле и выразительности написанного. Число дополнительных элементов конспекта должно быть логически обоснованным, записи должны распределяться в определенной последовательности, отвечающей логической структуре произведения. Для уточнения и дополнения необходимо оставлять поля.

Овладение навыками конспектирования требует от студента целеустремленности, повседневной самостоятельной работы.

5.3. Методические рекомендации по подготовке к практическим занятиям

Для того чтобы практические занятия приносили максимальную пользу, необходимо помнить, что упражнение и решение задач проводятся по вычитанному на лекциях материалу и связаны, как правило, с детальным разбором отдельных вопросов лекционного курса. Следует подчеркнуть, что только после усвоения лекционного материала с определенной точки зрения (а именно с той, с которой он излагается на лекциях) он будет закрепляться на лабораторных занятиях как в результате обсуждения и анализа лекционного материала, так и с помощью решения проблемных ситуаций, задач. При этих условиях студент не только хорошо усвоит материал, но и научится применять его на практике, а также получит дополнительный стимул (и это очень важно) для активной проработки лекции.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы (задачи), то нужно сравнить их и выбрать самый рациональный. Полезно до начала вычислений составить краткий план решения проблемы (задачи). Решение проблемных задач или примеров следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Полученный ответ следует проверить способами, вытекающими из существа данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты. Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

Практические работы № 1-5,8 выполняются студентами заочной и очно-заочной формы обучения самостоятельно.

5.4. Методические рекомендации по самопроверке знаний

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих задач на практических занятиях и самостоятельно

студенту рекомендуется провести самопроверку усвоенных знаний, ответив на контрольные вопросы по изученной теме.

В случае необходимости нужно еще раз внимательно разобраться в материале.

Иногда недостаточность усвоения того или иного вопроса выясняется только при изучении дальнейшего материала. В этом случае надо вернуться назад и повторить плохо усвоенный материал. Важный критерий усвоения теоретического материала – умение отвечать на вопросы для собеседования.

Критерии оценки:

Оценка «отлично» выставляется студенту, если он, отлично знает как использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования, отлично умеет использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования, отлично владеет навыками как использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования.

Оценка «хорошо» выставляется студенту, если он, знает как использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования, умеет использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования, владеет навыками как использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования.

Оценка «удовлетворительно» выставляется студенту, если он, плохо знает как использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования, плохо умеет использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования, плохо владеет навыками как использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования.

Оценка «неудовлетворительно» выставляется студенту, если он, не знает как использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования, не умеет использовать современные методы разработки и реализации конкретных

алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования, не владеет навыками как использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования.

Описание шкалы оценивания

Максимально возможный балл за весь текущий контроль устанавливается равным 55. Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставаемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	100
Хороший	80
Удовлетворительный	60
Неудовлетворительный	0

5.6. Методические рекомендации по подготовке к зачетам

Контроль самостоятельной работы студентов

Контроль самостоятельной работы проводится преподавателем в аудитории.

Предусмотрены следующие виды контроля: собеседование, оценка выполнения доклада и его презентации.

Подробные критерии оценивания компетенций приведены в Фонде оценочных средств для проведения текущей и промежуточной аттестации.

6. Список литературы для выполнения СРС

Перечень основной литературы

1. Сивков Д.И., Калугина А.С. "Обзор существующих атак на системы, основанные на искусственном интеллекте" (Научный журнал, 2024) — Обзор методов атак на системы ИИ, включая атаки на обученные модели и системы идентификации.
2. Подтопельный В.В. "Особенности моделирования атак на модели искусственного интеллекта" (Журнал ТУСУР, 2024) — Рассмотрение проблем моделирования атак на модели ИИ и формирование вектора атаки.

3. Котенко И.В., Саенко И.Б., Лаута О.С., Васильев Н.А., Садовников В.Е. "Атаки и методы защиты в системах машинного обучения" (CyberRus, 2024) — Анализ атак на системы машинного обучения и методов защиты от них.

Перечень дополнительной литературы

1. Артамонов А. «Безопасность искусственного интеллекта» (itzashita.ru, 2022) — обзор атак на модели машинного обучения и методов защиты.
2. Шакла Н. «Машинное обучение и TensorFlow» (перевод с английского) — основы машинного обучения и TensorFlow, которые могут быть полезны для понимания атак на ИИ.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Атаки на системы искусственного интеллекта». Ставрополь : СКФУ, 2025.
2. Методические указания к практическим занятиям по дисциплине «Атаки на системы искусственного интеллекта». Ставрополь : СКФУ, 2025.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. <http://biblioclub.ru/> – Университетская библиотека online "Библиоклуб"
2. <https://4brain.ru/liderstvo/> – Лидерство: уроки эффективного руководителя
3. <https://spravochnick.ru/psihologiya/> – Справочник по психологии