

**Федеральное государственное автономное образовательное
учреждение высшего образования
«Московский физико-технический институт
(национальный исследовательский университет)»**

УТВЕРЖДЕНО

**Директор физтех-школы
прикладной математики и
информатики**

А.М. Райгородский

	Рабочая программа дисциплины (модуля)
по дисциплине:	Машинное обучение
по направлению:	Прикладная математика и информатика
профиль подготовки:	А1360: Передовые методы искусственного интеллекта Физтех-школа Прикладной Математики и Информатики кафедра машинного обучения и цифровой гуманитаристики
курс:	2
квалификация:	бакалавр

Семестры, формы промежуточной аттестации:

3 (осенний) - Дифференцированный зачет

4 (весенний) - Дифференцированный зачет

Аудиторных часов: 120 всего, в том числе:

лекции: 60 час.

семинары: 60 час.

лабораторные занятия: 0 час.

Самостоятельная работа: 60 час.

Всего часов: 180, всего зач. ед.: 4

Программу составил: Р.Г. Нейчев, старший преподаватель

Программа обсуждена на заседании кафедры машинного обучения и цифровой гуманитаристики 12.02.2024

Аннотация

Курс знакомит студентов с современным состоянием машинного обучения и искусственного интеллекта: от классических алгоритмов до глубокого обучения и последних достижений в области искусственного интеллекта. В результате студенты формируют устойчивую теоретическую базу и практические навыки для дальнейшего развития в области ИИ.

1. Цели и задачи

Цель дисциплины

- сформировать теоретические и практические знания в области обучения машин, современных методов восстановления зависимостей по эмпирическим данным, включая дискриминантный, кластерный и регрессионный анализ.

Задачи дисциплины

- правильно формулировать задачу в терминах машинного обучения;
- овладеть навыками практического решения задач интеллектуального анализа данных.

2. Перечень формируемых компетенций

Освоение дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	Индикаторы достижения компетенции
ОПК-2 Способен использовать современные информационные технологии и программные средства при решении задач профессиональной деятельности, соблюдая требования информационной безопасности	ОПК-2.1 Способен применять современные вычислительную технику и сервисы сети Интернет в области (сфере) профессиональной деятельности
ML-2 Способен применять фундаментальные принципы и методы машинного обучения включая подготовку данных оценку качества моделей и работу с признаками	ML-2.1 Различает основные типы задач машинного обучения и применяет на практике принципы их решения
	ML-2.2 Применяет методы предварительной обработки данных и работы с признаками
	ML-2.3 Решает проблемы несбалансированных данных и оценивает качество моделей
ML-3 Способен применять классические алгоритмы машинного обучения с пониманием их математических основ и областей применения	ML-3.1 Обосновывает способы и варианты применения классических методов и моделей машинного обучения в задачах ИИ, включая их математическое (алгоритмическое) преобразование и адаптацию к специфике задачи
	ML-3.2 Эффективно применяет классические методы и модели машинного обучения для обеспечения достижимости функциональных характеристик систем ИИ
ML-6 Способен применять алгоритмы обучения с подкреплением	ML-6.1 Обосновывает способы и варианты применения алгоритмов обучения с подкреплением в задачах ИИ, включая их преобразование и адаптацию к специфике задачи
	ML-6.2 Применяет методы повышения устойчивости, надежности, безопасности алгоритмов обучения с подкреплением для проверки разведочных гипотез и подготовки данных к применению современных методов ИИ
	ML-6.3 Оценивает результативность применения методов повышения устойчивости, надежности, безопасности алгоритмов обучения с подкреплением в задачах ИИ на основе сопоставления с аналогами

3. Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны

знать:

- основные принципы и проблематику теории обучения машин;
- основные современные методы обучения по прецедентам — классификации, кластеризации и регрессии.

уметь:

- формализовать постановки прикладных задач анализа данных;
- использовать методы обучения по прецедентам для решения практических задач;
- оценивать точность и эффективность полученных решений.

владеть:

- основными понятиями теории машинного обучения.

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

4.1. Разделы дисциплины (модуля) и трудоемкости по видам учебных занятий

№	Тема (раздел) дисциплины	Трудоемкость по видам учебных занятий, включая самостоятельную работу, час.			
		Лекции	Семинары	Лаборат. работы	Самост. работа
1	Введение в машинное обучение. Метрические алгоритмы, оценка качества моделей	10	10		10
2	Линейные модели	10	10		10
3	Деревья и ансамбли моделей	10	10		10
4	Работа с признаками. Ограничения машинного обучения	10	10		10
5	Введение в глубокое обучение	10	10		10
6	Обучение без учителя	10	10		10
Итого часов		60	60		60
Подготовка к экзамену		0 час.			
Общая трудоёмкость		180 час., 4 зач.ед.			

