

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ



УТВЕРЖДАЮ
Декан РТФ

УТВЕРЖДАЮ /А.Н. Дедов/
(Ф.И.О. декана (директора института))

13.02.2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б.1.2.12 Инженерия и применение методов машинного обучения для отрасли
инфокоммуникаций

(код и наименование дисциплины по учебному плану)

Направление подготовки
(специальность)

09.03.02 Информационные системы и технологии

Квалификация выпускника

Бакалавр

(бакалавр/магистр/специалист)

Направленность

Интеллектуальные информационные системы и
технологии

Курс 4
Семестр 7, 8

Распределение учебного времени

Трудоемкость по учебному плану	324 / 9	часов/зачетных единиц
Лекции	64	часов
Лабораторные работы	32	часов
Практические занятия	32	часов
Иная контактная работа	-	часов
Всего контактной работы (без учета экз.)	128	часов
Контактная работа по экзамену	-	часов
Курсовой проект (работа)	-	семестр
Самостоятельная работа обучающихся (без учета экз.)	196	часов
Самостоятельная работа по подготовке к экзамену	-	часов
Экзамен	-	семестр
Зачет	7	семестр
БРК, ДЗ	8	семестр

(год)

Программа составлена в соответствии с требованиями ФГОС ВО направления подготовки (специальности) 09.03.02 Информационные системы и технологии

Программу составили:

старший преподаватель	ИТРС	СОГЛАСОВАНО	Н.А. Конкин
(должность)	(кафедра)		(И.О. Фамилия)

РАССМОТРЕНА и ОДОБРЕНА на заседании кафедры, за которой закреплена дисциплина
Кафедра информационных технологий, радиотехники и связи

(наименование кафедры)		
13.01.2025	протокол №	2
(дата)		

Заведующий кафедрой	СОГЛАСОВАНО	Н.В. Рябова
		(И.О. Фамилия)

Рабочая программа СОГЛАСОВАНА с факультетом (институтом), выпускающей(ими)
кафедрой(ами).

СООТВЕТСТВУЕТ действующей ОП.

Заведующий кафедрой	СОГЛАСОВАНО	Н.В. Рябова
		(И.О. Фамилия)

Председатель методической комиссии факультета (института), в который входит
выпускающая кафедра

СОГЛАСОВАНО	А.Н. Дедов
	(И.О. Фамилия)

Эксперт(ы): Дудин Александр Николаевич , Исполнительный директор ООО «Трэвел Лайн
Системс»

Рабочая программа проверена и зарегистрирована в УМЦ 17.02.2025 г.

Специалист учебно-методического центра СОГЛАСОВАНО /Т.А. Смирнова/

Раздел 1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является достижение планируемых результатов обучения, соответствующих установленным в ОПОП индикаторам достижения компетенций:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения
1. FC-1 Способен проводить фронтальные исследования в области архитектур, алгоритмов машинного обучения, оптимизации и математики	FC-1.1. Разрабатывает фундаментальные основы и новые алгоритмы машинного обучения	знания: Знает современный математический аппарат глубокого обучения: методы оптимизации высоких размерностей, спектральные свойства веса и их связь с обобщением, вероятностные представления, вариационные принципы, информационно-теоретические ограничения моделей; математические основы self-supervised learning, contrastive learning, автоэнкодеров, низкоранговых факторизаций; принципы построения гибридных архитектур (модели сигналов + статистические модели + нейронные сети). умения: Умеет применять математические методы для анализа поведения обучающихся моделей, выбирать формализацию задачи обучения, проектировать самообучающиеся и гибридные архитектуры под данные инфокоммуникаций (трафик, QoS, спектральные данные); использовать методы регуляризации, самообучения и контрастивного обучения для повышения устойчивости моделей при неполных или слабых разметках. навыки: Владеет инструментами разработки гибридных моделей (autoencoder + классификатор, SSL-модели, модели признаковового сжатия); методами построения компактных моделей (низкоранговые разложения, distillation, sparse- факторизации), средствами вычислительной оптимизации и применяет их для повышения эффективности ML-систем.

