МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
"Казанский (Приволжский) федеральный университет"
Институт вычислительной математики и информационных технологий

подписано электронно-цифровой подписью

Программа дисциплины

Машинное обучение

Направление подготовки: 10.03.01 - Информационная безопасность
Профиль подготовки: Безопасность компьютерных систем
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2024

Содержание

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП ВО

2. Место дисциплины (модуля) в структуре ОПОП ВО

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

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

4.1. Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)

4.2. Содержание дисциплины (модуля)

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

6. Фонд оценочных средств по дисциплине (модулю)

7. Перечень литературы, необходимой для освоения дисциплины (модуля)

8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

9. Методические указания для обучающихся по освоению дисциплины (модуля)

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

12. Средства адаптации преподавания дисциплины (модуля) к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья

13. Приложение №1. Фонд оценочных средств

14. Приложение №2. Перечень литературы, необходимой для освоения дисциплины (модуля)

15. Приложение №3. Перечень информационных технологий, используемых для освоения дисциплины (модуля), включая перечень программного обеспечения и информационных справочных систем

Программу дисциплины разработал(а)(и): старший преподаватель, б/с Денисов М.П. (кафедра системного анализа и информационных технологий, отделение фундаментальной информатики и информационных технологий), MPDenisov@kpfu.ru

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП ВО

Обучающийся, освоивший дисциплину (модуль), должен обладать следующими компетенциями:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОПК-11	Способен проводить эксперименты по заданной методике и обработку их результатов
ОПК-3	Способен использовать необходимые математические методы для решения задач профессиональной деятельности
ПК-4	Проведение анализа безопасности компьютерных систем и разработка требований по защите информации в компьютерных системах и сетях

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

- основы машинного обучения.
- возможности алгоритмов машинного обучения.

Должен уметь:

- применять на практике знания основ машинного обучения.
- применять на практике алгоритмы машинного обучения.
- обосновать применение того или иного алгоритма машинного обучения для решения конкретной задачи

Должен владеть:

- знаниями основ машинного обучения.
- базовым инструментарием машинного обучения.
- знаниями о задачах защиты информации, решаемых с помощью алгоритмов машинного обучения.

Должен демонстрировать способность и готовность:

- применять полученные знания и навыки в своей дальнейшей профессиональной деятельности.

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.В.08 Дисциплины (модули)" основной профессиональной образовательной программы 10.03.01 "Информационная безопасность (Безопасность компьютерных систем)" и относится к части ОПОП ВО, формируемой участниками образовательных отношений.

Осваивается на 3 курсе в 6 семестре.

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 4 зачетных(ые) единиц(ы) на 144 часа(ов).

Контактная работа - 72 часа(ов), в том числе лекции - 36 часа(ов), практические занятия - 0 часа(ов), лабораторные работы - 36 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 36 часа(ов).

Контроль (зачёт / экзамен) - 36 часа(ов).

Форма промежуточного контроля дисциплины: экзамен в 6 семестре.

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

4.1 Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)						Самостоятельная работа
			Лекции, всего	Лекции в эл. форме	Практические занятия, всего	Практические в эл. форме	Лабораторные работы, всего	Лабораторные в эл. форме	
1.	Тема 1. Введение в машинное обучение	6	2	0	0	0	4	0	4
2.	Тема 2. Линейные модели регрессии	6	4	0	0	0	4	0	5
3.	Тема 3. Логистическая регрессия	6	4	0	0	0	4	0	5
4.	Тема 4. Нейронные сети	6	6	0	0	0	8	0	4
5.	Тема 5. Деревья решений	6	6	0	0	0	4	0	6
6.	Тема 6. Алгоритм AdaBoost	6	8	0	0	0	8	0	6
7.	Тема 7. Кластеризация	6	6	0	0	0	4	0	6
	Итого		36	0	0	0	36	0	36

4.2 Содержание дисциплины (модуля)

Тема 1. Введение в машинное обучение

Что такое машинное обучение. Преимущество машинного обучения при решении задач. Обзор задач, решаемых алгоритмами машинного обучения. Примеры применения машинного обучения в анализе текста, компьютерном зрении, анализе видео и аудио. Классификация алгоритмов машинного обучения: машинное обучение с учителем, без учителя, обучение с подкреплением и т.д.