4.2. Содержание дисциплины (модуля), структурированное по темам (разделам)

Семестр: 3 (Осенний)

1. Введение в машинное обучение. Метрические алгоритмы, оценка качества моделей

Основные понятия в машинном обучении. Обзор приложений машинного обучения. Обучение с учителем и без учителя. Задачи: классификация, регрессия, кластеризация, снижение размерности.

Метрические алгоритмы. Метод ближайших соседей (kNN) в задаче классификации и регрессии. Кластеризация и алгоритм k средних (k means).

Байесовский подход. Понятие правдоподобия. Наивный байесовский классификатор.

Отложенная выборка. Кросс-валидация. Переобучение и недообучение. Гиперпараметры.

2. Линейные модели

Линейная регрессия. Метод наименьших квадратов. Градиентный спуск и стохастический градиентный спуск. Переобучение моделей. Регуляризация Тихонова. Теорема Гаусса-Маркова. Функции потерь в задаче регрессии.

Линейная классификация. Понятие отступа. Функции потерь в задаче классификации. Логистическая регрессия. Метод наибольшего правдоподобия. Логистическая функция потерь. Функции Softmax, Sigmoid. Многоклассовая классификация. Регуляризация линейных классификаторов.

Методы оценки качества классификации. Accuracy, Precision, Recall, ROC-AUC, PR-curve, Confusion matrix.

Метод опорных векторов (SVM). Теорема Каруша-Куна-Такера. Двойственная задача. Понятие опорных векторов. Kernel trick (подмена ядра). Регуляризация в SVM.

Метод главных компонент (PCA). Теорема Эккарта-Янга. SVD-разложение. Зависимость объясненной дисперсии от числа компонент.

3. Деревья и ансамбли моделей

Смещение и разброс. Bias-Variance decomposition. Неустойчивость моделей машинного обучения.

Решающее дерево. Рекурсивная процедура построения решающего дерева. Критерии информативности в задаче классификации: энтропийный, Джини; в задаче регрессии. Переобучение решающих деревьев. Прунинг. Регуляризация решающих деревьев. Алгоритмы построения: ID3, C4.5, C5, CART. Небинарные решающие деревья. Связь решающих деревьев и линейных моделей.

Бутстрап. Бэггинг. Out-of-bag error. Метод случайных подпространств (RSM). Случайный лес (Random Forest). Развитие идеи: Extremely Randomized Trees. Сравнение Random Forest и метрических алгоритмов (kNN). Isolation Forest.

Стекинг и блендинг моделей машинного обучения.

Бустинг. Историческая справка, алгоритм AdaBoost. Градиентный бустинг (GBM).

Семестр: 4 (Весенний)

4. Работа с признаками. Ограничения машинного обучения

Проклятие размерности. No Free Lunch Theorem, Wolpert (Теорема о бесплатных обедах). Принцип “Garbage in – garbage out”.

Типы признаков: континуальные, бинарные, категориальные. Работа с разреженными признаками. Работа с пропусками.

Работа с текстовыми данными. Мешок слов (bag of words), TF-IDF.

Оценка значимости признаков. Permutation importance, Partial-dependence plots, shap. Recursive Feature Elimination. LARS.

5. Введение в глубокое обучение

Исторический экскурс. Искусственные нейронные сети. Математическая модель нейрона Маккалока-Питтса. Персептрон Розенблатта. Проблема исключающего или (XOR problem).

Основные понятия в глубоком обучении (Deep Learning). Метод обратного распространения ошибки (backpropagation). Функции активации: Sigmoid, Tanh, ReLU, Leaky ReLU, ELU, Softmax. Полносвязный слой.

Градиентная оптимизация в глубоком обучении. Методы, основанные на градиентном спуске: Momentum, Nesterov Momentum, Adagrad, Adadelata, RMSprop, Adam, AdamW. Learning rate decay. Начальная инициализация параметров нейронной сети.

Регуляризация в нейронных сетях. Batch normalization. Instance and layer normalization. Dropout. Weight decay. Аугментация данных.

Рекуррентные нейронные сети. RNN. Проблема затухающего градиента (Vanishing gradient). Механизм памяти в LSTM и GRU. Рекуррентные нейронные сети в анализе текстов и последовательностей.