FC-1.2. Разрабатывает новые архитектуры глубоких нейросетей	знания: Знает современные архитектуры (CNN, RNN, LSTM, GRU, Transformers, GNN), их внутренние механизмы (attention, residual connections, positional encoding), их вычислительные профили, требования к памяти и пропускной способности; связи между типом данных (сигналы, сетевые логи, временные ряды), задач (прогнозирование, классификация, детекция), архитектурой и вычислителем (GPU, FPGA, ARM-ядра, SDR-модули). умения: Умеет подбирать архитектуру под инфраструктуру (edge-устройства, облачные инстансы, SDR-радиосистемы), согласовывать модель с ограничениями вычислительных ресурсов; анализировать trade-off-ы между точностью, latency и энергопотреблением; адаптировать архитектуры к особенностям инфокоммуникационных данных. навыки: Владеет методами настройки и адаптации архитектур под конкретные вычислительные устройства, применяет оптимизации графа вычислений, выбирает стратегии аппаратного ускорения (TensorRT, ONNX Runtime, мобильные бэкенды), внедряет архитектуры, хорошо работающие в условиях реальных сетевых нагрузок.
FC-1.3. Развивает методы ускорения обучения	знания: Знает концепции low-rank factorization, матричных и тензорных разложений (SVD, Tucker, CP-decomposition, LoRA-подобные методы), их роль в уменьшении размера сети; современные оптимизаторы (AdamW, Lion, AdaFactor, second-order методы), принципы gradient clipping и scheduling стратегий. умения: Умеет применять низкоранговые разложения к полносвязным и сверточным слоям, правильно выбирать ранги, учитывать специфику архитектуры и задачи; проектировать pipeline обучения сжатых моделей; использовать оптимизационные методы, устойчивые к разреженности и низкому рангу. навыки: Владеет практикой построения сильно сжатых моделей с сохранением качества; средствами профилирования (FLOPs, memory footprint, latency); управлением оптимизационным циклом для трудных моделей — гибридных, трансформерных и высокоразмерных.

	ФС-1.4. Развивает методы оптимизации распределенного и федеративного обучения больших ИИ моделей	знания: Знает фундаментальные алгоритмы федеративного и распределённого обучения (FedAvg, FedProx, FedOpt, Secure Aggregation), их допущения, ограничения и уязвимости; виды атак на распределённые модели (model poisoning, data poisoning, gradient leakage). умения: Умеет проектировать распределённые сценарии обучения под сетевые системы, выбирать стратегии агрегации, осуществлять fault-tolerant обучение в условиях потерь пакетов или вариаций пропускной способности каналов; применять методы защиты данных в сетевых ML-потоках. навыки: Владеет инструментами построения устойчивых распределённых ML-систем, использует безопасные протоколы агрегации, применяет методы приватности (DP, зашумление градиентов, secure MPC), обеспечивая надёжность обучения больших моделей в сетевой среде.
2. ML-3 Способен применять классические алгоритмы машинного обучения с пониманием их математических основ и областей применения	ML-3.2. Эффективно применяет классические методы и модели машинного обучения для обеспечения достижимости функциональных характеристик систем ИИ	знания: Знает основы байесовского вывода и классификации, вероятностные модели; ансамблевые методы (бэггинг, бустинг, стэкинг), их статистические свойства; методы работы с временными рядами (ARIMA, SARIMA, ETS, Prophet, линейные модели с лагами). умения: Умеет строить ансамбли под задачи инфокоммуникаций (QoS-классификация, аномалия трафика), корректно выбирать гиперпараметры; анализировать сезонность, тренды и нерегулярности в сетевых временных рядах; применять байесовские методы на малых данных. навыки: Владеет методами создания стабильных ансамблей, сравнения вариантов, калибровки вероятностей; инструментами обработки временных рядов различной природы — дискретных, агрегированных, зашумлённых сетевых данных.

