Министерство науки и высшего образования РФ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Дагестанский государственный технический университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина Технологии машинного обучения в кибербезопасности
наименование дисциплины по ОПОП

для направления подготовки 10.04.01 Информационная безопасность
код и полное наименование специальности

для направления подготовки 10.04.01 Информационная безопасность
код и полное наименование направления

по направленности Кибербразведка и противодействие угрозам с применением технологий искусственного интеллекта

факультет Компьютерных технологий и энергетики
наименование факультета, где ведется дисциплина

кафедра Информационная безопасность и программная инженерия
наименование кафедры, за которой закреплена дисциплина

Форма обучения очная курс 1 семестр (ы) 2
очная

г. Махачкала – 2026

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность с учетом рекомендаций и ОПОП ВО по направлению подготовки и программе магистратуры «Кибербразведка и противодействие угрозам с применением технологий искусственного интеллекта»

Разработчик _____ Качаева Г.И., к.э.н.
(подпись) (ФИО уч. степень, уч. звание)

« 02 » февраля 2026 г.

Зав. кафедрой, за которой закреплена дисциплина

_____ Качаева Г.И., к.э.н.
(подпись) (ФИО уч. степень, уч. звание)

« 03 » февраля 2026 г.

Программа одобрена на заседании выпускающей кафедры информационной безопасности и программной инженерии от « 05 » февраля 2026 года, протокол № 6/1

Зав. выпускающей кафедрой по данному направлению подготовки

_____ Качаева Г.И. к.э.н.
(подпись) (ФИО уч. степень, уч. звание)

« 05 » февраля 2026 г.

Программа одобрена на заседании Методического совета факультета компьютерных технологий и энергетики от « 10 » февраля 2026 г., протокол № 5/1

Председатель Методического совета факультета КТиЭ

_____ Исабекова Т.И.. к.ф.-м.н., доцент
(подпись) (ФИО уч. степень, уч. звание)

« 10 » февраля 2026 г.

Декан факультета _____ Т.А. Рагимова
(подпись) (ФИО)

Начальник УО _____ Л.Н. Мусаева
(подпись) (ФИО)

Проректор по УР _____ А.Ф. Демирова
(подпись) (ФИО)

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

1.1. Место дисциплины в структуре ОПОП

Дисциплина «Технологии машинного обучения в кибербезопасности» входит в обязательную часть учебного плана по программе магистратуры 10.04.01 Информационная безопасность, направленность «Кибербразведка и противодействие угрозам с применением технологий искусственного интеллекта».

Предшествующими дисциплинами, формирующими начальные знания, являются: Защищенные информационные системы, Технологии обеспечения информационной безопасности, Коммуникативные технологии в профессиональной сфере на иностранном языке, Интеллектуальные системы и технологии, Технологии извлечения знаний из больших данных.

Последующими дисциплинами являются: Принятие решений на основе проактивного поиска и обнаружения угроз, Интеллектуальные системы информационной безопасности в промышленных системах, Анализ защищенности систем искусственного интеллекта.

1.2. Цели и задачи освоения дисциплины

Дисциплина «Технологии машинного обучения в кибербезопасности» способствует формированию у обучающихся компетенций, предусмотренных данной рабочей программой в соответствии с требованиями ФГОС ВО и ОПОП ВО по направлению подготовки 10.04.01 Информационная безопасность с учетом специфики направленности подготовки – «Кибербразведка и противодействие угрозам с применением технологий искусственного интеллекта».

1.3. Компетенции обучающегося, формируемые в результате освоения дисциплины

В результате освоения дисциплины «Технологии машинного обучения в кибербезопасности» обучающийся должен овладеть следующими компетенциями:

Таблица 1.

Код и наименование компетенции	Код и наименование индикаторов достижения компетенции
ОПК-2. Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности.	ОПК-2.2 Выбирает и обосновывает преимущества методов решения задач для защиты информации компьютерных систем и сетей, а также систем обеспечения информационной безопасностью

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. Объем дисциплины и виды учебной работы

Таблица 2.