Тема 2. Линейные модели регрессии

Линейная регрессия. Линейные модели регрессии. Вывод целевой функции линейной регрессии с помощью метода максимального правдоподобия. Базисные функции. Матрица плана. Вычисление параметров модели, вывод формулы вычисления параметров. Регуляризация линейной регрессии, вывод формулы вычисления параметров при использовании регуляризации.

Тема 3. Логистическая регрессия

Задачи классификации. Способы измерения точности в задаче классификации. Базовый алгоритм классификации: логистическая регрессия. Целевая функция логистической регрессии, вывод целевой функции с помощью метода максимального правдоподобия. Регуляризация логистической регрессии. Метод градиентного спуска для вычисления параметров логистической регрессии.

Тема 4. Нейронные сети

Структура нейрона: входы, выход, веса, смещение, активация, функция активации. Виды функций активации: линейная функция активации, сигмоид, ReLU, Leaky ReLU. Структура нейронной сети. Многослойный перспептрон. Обучение нейронной сети с помощью метода градиентного спуска. Вычисление вектора градиента с помощью алгоритма обратного распространения ошибки.

Тема 5. Деревья решений

Дерево решений как алгоритм классификации. Структура деревьев решений: внутренние и терминальные узлы. Виды разделяющих функций: разделение гиперплоскостями, параллельными осям координат, линейное разделение, нелинейное разделение. Обучения дерева решений. Целевая функция внутреннего узла, критерии создания внутреннего узла. Регуляризация деревев решений. Алгоритм Random Forest.

Тема 6. Алгоритм AdaBoost

Объединение слабых классификаторов в ансамбль с учетом особенностей слабых классификаторов с помощью алгоритма AdaBoost. Описание алгоритма AdaBoost. Целевая функция для обучения слабых классификаторов, формула обновления весов, целевая функция AdaBoost. Математическое обоснование алгоритма. Каскад классификаторов.

Тема 7. Кластеризация

Методы машинного обучения без учителя. Обзор существующих алгоритмов кластеризации. Алгоритм k-means. Целевая функция алгоритма k-means. Методы инициализации центроидов, обновление центроидов. Вывод метода обновления центроидов из целевой функции. Критерий остановки алгоритма. Преимущества и недостатки алгоритма k-means.

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Самостоятельная работа обучающихся выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Самостоятельная работа подразделяется на самостоятельную работу на аудиторных занятиях и на внеаудиторную самостоятельную работу. Самостоятельная работа обучающихся включает как полностью самостоятельное освоение отдельных тем (разделов) дисциплины, так и проработку тем (разделов), осваиваемых во время аудиторной работы. Во время самостоятельной работы обучающиеся читают и конспектируют учебную, научную и справочную литературу, выполняют задания, направленные на закрепление знаний и отработку умений и навыков, готовятся к текущему и промежуточному контролю по дисциплине.

Организация самостоятельной работы обучающихся регламентируется нормативными документами, учебно-методической литературой и электронными образовательными ресурсами, включая:

Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры (утвержден приказом Министерства науки и высшего образования Российской Федерации от 6 апреля 2021 года №245)

Письмо Министерства образования Российской Федерации №14-55-996ин/15 от 27 ноября 2002 г. "Об активизации самостоятельной работы студентов высших учебных заведений"

Устав федерального государственного автономного образовательного учреждения "Казанский (Приволжский) федеральный университет"

Правила внутреннего распорядка федерального государственного автономного образовательного учреждения высшего профессионального образования "Казанский (Приволжский) федеральный университет"

Локальные нормативные акты Казанского (Приволжского) федерального университета

6. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств по дисциплине (модулю) включает оценочные материалы, направленные на проверку освоения компетенций, в том числе знаний, умений и навыков. Фонд оценочных средств включает оценочные средства текущего контроля и оценочные средства промежуточной аттестации.

