Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 08.09.2025 12:27:52
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Методы машинного обучения»

Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

Профиль
«Безопасность открытых информационных систем»

Квалификация
Специалист по защите информации

Формы обучения
Очная

Москва, 2025 г.

Разработчик(и):

степень, звание, должность / Е.А. Харченко /

Согласовано:
Заведующий кафедрой «Информационная безопасность»  И.В.Калуцкий

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине 4
2 Место дисциплины в структуре образовательной программы 4
3 Структура и содержание дисциплины 5
3.1 Виды учебной работы и трудоемкость 5
3.2 Тематический план изучения дисциплины 6
3.3 Содержание дисциплины 6
4 Учебно-методическое и информационное обеспечение 6
4.1 Основная литература 6
4.2 Дополнительная литература 7
5 Материально-техническое обеспечение 7
5.1 Требования к оборудованию и помещению для занятий 7
5.2 Требования к программному обеспечению 7
6 Методические рекомендации 7
6.1 Методические рекомендации для преподавателя по организации обучения 7
6.2 Методические указания для обучающихся по освоению дисциплины 7
7 Фонд оценочных средств 8
7.1 Методы контроля и оценивания результатов обучения 8
7.2 Шкала и критерии оценивания результатов обучения 8
7.3 Оценочные средства 11
7.3.1 Экзаменационные вопросы 11
7.3.2 Типовые практические задания 11
7.3.3 Типовой экзаменационный билет 13

1 Цели, задачи и планируемые результаты обучения по дисциплине

Цель изучения дисциплины – обучение студентов навыкам использования машинного обучения и анализа данных для последующей разработки стратегий продвижения продуктов и услуг в цифровом пространстве.

Обучение по дисциплине «Методы машинного обучения» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК-8. Способен разрабатывать алгоритмы и программы, пригодные для практического применения	ИОПК-8.1. Знает основные технологии создания и внедрения информационных систем, стандарты управления жизненным циклом информационной системы. ИОПК-8.2. Умеет проектировать блоксхемы алгоритмов, оценивать производительность алгоритмов и затраты памяти на работу алгоритма, разрабатывать программы на основе спроектированного алгоритма и проводить отладку программы, применять методы системного анализа и математического моделирования при разработке и эксплуатации ИС, проводить структурный анализ, функциональный анализ, объектно-ориентированный анализ иерархии классов. осуществлять организационное обеспечение выполнения работ на всех стадиях и в процессах жизненного цикла информационной системы. ИОПК-8.3. Владеет навыками разработки программ, построения блок-схем алгоритмов и оценки производительности алгоритмов, работы с унифицированным языком визуального моделирования, составления плановой и отчетной документации по управлению проектами создания информационных систем на стадиях жизненного цикла.

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса.

2 Место дисциплины в структуре образовательной программы

Дисциплина относится к базовой части основной профессиональной образовательной программы специалитета.

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ОПОП:

- Языки программирования.

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных единицы, т.е. 144 академических часа (из них 72 часов – самостоятельная работа студентов и 54 часа – лабораторные работы, лекции - 18 часов занятий).

Разделы дисциплины изучаются в девятом семестре обучения, т.е. на пятом курсе. Форма контроля – экзамен.

3.1 Виды учебной работы и трудоемкость (по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			Семестр	Неделя семестра
1	**Аудиторные занятия**	**72**	9	
	В том числе:			
1.1	Лекции	18	9	
1.2	Семинарские/практические занятия			
1.3	Лабораторные занятия	54	9	
2	**Самостоятельная работа**	**72**	9	
3	**Промежуточная аттестация**			
	Экзамен		9	
	Итого:	**144**		

3.2Тематический план изучения дисциплины (по формам обучения)

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	Тема 1. Введение	**32**	2	-	12	-	18
2	Тема 2. Введение в программирование	**38**	6	-	14	-	18

3	Тема 3. Практическое построение моделей	**38**	6	-	14	-	18
4	Тема 4. Нейронные сети: введение	**36**	4	-	14	-	18
Итого		**144**	**18**		**54**		**72**

3.3 Содержание дисциплины

1. Что такое большие данные и аналитика данных? Введение в теорию вероятности и её применение на практике. Введение в статистику и её применение на практике.
2. Введение в программирование на Python. Введение в машинное обучение. Практика работы с данными на основе задачи кластеризации.
3. Практическое построение моделей на основе логистической регрессии. Метрики качества в машинном обучении. Ансамбли моделей в машинном обучении.
4. Нейронные сети: введение. Нейронные сети: сверточные и рекуррентные сети. CRISP-DM и основы реализации проектов по аналитике данных.