Вид учебной работы	**Форма обучения**
	очная
Объем образовательной программы дисциплины (ЗЕТ/ в часах)	4/144
В том числе:	**Объем в часах**
Лекции	34
Практические занятия	-
Лабораторные занятия	51
Самостоятельная работа	23
Курсовой проект (работа), семестр	-
Промежуточная аттестация в форме экзамена**,** семестр	2 семестр
Часы на экзамен	36

2.2. Содержание дисциплины

Раздел дисциплины, тема лекции и вопросы	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Коды компетенций, формированию которых способствует элемент программы
Тема 1. Основные понятия машинного обучения	Формальная постановка задачи машинного обучения. Примеры применения машинного обучения. Проблема переобучения. Методология решения задач машинного обучения.	**2**	ОПК-2
	в том числе лабораторных занятий:	**3**	
	Лабораторная работа № 1. Практические методы предобработки данных на ЯП Python.		
	Самостоятельная работа обучающихся: Решающие деревья	**1**	
Тема 2. Библиотека анализа данных Pandas. Numpy, DataFrame	Нейронные сети. Дерево решений. Метод случайного леса. Кластеризация данных. Поиск ассоциативных правил.	**2**	ОПК-2
	в том числе лабораторных занятий:	**3**	
	Лабораторная работа № 2. Предобработка данных в Pandas		
	Самостоятельная работа обучающихся: Решающие деревья	**1**	
Тема 3. Метрические методы	Метод ближайших соседей. Метод окна Парзена. Метрические методы классификации в задаче восстановления регрессии. Обнаружение выбросов	**2**	ОПК-2
	в том числе лабораторных занятий:	**3**	
	Лабораторная работа № 3. Выбор числа соседей		
	Самостоятельная работа обучающихся: Линейные методы для классификации. Логистическая регрессия.	**1**	
Тема 4. Типы данных, классификация задач	Типы данных. Классификация задач машинного обучения	**2**	ОПК-2
	в том числе лабораторных занятий:	**3**	

машинного обучения	Лабораторная работа № 4. Обнаружение выбросов		
	Самостоятельная работа обучающихся: Линейные методы для классификации. Логистическая регрессия.	**1**	
Тема 5. Линейные методы классификации	Метод стохастического градиента. Постановка задачи. Градиентные методы численной минимизации и алгоритм SG. Алгоритм SAG. Метод стохастического градиента. Достоинства и недостатки. Проблема переобучения	**2**	ОПК-2
	в том числе лабораторных занятий:	**3**	
	Лабораторная работа № 5. Реализация в Scikit-Learn		
	Самостоятельная работа обучающихся: Линейные методы для классификации. Логистическая регрессия.	**1**	
Тема 6. Библиотека Scikit-Learn.	Создание моделей машинного обучения. Настройка гиперпараметров	**2**	ОПК-2
	в том числе лабораторных занятий:	**3**	
	Лабораторная работа № 5. Реализация в Scikit-Learn		
	Самостоятельная работа обучающихся: Аппроксимация эмпирического риска	**1**	
Тема 7. Метод опорных векторов. Логистическая регрессия	Метод опорных векторов. Метод опорных векторов. Обобщение для нелинейного случая. Логистическая регрессия. Пример применения логистической регрессии. Регуляризованная логистическая регрессия.	**2**	ОПК-2
	в том числе лабораторных занятий:	**3**	
	Лабораторная работа № 6. Реализация метода SVM, логистическая регрессия		
	Самостоятельная работа обучающихся: Аппроксимация эмпирического риска	**1**	
Тема 8. Введение в нейронные сети.	Введение в нейронные сети.	**2**	ОПК-2
	в том числе лабораторных занятий:	**3**	
	Лабораторная работа № 7. Логистическая регрессия		
	Самостоятельная работа обучающихся: Бэггинг и метод случайных подпространств	**1**	