	ML-3.3. Оценивает результативность применения классических методов и моделей машинного обучения в задачах ИИ на основе сопоставления с аналогами	знания: Знает ограничения моделей: мультиколлинеарность, переобучение, проблемы несбалансированности, зависимость от масштаба признаков, неустойчивость к шуму; различия между классическими и современными deep-learning методами, области применимости ARIMA/SARIMA, SVM, GBDT. умения: Умеет анализировать применимость моделей к сетевым данным, выявлять случаи, когда классические методы не обеспечивают нужной точности или устойчивости; корректно выбирать альтернативы (глубокие модели, гибридные архитектуры, ансамбли). навыки: Владеет навыками построения обоснованных рекомендаций по выбору методов для телеком-систем, учитывая требования QoS, латентности, доступности вычислителей, особенности распределённых данных.
--	---	--

Раздел 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к части, формируемой участниками образовательных отношений ОПОП.

Дисциплина является обязательной

Для продолжения формирования заявленных компетенций необходимы знания предшествующих практик: Производственная практика. Технологическая (проектно-технологическая) практика (рассредоточенная) (FC-1), Производственная практика. Технологическая (проектно-технологическая) практика (FC-1), Производственная практика. Научно-исследовательская работа (FC-1), Производственная практика. Технологическая (проектно-технологическая) практика (рассредоточенная) (ML-3), Производственная практика. Технологическая (проектно-технологическая) практика (ML-3), Производственная практика. Научно-исследовательская работа (ML-3)

Изучаемая дисциплина является основой для продолжения формирования указанных компетенций в следующих государственной итоговой аттестации в форме: Выполнение и защита выпускной квалификационной работы (FC-1), Выполнение и защита выпускной квалификационной работы (ML-3)

Раздел 3. ОПИСАНИЕ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

Для формирования заявленных компетенций используются методологические технологии, реализующие деятельностный, личностно-ориентированный, практико-ориентированный подходы.

Основными стратегическими технологиями являются: лекционные занятия, практические и лабораторные занятия

На достижение конкретных целей обучения направлены применяемые тактические технологии: информационные, классическая лекция, мини-проекты

Раздел 4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Виды и темы занятий	Количество часов	Формируемые компетенции
№1 Классические методы и инженерные основы МО	108	FC-1, ML-3
Лекция. Лекция 1. Введение в инженерные аспекты машинного обучения в инфокоммуникациях – Роль МО в обработке сигналов и сетевых данных. – Цепочка ML-инженерии: данные, модель, развертывание. – Примеры применения (оптимизация каналов, QoS, адаптация протоколов).	8	
Лекция. Лекция 2. Классические алгоритмы классификации и регрессии – Байесовские методы, деревья решений, ансамбли (Bagging, Boosting, Stacking). – Анализ ограничений и выбора моделей для инфокоммуникационных-данных.	8	
Лекция. Лекция 3. Методы прогнозирования временных рядов – ARIMA, SARIMA, экспоненциальное сглаживание, Prophet. – Анализ трафика, QoE, задержки и помехи.	8	
Лекция. Лекция 4. Методы отбора признаков и снижения размерности – PCA, LDA, t-SNE, автоэнкодеры для признаков. – Отбор признаков для задач радиосетей и IoT-сенсорных систем.	8	
Практическое занятие. • Классификация сетевых пакетов с применением ансамблей (sklearn). • Прогноз нагрузки на канал связи с ARIMA и Prophet. • Применение PCA и автоэнкодеров для снижения размерности данных телеметрии. • Оценка эффективности моделей (cross-validation, ROC-AUC, F1, RMSE).	32	
Задания для самостоятельной работы, в том числе выполнение • Исследование современных методов классического МО в инфокоммуникационной-сфере. • Обзор сравнения ансамблей и нейросетей по критерию explainability. • Подготовка отчёта «Сравнение ARIMA и нейросетей для предсказания нагрузки».	44	
Иная контактная работа:	0	

8 семестр

Виды и темы занятий	Количество часов	Формируемые компетенции
№2 Глубокие и гибридные архитектуры	72	FC-1, ML-3
Лекция. Лекция 5. (4 ч) Современные архитектуры нейросетей – CNN, RNN, Transformers. – Особенности для сигналов, временных рядов, сетевых данных.	4	
Лекция. Лекция 6. (4 ч) Гибридные и самообучающиеся модели – Self-supervised learning, contrastive learning, autoencoder + классификатор. – Применение для задач с частично размеченными данными (QoS-мониторинг, радиоспектр).	4	

