

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Грובה Татьяна Антоновна

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

Модели машинного обучения, сохраняющие конфиденциальность

Направление подготовки	02.04.01 Математика и компьютерные науки
Направленность (профиль)	Искусственный интеллект в кибербезопасности
Год начала обучения	2026
Форма обучения	очная
Реализуется в семестрах	4

Разработано

ассистент кафедры вычислительной
математики и кибернетики
Ширяев Е.М.

Ставрополь 2026 г.

1. Цель и задачи освоения дисциплины

Целью освоения дисциплины является формирование набора общепрофессиональных и профессиональных компетенций будущего магистра по направлению подготовки 02.04.01 Математика и компьютерные науки, профиль Искусственный интеллект в кибербезопасности.

Задачи освоения дисциплины – получение практических навыков работы с нормативно правовыми документами в области моделями машинного обучения, сохраняющие конфиденциальность; получения практических навыков разработки моделей машинного обучения, сохраняющие конфиденциальность; научиться оценивать корректность принятия решений моделей машинного обучения, сохраняющие конфиденциальность.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Модели машинного обучения, сохраняющие конфиденциальность» относится к дисциплинам факультативной части. Ее освоение происходит в 4 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-3 Способен проводить методические и экспертные работы в области математики и информатики	ИД-1ПК-3 проводит экспертные работы по математике	Проведение анализа и обсуждения экспертных оценок в области математики
	ИД-2ПК-3 проводит экспертные работы в области информатике.	Разработка и обсуждение экспертных оценок в сфере информатики
	ИД-3ПК-3 готовит методические материалы в области математики и информатики.	Создание и представление методических материалов для обучения

4. Объем учебной дисциплины и формы контроля *

Объем занятий: всего: 4 з.е. 144 академ.ч.	ОФО, в академ. часах
Контактная работа:	60.00
Лекции/из них практическая подготовка	20.00/0
Лабораторных работ/из них практическая подготовка	0
Практических занятий/из них практическая подготовка	40.00/0
Самостоятельная работа	84.00
Формы контроля	
Зачет в 4 семестре	

* Дисциплина предусматривает применение электронного обучения, дистанционных образовательных технологий (если иное не установлено образовательным стандартом)

5. Содержание дисциплины, структурированное по темам (разделам) с указанием количества 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			Самостоятельная работа, часов	
			Лекции	Практические занятия	Лабораторные работы		
1 семестр							
1.	Методы машинного обучения 1. Линейная регрессия 2. Логистическая регрессия	ИД-1 _{ПК-3} ИД-2 _{ПК-3}	2.00	5.00			Защита практической работы Собеседование
2.	Применение методов машинного обучения 1. Нейронные сети 2. Сверточные нейронные сети 3. Наборы данных для обучения нейронных сетей.	ИД-1 _{ПК-3} ИД-2 _{ПК-3}	4.00	5.00			Защита практической работы Собеседование
3.	Введение в использование TenSEAL 1. Полностью гомоморфное шифрование 2. Схема CKKS 3. Гомоморфные операции над зашифрованными значениями.	ИД-1 _{ПК-3} ИД-2 _{ПК-3}	2.00	5.00			Защита практической работы Собеседование
4.	Исследование линейной регрессии, сохраняющей конфиденциальность 1. Модель зашифрованной линейной регрессии. 2. Приближенные функции активации	ИД-1 _{ПК-3} ИД-2 _{ПК-3}	4.00	5.00			Защита практической работы Собеседование

5.	Работа с приближенными числами в гомоморфном шифровании. 1. Параметры схемы CKKS 2. Влияние параметров на точность вычислений 3. Управление погрешностью.	ИД-1 _{ПК-3} ИД-2 _{ПК-3}	4.00	10.0 0			Защита практической работы Собеседование
6.	Разработка сверточной нейронной сети, сохраняющей конфиденциальность, на базе набора данных MNIST 1. Обучение нейронных сетей 2. Приближенная модель нейронной сети 3. Модель зашифрованной нейронной сети. 4. Оценка точности распознавания изображений зашифрованной нейронной сети	ИД-1 _{ПК-3} ИД-2 _{ПК-3}	4.00	10.0 0			Защита практической работы Собеседование
	ИТОГО за 4 семестр		20.00	40.0 0			60.00
	ИТОГО		20.00	40.0 0			60.00

6. Фонд оценочных средств по дисциплине

Фонд оценочных средств (ФОС) по дисциплине «Модели машинного обучения, сохраняющие конфиденциальность» базируется на перечне осваиваемых компетенций с указанием этапов их формирования в процессе освоения дисциплины. 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;
- типовые контрольные задания и иные материалы, необходимые для оценки знаний, умений и уровня овладения формируемыми компетенциями в процессе освоения дисциплины.

ФОС является приложением к данной программе дисциплины.

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 и разъяснению учебных заданий, выносимых на самостоятельную работу студентов.

Практические работы направлены на приобретение опыта практической работы в соответствующей предметной области.

Самостоятельная работа студентов направлена на самостоятельное изучение дополнительного материала, подготовку к лабораторным 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, необходимой для освоения дисциплины

8.1.1. Перечень основной литературы:

1. Бабенко Л. К. и др. Полностью гомоморфное шифрование (обзор) //Вопросы защиты информации. – 2015. – №. 3. – С. 3-26.
2. Бабенко Л. К. и др. Защищенные вычисления и гомоморфное шифрование //Программные системы: теория и приложения.–2014.–25 с. – 2014.

8.1.2. Перечень дополнительной литературы:

1. Бабенко Л. К. и др. Методы полностью гомоморфного шифрования на основе матричных полиномов //Вопросы кибербезопасности. – 2015. – №. 1 (9). – С. 14-25.

8.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Wiryen Y. B. et al. A Comparative Study of BFV and CKKs Schemes to Secure IoT Data Using TenSeal and Pyfhel Homomorphic Encryption Libraries //International Journal of Smart Security Technologies (IJSST). – 2024. – Т. 10. – №. 1. – С. 1-17.

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

1. <http://informatics.mccme.ru/> (дистанционная подготовка по информатике)
2. www.ibxt.ru (новости вычислительной техники)
3. <https://ru.wikipedia.org/wiki> Википедия свободная энциклопедия.
4. <http://www.intuit.ru> Национальный открытый университет ИНТУИТ

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, BigBlueButton, Replit. На лабораторных занятиях студенты представляют коды программ и оформленные отчеты, подготовленные ими в часы самостоятельной работы с использованием соответствующего ПО.

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

1. <http://www.iprbookshop.ru> - ЭБС IPRbooks
2. <http://biblio-online.ru/> - ЭБС «Biblio-online.ru» издательства «Юрайт» ONLINE»
3. <http://www.intuit.ru> - Интернет-университет технологий

Программное обеспечение:

1	LibreOffice
2	Ubuntu 20.4 / Astra Linux 1.8
3	Python 3.11
4	Pytorch
5	TenSEAL

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 с возможностью подключения к сети "Интернет" и возможностью доступа к электронной информационно-образовательной среде университета ПЭВМ с микропроцессором не ниже Pentium 5 объем ПЗУ не менее 2-3 гб, объем ОЗУ не менее 512 мб со средой VisualStudio
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 ПЭВМ с микропроцессором не ниже Pentium 5 объем ПЗУ не менее 2-3 гб, объем ОЗУ не менее 512 мб со средой VisualStudio

11. Особенности освоения дисциплины 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 обучающимися с ограниченными возможностями здоровья может быть организовано совместно с другими обучающимися, а также в отдельных группах.

Освоение дисциплины 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 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-видео конференцсвязь, 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.