Тема 9. Метрики качества классификации. Линейная регрессия.	Метрики качества классификации. Многоклассовая классификация. Решение задачи многомерной линейной регрессии с помощью сингулярного разложения. Гребневая регрессия	**2**	ОПК-2
	в том числе лабораторных занятий:	**3**	
	Лабораторная работа № 8. Метрика качества		
	Самостоятельная работа обучающихся: Бэггинг и метод случайных подпространств	**1**	
Тема 10. Свёрточные нейронные сети	Принцип работы свёрточных нейронных сетей	**2**	ОПК-2
	в том числе лабораторных занятий:	**3**	
	Лабораторная работа № 9. Гребневая регрессия		
	Самостоятельная работа обучающихся: Бэггинг и метод случайных подпространств	**2**	
Тема 11. Композиции алгоритмов.	Бэггинг и случайный лес. Градиентный бустинг. Градиентный бустинг: модификации и эвристики	**2**	ОПК-2
	в том числе лабораторных занятий:	**3**	
	Лабораторная работа № 10. Метод главных компонент.		
	Самостоятельная работа обучающихся: Нейронная реализация логических функций	**2**	
Тема 12. Обработка текстов	Обработка текстов на основе свёрточных НС Обработка текстов на основе рекуррентных НС	**2**	ОПК-2
	в том числе лабораторных занятий:	**3**	
	Лабораторная работа № 10. Метод главных компонент.		
	Самостоятельная работа обучающихся: Нейронная реализация логических функций	**2**	
Тема 13. Кластеризация и визуализация	Кластеризация. Иерархическая кластеризация. Нелинейные методы понижения размерности	**2**	ОПК-2
	в том числе лабораторных занятий:	**3**	
	Лабораторная работа № 11. Градиентный бустинг		

	Самостоятельная работа обучающихся: Нейронная реализация логических функций	**2**	
Тема 14. Прогнозирование временных рядов	Нейронные сети для прогнозирования рядов	**2**	ОПК-2
	в том числе лабораторных занятий:	**4**	
	Лабораторная работа № 12. Кластеризация.		
	Самостоятельная работа обучающихся: Метод k-средних	**2**	
Тема 15. Машинное обучение в прикладных задачах	Этапы анализа данных. Работа с числовыми признаками. Предобработка данных. Оценивание качества. Обзор алгоритмов	**2**	ОПК-2
	в том числе лабораторных занятий:	**4**	
	Лабораторная работа № 13. Нелинейные методы понижения размерности.		
	Самостоятельная работа обучающихся: Предобработка данных	**2**	
Тема 16. Задачи машинного обучения по обработке изображений	Свёрточные НС для обработки	**4**	ОПК-2
	в том числе лабораторных занятий:	**4**	
	Лабораторная работа № 14. Анализ данных и оценка качества		
	Самостоятельная работа обучающихся: Понимание задачи машинного обучения	**2**	
Итого за 2 семестр:			
Лекции		**34**	
Лабораторные работы		**51**	
Самостоятельная работа		**23**	
Промежуточная аттестация в форме экзамена		**36**	
Всего:		**144**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Материально-техническое обеспечение дисциплины «Технологии машинного обучения в кибербезопасности» включает:

Наименование помещения	Перечень основного оборудования
Лаборатория защиты информации	Рабочее место преподавателя; Посадочные места по количеству обучающихся; Автоматизированные рабочие места (ПК в сборе) с доступом в сеть Интернет; Интерактивная система в составе: проектор интерактивная доска Программное обеспечение: Служебный носитель «Секрет Особого Назначения» криптографический с быстрым процессором, 32Гб (арт. 620520); CIC-IDS2017, NSL-KDD, Malware-Bazaar; Jupyter Notebook, Pandas, NumPy, MLflow; Docker, Kubernetes, FastAPI;
Аудитория для проведения занятий лекционного типа	Рабочее место преподавателя; Посадочные места по количеству обучающихся; Автоматизированные рабочие места (ПК в сборе) с доступом в сеть Интернет; Интерактивная система в составе: проектор, интерактивная доска
Аудитория для самостоятельной работы обучающихся	Автоматизированные рабочие места (ПК в сборе) с доступом в сеть Интернет; Интерактивная система в составе: проектор, интерактивная доска