Лекция. Лекция 7. (4 ч) Сжатие и ускорение моделей – Pruning, quantization, knowledge distillation, low-rank factorization. – Инференс на ограниченных устройствах (SDR, IoT-узлы).	4	FC-1, ML-3
Лабораторная работа. • Реализация CNN и RNN для анализа сигналов и временных рядов. • Сжатие модели с помощью pruning и distillation. • Использование PyTorch Lightning для ускоренного	10	
Задания для самостоятельной работы, в том числе выполнение • Анализ современных архитектур CNN, RNN и Transformer по публикациям IEEE и arXiv. • Реализация прототипа гибридной модели (autoencoder + классификатор) на данных телеком-сети. • Сравнение эффективности методов самообучения и традиционного обучения на малых выборках. • Исследование методов сжатия моделей (quantization, pruning) на примере предобученной сети	50	
№3 Оптимизация и распределённое обучение	68	
Лекция. Лекция 8. (4 ч) Современные методы оптимизации – Адаптивные оптимизаторы (AdamW, Lion, Lookahead). – Learning rate schedules, second-order методы, gradient clipping.	4	
Лекция. Лекция 9. (4 ч) Федеративное и распределённое обучение – Архитектуры Federated Averaging, Secure Aggregation. – Применение в распределённых сетевых средах, защита данных.	4	FC-1, ML-3
Лабораторная работа. • Эксперимент с распределённым обучением PyTorch DDP. • Моделирование федеративного обучения для IoT-узлов. • Анализ компромисса «скорость — конфиденциальность — точность».	10	
Задания для самостоятельной работы, в том числе выполнение • Сравнение оптимизаторов (AdamW, Lion, RMSProp) на задаче предсказания параметров канала связи. • Исследование влияния параметров обучения (learning rate, batch size) на сходимость модели. • Подготовка отчёта по современным подходам федеративного обучения и их применению в IoT. • Моделирование распределённого обучения в симуляторе (PyTorch DDP или Ray).	50	
№4 Исследовательская и проектная ин	26	FC-1, ML-3
Лекция. Лекция 10. (4 ч) Проектирование и оценка эффективности ИИ-систем – Метрики, А/В-тесты, доверительные интервалы, бизнес-эффект. – Верификация моделей в производственной телеком-среде.	4	
Лекция. Лекция 11. (4 ч) Инженерные практики MLOps для инфокоммуникаций – CI/CD для ML, MLflow, Kubeflow, мониторинг моделей, retraining. – Архитектура ML-поток в телеком-инфраструктуре.	4	
Лекция. Лекция 12. (4 ч) Фронтирные направления ML для	4	

инфокоммуникаций – Edge AI, Graph Neural Networks, reinforcement learning для управления сетями. – Обзор современных публикаций IEEE, ITU, Elsevier.		
Лабораторная работа. • MLOps pipeline: автоматическое развертывание модели прогноза QoS. • Проектирование гибридной модели (CNN + GRU) для анализа сетевого трафика. • Исследовательский мини-проект по теме студента (с отчётом и презентацией).	12	
Задания для самостоятельной работы, в том числе выполнение РГР Задания для самостоятельной работы, в том числе выполнение Курсового проекта в рамках задач от АО "ММЗ" (общее направление): Разработка ML-системы для решения задач отрасли, связанных с автоматизацией процессов предприятия, обработкой данных, безопасностью и повышением эффективности производственных и информационных систем.	2	
Иная контактная работа:	0	

Раздел 5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Изучение модуля рекомендуется начать с ознакомления с рабочей программой, ее структурой и содержанием разделов. Учебный материал структурирован, изучение дисциплины осуществляется в тематической последовательности.