Сверточные нейронные сети. Операция свертки. Сверточный слой (convolutional layer). Нормализация данных. Pooling layer. Пропуск градиента с помощью skip connections. Исторический обзор архитектур и их основных свойств: LeNet, AlexNet, VGGNet, GoogLeNet, ResNet.

Классические подходы к векторизации текстов. Векторное представление слов с помощью нейронных сетей. Word2Vec, GloVe.

Снижение размерности с помощью нейронных сетей. Автоэнкодеры в различных задачах (снижение размерности, фильтрация шумов, поиск аномалий).

6. Обучение без учителя

Кластеризация. Метрический подход, алгоритм k-means. Иерархическая кластеризация. Алгоритм DBSCAN.

Методы снижения размерности. Многомерное шкалирование. Isomap. Locally Linear Embedding. SNE, t-SNE.

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

Учебная аудитория, оснащенная мультимедиапроектором и экраном и доступом в интернет.

6. Перечень рекомендуемой литературы

Основная литература

Машинное обучение [Текст]/Х. Бринк, Дж. Ричардс, М. Феверолф, Real-World Machine Learning, -СПб., Питер, 2017

Дополнительная литература

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

1. <https://ml-mipt.github.io> – сайт с описанием курса и ссылками на дополнительные ресурсы
2. <http://www.machinelearning.ru> – профессиональный информационно-аналитический ресурс, посвященный машинному обучению, распознаванию образов и интеллектуальному анализу данных.
3. <http://shad.yandex.ru> – сайт школы анализа данных Яндекса.

4.

[http://www.machinelearning.ru/wiki/index.php?title=Машинное_обучение_\(курс_лекций,_К.В.Воронцов\)](http://www.machinelearning.ru/wiki/index.php?title=Машинное_обучение_(курс_лекций,_К.В.Воронцов))

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

На лекционных занятиях используются мультимедийные технологии, включая демонстрацию презентаций.

В процессе самостоятельной работы обучающихся предполагается использование таких программных средств, как git, CLI (command-line interface), Jupyter Notebook и др.

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

Студент, изучающий дисциплину, должен с одной стороны, овладеть общим понятийным аппаратом, а с другой стороны, должен научиться применять теоретические знания на практике.

Успешное освоение дисциплины требует:

- посещения студентом всех видов аудиторных занятий;
- ведения конспекта в ходе лекционных занятий;
- качественной самостоятельной подготовки к практическим занятиям, активной работы на них;
- активной самостоятельной и аудиторной работы студента;
- своевременной сдачи преподавателю заданий по аудиторным видам работ.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

по направлению:	Прикладная математика и информатика
профиль подготовки:	АІ360: Передовые методы искусственного интеллекта Физтех-школа Прикладной Математики и Информатики кафедра машинного обучения и цифровой гуманитаристики
курс:	<u>2</u>
квалификация:	бакалавр

Семестры, формы промежуточной аттестации:

- 3 (осенний) - Дифференцированный зачет
- 4 (весенний) - Дифференцированный зачет

Разработчик: Р.Г. Нейчев, старший преподаватель

1. Компетенции, формируемые в процессе изучения дисциплины

Код и наименование компетенции	Индикаторы достижения компетенции
ОПК-2 Способен использовать современные информационные технологии и программные средства при решении задач профессиональной деятельности, соблюдая требования информационной безопасности	ОПК-2.1 Способен применять современные вычислительную технику и сервисы сети Интернет в области (сфере) профессиональной деятельности
ML-2 Способен применять фундаментальные принципы и методы машинного обучения включая подготовку данных оценку качества моделей и работу с признаками	ML-2.1 Различает основные типы задач машинного обучения и применяет на практике принципы их решения
	ML-2.2 Применяет методы предварительной обработки данных и работы с признаками
	ML-2.3 Решает проблемы несбалансированных данных и оценивает качество моделей
ML-3 Способен применять классические алгоритмы машинного обучения с пониманием их математических основ и областей применения	ML-3.1 Обосновывает способы и варианты применения классических методов и моделей машинного обучения в задачах ИИ, включая их математическое (алгоритмическое) преобразование и адаптацию к специфике задачи
	ML-3.2 Эффективно применяет классические методы и модели машинного обучения для обеспечения достижимости функциональных характеристик систем ИИ
ML-6 Способен применять алгоритмы обучения с подкреплением	ML-6.1 Обосновывает способы и варианты применения алгоритмов обучения с подкреплением в задачах ИИ, включая их преобразование и адаптацию к специфике задачи
	ML-6.2 Применяет методы повышения устойчивости, надежности, безопасности алгоритмов обучения с подкреплением для проверки разведочных гипотез и подготовки данных к применению современных методов ИИ
	ML-6.3 Оценивает результативность применения методов повышения устойчивости, надежности, безопасности алгоритмов обучения с подкреплением в задачах ИИ на основе сопоставления с аналогами

2. Показатели оценивания компетенций

В результате изучения дисциплины «Машинное обучение» обучающийся должен:

знать:

- основные принципы и проблематику теории обучения машин;
- основные современные методы обучения по прецедентам — классификации, кластеризации и регрессии.

