

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Грובה Татьяна Анатольевна

Должность: и.о. декана факультета математики и компьютерных наук имени
профессора Н.И. Червякова

Дата подписания: 19.06.2026 15:10:47

Уникальный программный ключ:

bd39d4208aa94cf4422feb787c81619d42de79a7

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования

«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

И.о. декана факультета
математики и компьютерных
наук имени профессора Н. И.
Червякова
Грובה Т. А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Атаки на системы искусственного интеллекта

Направление подготовки

02.04.01 Математика и компьютерные
науки

Профиль

Искусственный интеллект в
кибербезопасности

Год начала обучения

2026

Форма обучения

очная

Реализуется в 3 семестре

РАЗРАБОТАНО:

Доцент кафедры вычислительной
математики и кибернетики

Ставрополь, 2026 г.

1. 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.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Атаки на системы искусственного интеллекта» относится к части, формируемой участниками образовательных отношений дисциплинам (модулям) по выбору. Ее освоение происходит в 3 семестре.

3. Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

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.
	ИД-2 использует современные методы разработки алгоритмов математических моделей	умеет использовать современные методы разработки и реализации конкретных алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования
	ИД-3 использует современные языки программирования для реализации конкретных	владеет навыками как использовать современные методы разработки и реализации конкретных

	алгоритмов и математических моделей.	алгоритмов математических моделей на базе языков программирования и пакетов прикладных программ моделирования
--	--------------------------------------	---

4. Объем учебной дисциплины (модуля) и формы контроля *

Объем занятий: всего: 5 з.е. 180 акад.ч.	ОФО, в акад. часах
Контактная работа:	
Лекции/из них практическая подготовка	18
Лабораторных работ/из них практическая подготовка	0
Практических занятий/из них практическая подготовка	18
Самостоятельная работа	108
Формы контроля	
Экзамен	
Зачет 3 семестр	-
Зачет с оценкой	-
Курсовая работа	есть

* Дисциплина (модуль) предусматривает применение электронного обучения, дистанционных образовательных технологий

5. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов занятий

№	Раздел (тема) дисциплины и краткое содержание	Формируемые компетенции, индикаторы	очная форма				Формы текущего контроля успеваемости
			Контактная работа обучающихся с преподавателем /из них в форме практической подготовки, часов			Самоотельная работа, часов	
			Лекции	Практические занятия	Лабораторные работы		
1	Постановка проблемы доверия искусственному интеллекту. Обсуждение индивидуальных заданий Введение в атаки на системы ИИ: основные концепции и типы атак	ИД-1ПК-9 ИД-2ПК-9 ИД-3ПК-9	2,0	2,0		12,0	Собеседование
2	Управление рисками искусственного интеллекта Уязвимости моделей машинного обучения и их эксплуатация	ИД-1ПК-9 ИД-2ПК-9 ИД-3ПК-9	2,0	2,0		12,0	Собеседование
3	Реализация объяснимого искусственного интеллекта и метрики объяснимости. Атаки на системы распознавания изображений и видео	ИД-1ПК-9 ИД-2ПК-9 ИД-3ПК-9	2,0	2,0		12,0	Собеседование
4	Оценка робастности модели искусственного интеллекта Защита от атак на системы обработки естественного языка	ИД-1ПК-9 ИД-2ПК-9 ИД-3ПК-9	2,0	2,0		12,0	Собеседование

5	Реализация функциональной безопасности искусственного интеллекта Атаки на системы ИИ в критической инфраструктуре	ИД-1 _{ПК-9} ИД-2 _{ПК-9} ИД-3 _{ПК-9}	2,0	2,0		12,0	Собеседование
6	Противодействие компьютерным атакам на искусственный интеллект. Состязательные атаки на нейронные сети	ИД-1 _{ПК-9} ИД-2 _{ПК-9} ИД-3 _{ПК-9}	2,0	2,0		12,0	Собеседование
7	Защита данных, используемых в системе искусственного интеллекта на этапах хранения, обучения и использования. Этика и правовые аспекты атак на системы ИИ	ИД-1 _{ПК-9} ИД-2 _{ПК-9} ИД-3 _{ПК-9}	2,0	2,0		12,0	Собеседование
8	Обнаружение аномалий Методы защиты и реагирования на атаки на системы ИИ	ИД-1 _{ПК-9} ИД-2 _{ПК-9} ИД-3 _{ПК-9}	4,0	4,0		24,0	Собеседование
	ИТОГО за 3 семестр		18.0	18.0	-	108.0	

6. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств (ФОС) по дисциплине (модулю) базируется на перечне осваиваемых компетенций с указанием индикаторов. ФОС обеспечивает объективный контроль достижения запланированных результатов обучения. ФОС включает в себя:

- описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;
- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций (включаются в методические указания по тем видам работ, которые предусмотрены учебным планом и предусматривают оценку сформированности компетенций);
- типовые оценочные средства, необходимые для оценки знаний, умений и уровня сформированности компетенций.