В фонде оценочных средств содержится следующая информация:

- соответствие компетенций планируемым результатам обучения по дисциплине (модулю);

- критерии оценивания сформированности компетенций;

- механизм формирования оценки по дисциплине (модулю);

- описание порядка применения и процедуры оценивания для каждого оценочного средства;

- критерии оценивания для каждого оценочного средства;

- содержание оценочных средств, включая требования, предъявляемые к действиям обучающихся, демонстрируемым результатам, задания различных типов.

Фонд оценочных средств по дисциплине находится в Приложении 1 к программе дисциплины (модулю).

7. Перечень литературы, необходимой для освоения дисциплины (модуля)

Освоение дисциплины (модуля) предполагает изучение основной и дополнительной учебной литературы. Литература может быть доступна обучающимся в одном из двух вариантов (либо в обоих из них):

- в электронном виде - через электронные библиотечные системы на основании заключенных КФУ договоров с правообладателями;

- в печатном виде - в Научной библиотеке им. Н.И. Лобачевского. Обучающиеся получают учебную литературу на абонементе по читательским билетам в соответствии с правилами пользования Научной библиотекой.

Электронные издания доступны дистанционно из любой точки при введении обучающимся своего логина и пароля от личного кабинета в системе "Электронный университет". При использовании печатных изданий библиотечный фонд должен быть укомплектован ими из расчета не менее 0,5 экземпляра (для обучающихся по ФГОС 3++ - не менее 0,25 экземпляра) каждого из изданий основной литературы и не менее 0,25 экземпляра дополнительной литературы на каждого обучающегося из числа лиц, одновременно осваивающих данную дисциплину.

Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля), находится в Приложении 2 к рабочей программе дисциплины. Он подлежит обновлению при изменении условий договоров КФУ с правообладателями электронных изданий и при изменении комплектования фондов Научной библиотеки КФУ.

8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Научный портал по математическим наукам - http://www.mathnet.ru

Портал образовательных ресурсов по ИТ - http://www.intuit.ru

Портал статей по применению ИТ и машинному обучению - http://habrahabr.ru/hub/machine_learning/

Профессиональный интернет-ресурс по машинному обучению - http://www.machinelearning.ru/

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Вид работ	Методические рекомендации
лекции	Студенту рекомендуется внимательно слушать лектора, следить за тем, что написано на доске или представлено на слайдах презентации, анализировать получаемую им информацию. В случае, если материал лекции непонятен, следует задать вопрос в отведенное для вопросов время. Студенту также рекомендуется конспектировать материал лекции в тетради, что улучшает запоминание.
лабораторные работы	При выполнении лабораторных работ студенту рекомендуется внимательно анализировать поставленную задачу, уделяя особенное внимание критериям оценки точности решения задачи. Программный код должен быть объектно-ориентированным, чистым, с поясняющими комментариями. Особенное внимание следует уделить методологическим аспектам решения задачи, на корректное разделение выборки на обучающую, валидационную и тестовую. Результаты работы программы должны быть оформлены в виде таблиц и графиков.
самостоя-тельная работа	При ведении самостоятельной работы студенту рекомендуется внимательно подходить к изучению научных статей, обращать внимание на значимость полученного результата, на требования к обучающей выборке, на скорость работы предлагаемых алгоритмов, на результаты их сравнения с существующими. В случае, если изучаемый материал понятен не до конца, рекомендуется обращение к дополнительной литературе.
экзамен	На экзамене обучающийся должен продемонстрировать глубокое понимание изученного материала, как с точки зрения теории, так и с точки зрения практического применения алгоритмов машинного обучения. Необходимо четко формулировать ответ и быть готовым его пояснить. Использование дополнительных источников информации на экзамене запрещено.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем, представлен в Приложении 3 к рабочей программе дисциплины (модуля).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Материально-техническое обеспечение образовательного процесса по дисциплине (модулю) включает в себя следующие компоненты:

Помещения для самостоятельной работы обучающихся, укомплектованные специализированной мебелью (столы и стулья) и оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду КФУ.