3.2. Учебно-методическое и информационное обеспечение программы

Для реализации программы библиотечный фонд образовательной организации имеет печатные и/или электронные образовательные и информационные ресурсы для использования в образовательном процессе. При формировании библиотечного фонда образовательной организации выбирается не менее одного издания из перечисленных ниже печатных изданий и (или) электронных изданий в качестве основного, при этом список может быть дополнен новыми изданиями

3.2.1. Печатные издания

Основная литература:

1. Ростовцев В. С. Искусственные нейронные сети [Электронный ресурс]: учебник. - Санкт - Петербург: Лань, 2019. - 216 с. – URL: https://e.lanbook.com/book/122180.
2. Хливненко Л. В., Пятакович Ф. А. Практика нейросетевого моделирования [Электронный ресурс]:учебное пособие. - Санкт-Петербург: Лань, 2019. - 200 с. URL: https://e.lanbook.com/book/123697
3. Джонс М. Т. Программирование искусственного интеллекта в приложениях / Пер. с англ. Осипов А. И. / М.Т. Джонс. - Москва : ДМК Пресс, 2018. - 312 с. - ISBN 978-5-97060-579-0. - URL: https://ibooks.ru/bookshelf/385089/reading.

Дополнительные источники:

1. Остроух А. В., Суркова Н. Е. Системы искусственного интеллекта [Электронный ресурс]: монография. - Санкт-Петербург: Лань, 2019. - 228 с. URL: https://e.lanbook.com/book/113401
2. Болотова Л.С. Системы искусственного интеллекта: модели и технологии, основанные на знаниях: учебник / Л.С. Болотова. - Москва: Финансы и статистика, 2023. - 664 с. - ISBN 978-5-00184-097-8. - URL: https://ibooks.ru/bookshelf/389216

3.2.2. Основные электронные издания

1. Портал «Информационная безопасность»: новости, публикации, инновации – Архив изданий по информационной безопасности https://www.itsec.ru/articles2/allpubliks
2. Уязвимости, обзоры, аналитика и многое другое – Портал информационной безопасности — Securitylab.ru
3. Отслеживание тенденций, аналитика, информирование о наиболее значимых событиях - BugTraq.Ru
4. Backtrack Linux LiveCD и образ для виртуальной машины Сайт проекта Linux для анализа компьютерной безопасности
5. Блоги и статьи специалистов по ИБ InformIT
6. Электронная библиотека. - Режим доступа: http://elibrary.ru
7. Электронная библиотечная система «КнигаФонд» − http://www.knigafund.ru/
8. Электронная библиотечная система издательства «Лань» − http://e.lanbook.com/

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий.

Результаты обучения	**Критерии оценки**	**Методы оценки**
- Выбирает и обосновывает преимущества методов решения задач для защиты информации компьютерных систем и сетей, а также систем обеспечения информационной безопасностью	*Шкала оценивания для экзамена* *«Отлично»* Показывает высокий уровень сформированности компетенций, т.е.: - демонстрирует высокое и прочное освоение материала; - исчерпывающе, четко, последовательно, грамотно и логически стройно излагает теоретический материал; - правильно формирует определения; - демонстрирует умения самостоятельной работы с нормативно-правовой литературой; - умеет делать выводы по излагаемому материалу. *«Хорошо»* Показывает достаточный уровень сформированности компетенций, т.е.: - демонстрирует достаточно полное знание материала, основных теоретических положений; - достаточно последовательно, грамотно и логически стройно излагает теоретический материал; - демонстрирует умения ориентироваться в нормативно-правовой литературе; - умеет делать достаточно обоснованные выводы по излагаемому материалу. *«Удовлетворительно»* Показывает пороговый уровень сформированности компетенций, т.е.: - демонстрирует общее знание изучаемого материала; - испытывает затруднения при ответах на дополнительные вопросы; - знает основную рекомендуемую литературу; - умеет строить ответ в соответствии со структурой излагаемого материала. *Неудовлетворительно»* Ставится в случае: - незнания значительной части программного материала; - невладения понятийным аппаратом дисциплины; - допущения существенных ошибок при изложении учебного материала; - неумения строить ответ в соответствии со структурой излагаемого вопроса; - неумения делать выводы по излагаемому материалу.	Текущий контроль при проведении: - письменного/устного опроса; - тестирования; - оценки результатов самостоятельной работы (докладов, рефератов). Промежуточная аттестация в форме: -экзамена, - письменных/ устных ответов, - тестирования.