ФОС является приложением к данной программе дисциплины (модуля).

7. Методические указания для обучающихся по освоению дисциплины

Приступая к работе, каждый студент должен принимать во внимание следующие положения.

Дисциплина построена по тематическому принципу, каждая тема представляет собой логически заверченный раздел.

Лекционный материал посвящен рассмотрению ключевых, базовых положений курсов и разъяснению учебных заданий, выносимых на самостоятельную работу студентов.

Практические занятия проводятся с целью закрепления усвоенной информации, приобретения навыков ее применения при решении практических задач в соответствующей предметной области.

Самостоятельная работа студентов направлена на самостоятельное изучение дополнительного материала, подготовку к практическим занятиям, а также выполнения всех видов самостоятельной работы.

Для успешного освоения дисциплины, необходимо выполнить все виды самостоятельной работы, используя рекомендуемые источники информации.

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Перечень основной и дополнительной литературы, необходимый для освоения дисциплины

8.1.1. Перечень основной литературы:

1. Виятно Р. Р. и др. Состязательные примеры в современном машинном обучении: обзор //Препринт arXiv arXiv: 1911.05268. – 2019.
2. Юань Х. и др. Состязательные примеры: атаки и средства защиты для глубокого обучения //IEEE transactions on neural networks and learning systems. – 2019. – Т. 30. – №. 9. – С. 2805-2824.
3. Сюэ М. и др. Безопасность машинного обучения: угрозы, контрмеры и оценки //IEEE Access. – 2020. – Т. 8. – С. 74720-74742

8.1.2. Перечень дополнительной литературы:

1. Афанасьева Д. В. Применение искусственного интеллекта в обеспечении безопасности данных //Известия Тульского государственного университета. Технические науки. – 2020. – №. 2. – С. 151-154.
2. Негодин В. А. Машинное обучение в языке программирования Python //Форум молодых ученых. – 2019. – №. 8 (36). – С. 201-203.

8.2. 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, 2026.
2. Методические указания к практическим занятиям по дисциплине «Атаки на системы искусственного интеллекта». Ставрополь : СКФУ, 2026.

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

www.biblioclub.ru - Электронная библиотечная система «Университетская библиотека онлайн»

www.eLibrary.ru - Научная электронная библиотека

www.iprbookshop.ru - Электронно-библиотечная система IPRbooks

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

При чтении лекций используется компьютерная техника, демонстрации презентационных мультимедийных материалов. На практических занятиях студенты защищают отчеты по работам, которые они выполняют самостоятельно или в команде с применением компьютерной техники и Интернет-технологий

Информационные справочные системы:

Информационно-справочные и информационно-правовые системы, используемые при изучении дисциплины:

1	https://www.garant.ru/
2	http://www.consultant.ru/

Программное обеспечение:

1.	Альт Рабочая станция 10
2.	Альт Рабочая станция К
3.	Альт «Сервер»
4.	Пакет офисных программ - Р7-Офис

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия	Учебная аудитория для проведения учебных занятий, оснащенная мультимедийным оборудованием и техническими средствами обучения.
Практические занятия	Учебная аудитория для проведения учебных занятий, оснащенная мультимедийным оборудованием и техническими средствами обучения.
Самостоятельная работа	Помещение для самостоятельной работы обучающихся оснащенное компьютерной техникой с возможностью подключения к сети "Интернет" и возможностью доступа к электронной информационно-образовательной среде университета

11. Особенности освоения дисциплины (модуля) лицами с ограниченными возможностями здоровья

Обучающимся с ограниченными возможностями здоровья предоставляются специальные учебники, учебные пособия и дидактические материалы, специальные

технические средства обучения коллективного и индивидуального пользования, услуги ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, а также услуги сурдопереводчиков и тифлосурдопереводчиков.

Освоение дисциплины (модуля) обучающимися с ограниченными возможностями здоровья может быть организовано совместно с другими обучающимися, а также в отдельных группах.