Учебные аудитории для контактной работы с преподавателем, укомплектованные специализированной мебелью (столы и стулья).

Компьютер и принтер для распечатки раздаточных материалов.

Мультимедийная аудитория.

Компьютерный класс.

12. Средства адаптации преподавания дисциплины к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья

При необходимости в образовательном процессе применяются следующие методы и технологии, облегчающие восприятие информации обучающимися инвалидами и лицами с ограниченными возможностями здоровья:

- создание текстовой версии любого нетекстового контента для его возможного преобразования в альтернативные формы, удобные для различных пользователей;

- создание контента, который можно представить в различных видах без потери данных или структуры, предусмотреть возможность масштабирования текста и изображений без потери качества, предусмотреть доступность управления контентом с клавиатуры;

- создание возможностей для обучающихся воспринимать одну и ту же информацию из разных источников - например, так, чтобы лица с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально;

- применение программных средств, обеспечивающих возможность освоения навыков и умений, формируемых дисциплиной, за счёт альтернативных способов, в том числе виртуальных лабораторий и симуляционных технологий;

- применение дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем, в том числе вебинаров, которые могут быть использованы для проведения виртуальных лекций с возможностью взаимодействия всех участников дистанционного обучения, проведения семинаров, выступления с докладами и защиты выполненных работ, проведения тренингов, организации коллективной работы;

- применение дистанционных образовательных технологий для организации форм текущего и промежуточного контроля;

- увеличение продолжительности сдачи обучающимся инвалидом или лицом с ограниченными возможностями здоровья форм промежуточной аттестации по отношению к установленной продолжительности их сдачи:

- продолжительности сдачи зачёта или экзамена, проводимого в письменной форме, - не более чем на 90 минут;

- продолжительности подготовки обучающегося к ответу на зачёте или экзамене, проводимом в устной форме, - не более чем на 20 минут;

- продолжительности выступления обучающегося при защите курсовой работы - не более чем на 15 минут.

Программа составлена в соответствии с требованиями ФГОС ВО и учебным планом по направлению 10.03.01 "Информационная безопасность" и профилю подготовки "Безопасность компьютерных систем".

Приложение 2
к рабочей программе дисциплины (модуля)
Б1.В.08 Машинное обучение

Перечень литературы, необходимой для освоения дисциплины (модуля)

Направление подготовки: 10.03.01 - Информационная безопасность
Профиль подготовки: Безопасность компьютерных систем
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2024

Основная литература:

1. Ростовцев, В. С. Искусственные нейронные сети: учебник / В. С. Ростовцев. - 4-е изд., стер. - Санкт-Петербург : Лань, 2024. - 216 с. - ISBN 978-5-507-47362-5. - Текст : электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/364517 (дата обращения: 20.01.2024). - Режим доступа: для авториз. пользователей.

2. Ясницкий, Л. Н. Интеллектуальные системы : учебник / Л. Н. Ясницкий. - 2-е изд. - Москва : Лаборатория знаний, 2020. - 224 с. - ISBN 978-5-00101-897-1. - Текст : электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/151510 (дата обращения: 20.01.2024). - Режим доступа: для авториз. пользователей.

3. Жданов, А. А. Автономный искусственный интеллект : учебное пособие / А. А. Жданов. - 5-е изд. (эл.). - Москва : Лаборатория знаний, 2024. - 362 с. - ISBN 978-5-93208-674-2. - Текст : электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/387629 (дата обращения: 20.01.2024). - Режим доступа: для авториз. пользователей.