3.4 Тематика курсовых проектов

Темы курсовых работ:

1. Обнаружение аномалий в сетевом трафике с использованием методов глубокого обучения
2. Классификация вредоносного ПО с помощью алгоритмов машинного обучения
3. Генеративно-состязательные сети (GAN) для создания и обнаружения фишинговых веб-страниц
4. Методы обработки естественного языка (NLP) для анализа текстовых угроз в социальных сетях
5. Обнаружение атак на основе данных журналов событий (SIEM) с применением ансамблевых методов
6. Адверсарные атаки на модели машинного обучения: методы защиты в системах информационной безопасности
7. Детектирование ботнетов на основе поведения устройств в IoT-сетях
8. Кластеризация данных для выявления скрытых угроз в корпоративных сетях
9. Машинное обучение в стеганографии: обнаружение скрытых сообщений в мультимедийных файлах
10. Использование машинного обучения для анализа уязвимостей в программном обеспечении

4 Учебно-методическое и информационное обеспечение

4.1Основная литература

1. Платонов, А. В. Машинное обучение : учебное пособие для вузов / А. В. Платонов. — Москва : Издательство Юрайт, 2023. — 85 с. — (Высшее образование). — ISBN 978-5-534-15561-7. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/520544
2. Воронов, М. В. Системы искусственного интеллекта : учебник и практикум для вузов / М. В. Воронов, В. И. Пименов, И. А. Небаев. — Москва : Издательство Юрайт, 2023. — 256 с. — (Высшее образование). — ISBN 978-5534-14916-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/519916
3. Иванов, В. М. Интеллектуальные системы : учебное пособие для вузов / В. М. Иванов ; под научной редакцией А. Н. Сесекина. — Москва : Издательство Юрайт, 2022. — 91 с. — (Высшее образование). — ISBN 978-5534-00551-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/492094
4. Загорулько, Ю. А. Искусственный интеллект. Инженерия знаний : учебное пособие для вузов / Ю. А. Загорулько, Г. Б. Загорулько. — Москва : Издательство Юрайт, 2022. — 93 с. — (Высшее образование). — ISBN 978-5534-07198-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/494205

4.2 Дополнительная литература

1. Бессмертный, И. А. Системы искусственного интеллекта : учебное пособие для вузов / И. А. Бессмертный. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023. — 157 с. — (Высшее образование). — ISBN 978-5-534-07467-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512657
2. Анализ данных : учебник для вузов / В. С. Мхитарян [и др.] ; под редакцией В. С. Мхитаряна. — Москва : Издательство Юрайт, 2023. — 490 с. — (Высшее образование). — ISBN 978-5-534-00616-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511020

4.3. Электронные образовательные ресурсы

Электронный образовательный ресурс в разработке

5 Материально-техническое обеспечение

5.1 Требования к оборудованию и помещению для занятий

Практические занятия (семинары) и самостоятельная работа студентов должна проводиться в специализированных аудиториях с комплектом мультимедийного оборудования и/или доской для записей материалов. Число рабочих мест в аудитории должно быть достаточным для обеспечения индивидуальной работы студентов.

5.2 Требования к программному обеспечению

Для проведения практических занятий (семинаров) специального программного обеспечения для освоения дисциплины не требуется.

6 Методические рекомендации

6.1 Методические рекомендации для преподавателя по организации обучения

1. При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.
2. При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

6.2 Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются аудиторные занятия, семинары и практики.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, дорабатывают конспекты и записи, готовятся к промежуточной аттестации, а также самостоятельно изучают отдельные темы учебной программы.

На занятиях студентов, в том числе предполагающих практическую деятельность, осуществляется закрепление полученных, в том числе и в процессе самостоятельной работы, знаний. Особое внимание обращается на развитие умений и навыков установления связи положений теории с профессиональной деятельностью будущего специалиста.

Самостоятельная работа осуществляется индивидуально. Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;
- контроль со стороны преподавателей (текущий и промежуточный).