уметь:

- формализовать постановки прикладных задач анализа данных;
- использовать методы обучения по прецедентам для решения практических задач;
- оценивать точность и эффективность полученных решений.

владеть:

- основными понятиями теории машинного обучения.

3. Перечень типовых (примерных) вопросов, заданий, тем для подготовки к текущему контролю

1. Постановка задач обучения с учителем (supervised learning).
2. Задачи обучения без учителя. Назвать хотя бы две.

3. Что означает свойство i.i.d.?
4. Основная идея наивного Байесовского классификатора. В чём его наивность?
5. Запишите формулы для модели линейной регрессии и для среднеквадратичной ошибки.
6. Запишите формулу для одного шага градиентного спуска. Как модифицировать градиентный спуск для очень большой выборки?
7. Что такое правдоподобие, метод максимального правдоподобия? Является ли правдоподобие вероятностью?
8. Что такое кросс-валидация? На что влияет количество блоков в кросс-валидации?
9. Что такое переобучение и недообучение? Как их можно детектировать?
10. Чем гиперпараметры отличаются от параметров? Что является параметрами и гиперпараметрами в линейных моделях и в решающих деревьях?
11. Что такое регуляризация? Чем на практике отличается L1-регуляризация от L2?
12. Учитывается ли коэффициент сдвига w_0 в регуляризаторе? Почему?
13. Почему линейные модели рекомендуется применять к выборке с нормированными значениями признаков?
14. Запишите формулу для линейной модели классификации. Что такое отступ?
15. Что такое точность и полнота? Почему нужно учитывать их вместе?
16. В задаче бинарной классификации доля одного класса составляют 95% выборки. Какие метрики разумно использовать для оценки работы модели? почему?
17. Что такое ROC-AUC? Как построить ROC-кривую?
18. Запишите функционал логистической регрессии. Как он связан с методом максимума правдоподобия?
19. Идея метода опорных векторов (в случае разделимой выборки).
20. Опишите жадный алгоритм обучения решающего дерева.
21. Почему с помощью решающего дерева можно достичь нулевой ошибки на обучающей выборке без повторяющихся объектов?
22. Если в лист дерева попали объекты разных классов, то какие предсказания нужно выдавать в этом листе? Почему?
23. Какое предсказание нужно выдавать в листе дерева в задаче регрессии если мы минимизируем MSE? а в случае MAE?
24. Что такое bagging?

4. Перечень типовых (примерных) вопросов и тем для проведения промежуточной аттестации обучающихся

3 семестр:

1. Задачи обучения по прецедентам. Supervised, unsupervised и semi-supervised обучение. Понятия переобучения и обобщающей способности. Скользящий контроль (cross-validation).
2. Метрические алгоритмы классификации. Обобщённый метрический классификатор, понятие отступа. Метод ближайших соседей (kNN) и его обобщения. Подбор числа k по критерию скользящего контроля. Отбор эталонных объектов. алгоритм СТОЛП. Функция конкурентного сходства (FRiS).
3. Построение метрик и отбор признаков. Стандартные метрики. Оценивание качества метрики. Проклятие размерности. Жадный алгоритм отбора признаков.
4. Логические закономерности. Статистический критерий информативности I с (φ, X, I) : смысл и способы вычисления. Энтропийный критерий информативности — информационный выигрыш $IGain$ с (φ, X, I) . Многоклассовые варианты критериев. Индекс Gini. Задача перебора конъюнкций. “Градиентный” алгоритм синтеза конъюнкций и его частные случаи: жадный алгоритм, стохастический локальный поиск, стабилизация, редукция.
5. Бинаризация признаков, алгоритм выделения информативных зон. Решающие списки. Решающие деревья: принцип работы. Разбиение пространства объектов на подмножества, выделяемые конъюнкциями терминальных вершин. Алгоритм ID3. Пре-прунинг и пост-прунинг. RandomForest.