4. Флах, П. Машинное обучение. Наука и искусство построения алгоритмов, которые извлекают знания из данных / П. Флах; пер. с англ. А. А. Слинкина. - 2-е изд. - Москва : ДМК Пресс, 2023. - 401 с. - Систем. требования: Adobe Reader XI либо Adobe Digital Editions 4.5 ; экран 10'. - ISBN 978-5-89818-300-4. - Текст : электронный // ЭБС 'Консультант студента' : [сайт]. - URL : https://www.studentlibrary.ru/book/ISBN9785898183004.html (дата обращения: 20.01.2024). - Режим доступа : по подписке.

5. Вьюгин, В. В. Математические основы машинного обучения и прогнозирования : учебное пособие / В. В. Вьюгин. - Москва : МЦНМО, 2014. - 304 с. - ISBN 978-5-4439-2014-6. - Текст : электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/56397 (дата обращения: 20.01.2024). - Режим доступа: для авториз. пользователей.

Дополнительная литература:

1. Сириченко, А. В. Искусственные нейронные сети. Практикум : учебное пособие / А. В. Сириченко. - Москва : Московский институт стали и сплавов, 2022. - 26 с. - Текст : электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/305447 (дата обращения: 20.01.2024). - Режим доступа: для авториз. пользователей.

2. Данилов, В. В. Нейронные сети : учебное пособие / В. В. Данилов. - Донецк : Донецкий национальный университет, 2020. - 158 с. - Текст : электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/179953 (дата обращения: 20.01.2024). - Режим доступа: для авториз. пользователей.

3. Смолин, Д. В. Введение в искусственный интеллект: конспект лекций : учебное пособие / Д. В. Смолин. - 2-е изд., перераб. - Москва : ФИЗМАТЛИТ, 2007. - 264 с. - ISBN 978-5-9221-0862-1. - Текст : электронный // Лань : электронно-библиотечная система. - URL: https://e.lanbook.com/book/2325 (дата обращения: 20.01.2024). - Режим доступа: для авториз. пользователей.

4. Осипов, Г. С. Методы искусственного интеллекта : монография / Г. С. Осипов. - Москва : Физматлит, 2011. - 296 с. - ISBN 978-5-9221-1323-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/544787 (дата обращения: 20.01.2024). - Режим доступа : по подписке.

Приложение 3
к рабочей программе дисциплины (модуля)
Б1.В.08 Машинное обучение

Перечень информационных технологий, используемых для освоения дисциплины (модуля), включая перечень программного обеспечения и информационных справочных систем

Направление подготовки: 10.03.01 - Информационная безопасность

Профиль подготовки: Безопасность компьютерных систем

Квалификация выпускника: бакалавр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2024

Освоение дисциплины (модуля) предполагает использование следующего программного обеспечения и информационно-справочных систем:

Операционная система Microsoft Windows 7 Профессиональная или Windows XP (Volume License)

Пакет офисного программного обеспечения Microsoft Office 365 или Microsoft Office Professional plus 2010

Браузер Mozilla Firefox

Браузер Google Chrome

Adobe Reader XI или Adobe Acrobat Reader DC

Kaspersky Endpoint Security для Windows

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен обучающимся. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, учебно-методические комплексы, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего образования (ФГОС ВО) нового поколения.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе Издательства "Лань" , доступ к которой предоставлен обучающимся. ЭБС Издательства "Лань" включает в себя электронные версии книг издательства "Лань" и других ведущих издательств учебной литературы, а также электронные версии периодических изданий по естественным, техническим и гуманитарным наукам. ЭБС Издательства "Лань" обеспечивает доступ к научной, учебной литературе и научным периодическим изданиям по максимальному количеству профильных направлений с соблюдением всех авторских и смежных прав.

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "Консультант студента", доступ к которой предоставлен обучающимся. Многопрофильный образовательный ресурс "Консультант студента" является электронной библиотечной системой (ЭБС), предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Полностью соответствует требованиям федеральных государственных образовательных стандартов высшего образования к комплектованию библиотек, в том числе электронных, в части формирования фондов основной и дополнительной литературы.