Текущий контроль осуществляется на аудиторных занятиях, промежуточный контроль осуществляется на зачете в письменной (устной) форме.

Критериями оценки результатов самостоятельной работы студента являются:

- уровень освоения студентом учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- сформированность компетенций;
- оформление материала в соответствии с требованиями.

7 Фонд оценочных средств

7.1Методы контроля и оценивания результатов обучения

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

● экзамен.

7.2 Шкала и критерии оценивания результатов обучения

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине.

Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
ОПК-8. Способен разрабатывать алгоритмы и программы, пригодные для практического применения				
ИОПК-8.1. Знает основные технологии создания и внедрения информационных систем, стандарты управления жизненным	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие	Обучающийся демонстрирует неполное соответствие следующих знаний, указанных в индикаторах компетенций	Обучающийся демонстрирует частичное соответствие следующих знаний, указанных в индикаторах компетенций	Обучающийся демонстрирует полное соответствие следующих знаний, указанных в индикаторах компетенций

циклом информационной системы. ИОПК-8.2. Умеет проектировать блок-схемы алгоритмов, оценивать производительнос ть алгоритмов и затраты памяти на работу алгоритма, разрабатывать программы на основе спроектированног о алгоритма и проводить отладку программы, применять методы системного анализа и математического моделирования при разработке и эксплуатации ИС, проводить структурный анализ, функциональный анализ, объектноориентированный анализ иерархии классов. осуществлять организационное обеспечение выполнения работ на всех стадиях и в процессах жизненного цикла информационной системы. ИОПК-8.3. Владеет навыками разработки программ, построения блоксхем алгоритмов и оценки производительнос	материалу дисциплины знаний, указанных в индикаторах компетенций дисциплины «Знать» (см. п. 3).	дисциплины «Знать» (см. п. 3). Допускаются значительные ошибки, проявляется недостаточнос ть знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	дисциплины «Знать» (см. п. 3). Но допускаются незначительны е ошибки, неточности, затруднения при аналитических операциях.	дисциплины «Знать» (см. п. 3). Свободно оперирует приобретенным и знаниями.

ти алгоритмов, работы с унифицированным языком визуального моделирования, составления плановой и отчетной документации по управлению проектами создания информационных систем на стадиях жизненного цикла.				

Шкала оценивания результатов промежуточной аттестации и её описание:

Форма промежуточной аттестации: экзамен.

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

К промежуточной аттестации допускаются только студенты, выполнившие все виды учебной работы, предусмотренные рабочей программой по дисциплине.

Шкала оценивания	Описание
Отлично	Среднее значение для всех формируемых на момент проведения аттестации уровней компетенций – 5. Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Среднее значение для всех формируемых на момент проведения аттестации уровней компетенций – 4. Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.

Удовлетворительно	Среднее значение для всех формируемых на момент проведения аттестации уровней компетенций – 3. Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не достигнуто пороговое значение хотя бы для одного уровня формируемых на момент проведения аттестации компетенций. Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

7.3Оценочные средства

7.3.1 Экзаменационные вопросы

1. Обзор задач, решаемых алгоритмами машинного обучения.
2. Классификация алгоритмов машинного обучения.
3. Линейные модели регрессии.
4. Базисные функции.
5. Регуляризация.
6. Целевая функция логистической регрессии.
7. Регуляризация логистической регрессии.
8. Структура нейрона.
9. Структура нейронной сети.
10. Перцептрон.
11. Обучения нейронной сети с помощью алгоритма обратного распространения ошибки.
12. Структура деревьев решений.
13. Виды разделяющих функций.
14. Обучения дерева решений.
15. Алгоритм RandomForest.
16. Алгоритм AdaBoost.
17. Каскад классификаторов.
18. Кластеризация.
19. Обучение без учителя.
20. Алгоритм k-means.
21. Иерархическая кластеризация.
22. Метод опорных векторов.
23. Метод k-ближайших соседей.
24. Логистическая регрессия.
25. Бинарная линейная классификация.
26. Композиции моделей градиентный бустинг и блендинг.
27. Задача кластеризации. Карты Кахоннена.

28. Приведите классификацию экспертных систем по степени проработанности и отлаженности.
29. В чем отличие статических экспертных систем от динамических?
30. Опишите назначение и основные принципы построения экспертной системы MYCIN.