Освоение дисциплины (модуля) обучающимися с ограниченными возможностями здоровья осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья.

В целях доступности получения высшего образования по образовательной программе лицами с ограниченными возможностями здоровья при освоении дисциплины (модуля) обеспечивается:

1) для лиц с ограниченными возможностями здоровья по зрению:

- присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочесть и оформить задание, в том числе, записывая под диктовку),

- письменные задания, а также инструкции о порядке их выполнения оформляются увеличенным шрифтом,

- специальные учебники, учебные пособия и дидактические материалы (имеющие крупный шрифт или аудиофайлы),

- индивидуальное равномерное освещение не менее 300 люкс,

- при необходимости студенту для выполнения задания предоставляется увеличивающее устройство;

2) для лиц с ограниченными возможностями здоровья по слуху:

- присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочесть и оформить задание, в том числе, записывая под диктовку),

- обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающемуся предоставляется звукоусиливающая аппаратура индивидуального пользования;

- обеспечивается надлежащими звуковыми средствами воспроизведения информации;

3) для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата (в том числе с тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):

- письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;

- по желанию студента задания могут выполняться в устной форме.

12. Особенности реализации дисциплины с применением дистанционных образовательных технологий и электронного обучения

Согласно части 1 статьи 16 Федерального закона от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации» под *электронным обучением* понимается организация образовательной деятельности с применением содержащейся в базах данных и используемой при реализации образовательных программ информации и обеспечивающих ее обработку информационных технологий, технических средств, а также информационно-телекоммуникационных сетей, обеспечивающих передачу по линиям связи указанной информации, взаимодействие обучающихся и педагогических работников. Под *дистанционными образовательными технологиями* понимаются образовательные технологии, реализуемые в основном с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии обучающихся и педагогических работников.

Реализация дисциплины может быть осуществлена с применением дистанционных образовательных технологий и электронного обучения полностью или частично. Компоненты УМК дисциплины (рабочая программа дисциплины, оценочные и методические материалы, формы аттестации), реализуемой с применением дистанционных образовательных технологий и электронного обучения, содержат указание на их использование.

При организации образовательной деятельности с применением дистанционных образовательных технологий и электронного обучения могут предусматриваться асинхронный и синхронный способы осуществления взаимодействия участников образовательных отношений посредством информационно-телекоммуникационной сети «Интернет».

При применении дистанционных образовательных технологий и электронного обучения в расписании по дисциплине указываются: способы осуществления взаимодействия участников образовательных отношений посредством информационно-телекоммуникационной сети «Интернет» (ВКС-видеоконференцсвязь, ЭТ – электронное тестирование); ссылки на электронную информационно-образовательную среду СКФУ, на образовательные платформы и ресурсы иных организаций, к которым предоставляется открытый доступ через информационно-телекоммуникационную сеть «Интернет»; для синхронного обучения - время проведения онлайн-занятий и преподаватели; для асинхронного обучения - авторы онлайн-курсов.

При организации промежуточной аттестации с применением дистанционных образовательных технологий и электронного обучения используются Методические рекомендации по применению технических средств, обеспечивающих объективность результатов при проведении промежуточной и государственной итоговой аттестации по образовательным программам высшего образования - программам бакалавриата, программам специалитета и программам магистратуры с применением дистанционных образовательных технологий (Письмо Минобрнауки России от 07.12.2020 г. № МН-19/1573-АН "О направлении методических рекомендаций").

Реализация дисциплины с применением электронного обучения и дистанционных образовательных технологий осуществляется с использованием электронной информационно-образовательной среды СКФУ, к которой обеспечен доступ обучающихся через информационно-телекоммуникационную сеть «Интернет», или с использованием ресурсов иных организаций, в том числе платформ, предоставляющих сервисы для проведения видеоконференций, онлайн-встреч и дистанционного обучения (МТС-Линк), а также с использованием возможностей социальных сетей для осуществления коммуникации обучающихся и преподавателей.

Учебно-методическое обеспечение дисциплины, реализуемой с применением электронного обучения и дистанционных образовательных технологий, включает представленные в электронном виде рабочую программу, учебно-методические пособия или курс лекций, методические указания к выполнению различных видов учебной деятельности обучающихся, предусмотренных дисциплиной, и прочие учебно-методические материалы, размещенные в информационно-образовательной среде СКФУ.