6. Линейная классификация. Непрерывные аппроксимации пороговой функции потерь. Метод минимизации аппроксимированного эмпирического риска. SG, SAG. Связь минимизации аппроксимированного эмпирического риска и максимизации совместного правдоподобия данных и модели. Регуляризация (l1, l2, elasticnet). Вероятностный смысл регуляризаторов. Примеры различных функций потерь и классификаторов. Эвристический вывод логистической функции потерь.
7. Метод опорных векторов. Оптимизационная задача с ограничениями в виде неравенств и безусловная. Опорные векторы. Kerneltrick. Оптимизационная задача в S3VM и SVR. SVM и беспризнаковое машинное обучение на примере ядер графов и классификации вершин графа.
8. Задача снижения размерности пространства признаков. Идея метода главных компонент (PCA). Связь PCA и сингулярного разложения матрицы признаков (SVD). Вычисление SVD в пространствах высокой размерности методом стохастического градиента (SG SVD).
9. Многомерная линейная регрессия. Геометрический и аналитический вывод. Регуляризация в задаче регрессии. Непараметрическая регрессия. Формула Надарая-Ватсона. Регрессионные деревья.
10. Байесовская классификация и регрессия. Функционал риска и функционал среднего риска. Оптимальный байесовский классификатор и теорема о минимизации среднего риска. Наивный байесовский классификатор.

4 семестр:

1. Восстановление плотности: параметрический и непараметрический подход. Метод Парзенковского окна. Параметрический подход на примере нормального дискриминантного анализа. Линейный дискриминант Фишера.
2. Задача прогнозирования временного ряда, примеры задач. Адаптивные алгоритмы прогнозирования: экспоненциальное сглаживание, модели Брауна, Тейла-Вейджа, Хольта-Винтерса. Преимущества и недостатки адаптивных алгоритмов прогнозирования.
3. Модели ARMA, ARIMA, а также регрессионные методы решения задачи прогнозирования временного ряда. Композиции адаптивных алгоритмов: селекция, композиция, ЛАВР, агрегирующий алгоритм.
4. Задача кластеризации. Агломеративная и дивизионная кластеризация. Алгоритмы k-Means, k-Means++. Кластеризация с помощью EM-алгоритма (без вывода M-шага). Формула Ланса-Уилльямса.
5. Что такое случайный лес? Чем он отличается от бэггинга над решающими деревьями?
6. Как в градиентном бустинге обучаются базовые алгоритмы?
7. Зачем нужен backprop, что такое производная вектора по вектору?
8. Опишите принцип работы свёрточного слоя (CNN).
9. В чем недостатки полносвязных нейронных сетей какая мотивация к использованию свёрточных?
10. Опишите принцип работы базового рекуррентного слоя (RNN).
11. Что такое dropout?
12. Как dropout и batch normalization меняют свое поведение при эксплуатации модели (в режиме inference)?
13. Запишите постановку задачи в методе главных компонент.
14. Как работает метод k-means?

Критерии оценивания

Оценка "Отлично" (10) - полностью и вовремя решены все задачи без ошибок. Продemonстрирован грамотный подход к решению задач, реализованы оптимальные алгоритмы, код оформлен в едином удобочитаемом стиле.

Оценка "Отлично" (9) - полностью и вовремя решены все задачи без ошибок. Продemonстрирован грамотный подход к решению задач, реализованы оптимальные алгоритмы.

Оценка "Отлично" (8) - полностью и вовремя решены все задачи без ошибок. Продemonстрирован грамотный подход к решению задач.

Оценка "Хорошо" (7) - полностью решены все задачи. Допущены несущественные ошибки.

Оценка "Хорошо" (6) - полностью решено большинство задач. В некоторых задачах допущены и не исправлены ошибки, либо некоторые задачи решены частично.

Оценка "Хорошо" (5) - полностью решено две трети задач. В некоторых задачах допущены и не исправлены ошибки, либо некоторые задачи решены частично.

Оценка "Удовлетворительно" (4) - полностью решено более половины задач. В остальных задачах допущены и не исправлены ошибки, либо некоторые задачи решены частично.

Оценка "Удовлетворительно" (3) - полностью решено более половины задач.

Оценка "Неудовлетворительно" (2) - решено менее половины задач.

Оценка "Неудовлетворительно" (1) - не решено ни одной задачи.

5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Дифференцированный зачет может проводиться по итогам текущей успеваемости и сдачи заданий и других видов работ, предусмотренных программой дисциплины и (или) путем организации специального опроса, проводимого в устной и (или) письменной форме.

При проведении устного дифференцированного зачета обучающемуся предоставляется 30 минут на подготовку. Опрос обучающегося не должен превышать одного астрономического часа.

Во время проведения дифференцированного зачета обучающиеся могут пользоваться программой дисциплины, а также справочной литературой, конспектами лекций или другими материалами.