7.3.2 Типовые практические задания

1. Что называют данными в машинном обучении?

0. матрицы
a. объекты
b. признаки
c. алгоритм
d. функция

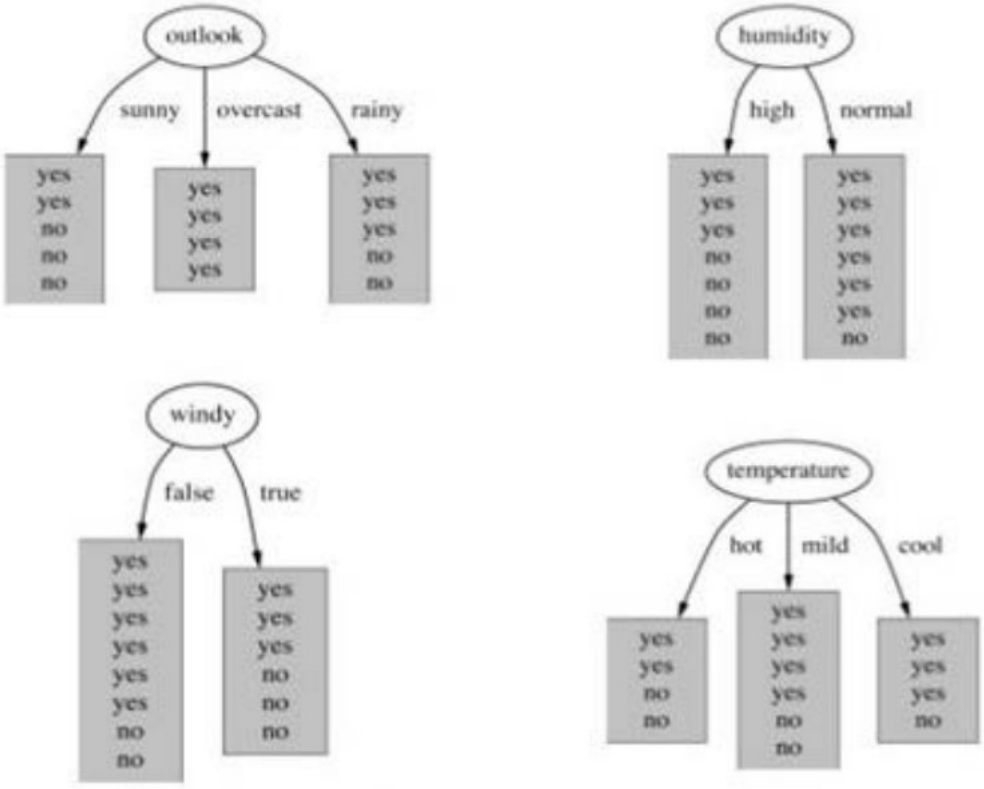
0. Предположим, у вас есть 5 ядер свертки в первом слое сверточной нейронной сети.Каждое ядро свертки имеет размер 7 × 7, имеет нулевое заполнение и имеет шаг 1. Размер входного изображения этого слоя составляет 224 × 224 × 3. Каков размер выходного сигнала этого слоя?

а) 218 x 218 x 5
б) 217 x 217 x 3
в) 217 x 217 x 8
г) 220 x 220 x 7

0. Какие из следующих форм алгоритм K-Means может не агрегировать?

а) Спиральное распределение
б) Круговое распределение
в) Ленточное распространение
г) Выпуклое распределение полигонов

0. При построении модели дерева решений мы разделяем узел для определенного атрибута. Какое из четырех изображений ниже соответствует наибольшему приросту информации?



а) outlook
б) humidity
в) windy
г) temperature

0. В n-мерном пространстве (n> 1) какой из следующих методов наиболее подходит для обнаружения выбросов?

а) расстояние Махаланобиса
б) Нормальная вероятность графика
в) Коробочный сюжет
г) поле корреляции

7.3.3 Типовой экзаменационный билет

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №1
по дисциплине
«Методы машинного обучения»
направление подготовки 09.03.01 Информатика и вычислительная техника

ВОПРОСЫ:

1. Регуляризация.

2. Иерархическая кластеризация.
3. Задача кластеризации. Карты Кахоннена.

Утверждено: _____ / _____ / «__» _____ 20__г.