Специальные условия инвалидам и лицам с ограниченными возможностями здоровья (ОВЗ)

Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

Специальные условия обучения и направления работы с инвалидами и лицами с ОВЗ определены на основании:

- Федерального закона от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации»;

- Федерального закона от 24.11.1995 № 181-ФЗ «О социальной защите инвалидов в Российской Федерации»;

- приказа Минобрнауки России от 06.04.2021 № 245 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры»;

- методических рекомендаций по организации образовательного процесса для обучения инвалидов и лиц с ограниченными возможностями здоровья в образовательных организациях высшего образования, в том числе оснащенности образовательного процесса, утвержденных Минобрнауки России 08.04.2014 № АК-44/05вн).

Под специальными условиями для получения образования обучающихся с ОВЗ понимаются условия обучения, воспитания и развития, включающие в себя использование при необходимости адаптированных образовательных программ и методов обучения и воспитания, специальных учебников, учебных пособий и дидактических материалов, специальных технических средств обучения коллективного и индивидуального пользования, предоставление услуг ассистента (помощника), оказывающего необходимую помощь, проведение групповых и индивидуальных коррекционных занятий, обеспечение доступа в здания ДГТУ и другие условия, без которых невозможно или затруднено освоение ОПОП обучающихся с ОВЗ.

Обучение в рамках учебной дисциплины обучающихся с ОВЗ осуществляется ДГТУ с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

Обучение по учебной дисциплине обучающихся с ОВЗ может быть организовано как совместно с другими обучающимися, так и в отдельных группах.

В целях доступности обучения по дисциплине обеспечивается:

1) для лиц с ограниченными возможностями здоровья по зрению:

- наличие альтернативной версии официального сайта ДГТУ в сети «Интернет» для слабовидящих;

- весь необходимый для изучения материал, согласно учебному плану (в том числе, для обучающихся по индивидуальным учебным планам) предоставляется в электронном виде на диске.

- индивидуальное равномерное освещение не менее 300 люкс;

- присутствие ассистента, оказывающего обучающемуся необходимую помощь;

- обеспечение возможности выпуска альтернативных форматов печатных материалов (крупный шрифт или аудиофайлы);

- обеспечение доступа обучающегося, являющегося слепым и использующего собаку-проводника, к зданию ДГТУ.

2) для лиц с ОВЗ по слуху:

- наличие микрофонов и звукоусиливающей аппаратуры коллективного пользования (аудиоколонки);

3) для лиц с ОВЗ, имеющих нарушения опорно-двигательного аппарата, материально-технические условия должны обеспечивать возможность беспрепятственного доступа обучающихся в учебные помещения, столовые, туалетные и другие помещения организации, а также пребывания в указанных помещениях (наличие пандусов, поручней, расширенных дверных проемов и других приспособлений).

Перед началом обучения могут проводиться консультативные занятия, позволяющие студентам с ОВЗ адаптироваться к учебному процессу.

В процессе ведения учебной дисциплины научно-педагогическим работникам рекомендуется использование социально-активных и рефлексивных методов обучения, технологий социокультурной реабилитации с целью оказания помощи обучающимся с ОВЗ в установлении полноценных межличностных отношений с другими обучающимися, создании комфортного психологического климата в учебной группе.

Особенности проведения текущей и промежуточной аттестации по дисциплине для обучающихся с ОВЗ устанавливаются с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и др.). При необходимости предоставляется дополнительное время для подготовки ответа на зачете или экзамене