Занятия лекционного типа дают систематизированные знания по модулю, концентрируют внимание на наиболее сложных и важных вопросах. Во время лекционных занятий рекомендуется вести конспектирование учебного материала; обращать внимание на формулировки и категории, раскрывающие суть проблемы, явления или процесса; зафиксировать выводы и практические рекомендации. Подготовка к **занятиям семинарского типа** включает ознакомление с планом лабораторного занятия; работу с конспектом лекций, выполнение домашнего задания, работу с учебной и учебно-методической литературой, научными изданиями и электронными образовательными ресурсами, рекомендованными рабочей программой модуля.

Содержание **самостоятельной работы** определяется рабочей программой модуля, оценочными и методическими материалами, заданиями и указаниями преподавателя. Самостоятельная работа может осуществляться в аудиторной и внеаудиторной формах. Эффективным средством осуществления самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к образовательной программе, рабочей программе модуля, к электронным библиотечным системам, профессиональным базам данных и информационным справочным системам. Периодичность проведения, формы текущего контроля успеваемости, система оценивания хода освоения дисциплины представлены в рабочей программе. Формой промежуточной аттестации по модулю за 7 семестр является зачёт, за 8 семестр БРК.

Контроль и аттестация

Периодичность проведения, формы текущего контроля успеваемости, система оценивания хода освоения дисциплины представлены в рабочей программе.

Формой промежуточной аттестации по дисциплине является БРК.

1. Необходимое программное обеспечение и инструментальные средства

Среды разработки

В качестве среды разработки для языка программирования Python рекомендуется использовать следующие решения:

1. **Visual Studio Code** (<https://code.visualstudio.com/>) — универсальный редактор с богатыми возможностями для Python-разработки
2. **PyCharm Community Edition** (<https://www.jetbrains.com/pycharm/>) — специализированная IDE для Python
3. **Jupyter Notebook/JupyterLab** (<https://jupyter.org/>) — интерактивная среда для исследовательской работы с данными

Облачные платформы для машинного обучения

Для организации удаленного коллективного решения задач машинного обучения рекомендуется использовать следующие платформы:

1. **Google Colaboratory** (<https://colab.research.google.com/>) — облачная среда с бесплатным доступом к GPU/ TPU, интеграцией с Google Drive и поддержкой Jupyter Notebook
2. **Kaggle** (<https://www.kaggle.com/>) — платформа для соревнований по машинному обучению с большим разнообразием датасетов, примеров решений и возможностью работы в облачных ноутбуках с GPU
3. **Kaggle Learn** (<https://www.kaggle.com/learn>) — бесплатные интерактивные курсы по Python, машинному обучению и глубокому обучению.

2. Содержание дисциплины включает изучение исследований и разработок, представленных в научных публикациях на конференциях уровня А*, статьях, опубликованных в журналах 1 уровня Белого списка научных журналов Минобрнауки России (УММ на основе публикаций в научных журналах 1 или 2 уровня Белого списка научных журналов Минобрнауки России, публикаций на конференциях уровня А*/А.

Ниже приведен перечень конференций, рекомендуемых для подачи работ, соответствующих уровню подготовки студентов:

1. Conference on Neural Information Processing Systems (NeurIPS)

Conference on Neural Information Processing Systems (NeurIPS) : международная конференция по машинному обучению и вычислительной нейробиологии. – Электрон. дан. – Режим доступа: <https://neurips.cc/>

2. International Conference on Machine Learning (ICML)

International Conference on Machine Learning (ICML) : международная конференция по машинному обучению. – Электрон. дан. – Режим доступа: <https://icml.cc/>

3. International Conference on Learning Representations (ICLR)

International Conference on Learning Representations (ICLR) : международная конференция по обучению представлениям. – Электрон. дан. – Режим доступа: <https://iclr.cc/>

4. AAAI Conference on Artificial Intelligence (AAAI)

AAAI Conference on Artificial Intelligence (AAAI) : международная конференция по искусственному интеллекту. – Электрон. дан. – Режим доступа: <https://aaai.org/conference/>

5. International Joint Conference on Artificial Intelligence (IJCAI)

International Joint Conference on Artificial Intelligence (IJCAI) : международная конференция по искусственному интеллекту. – Электрон. дан. – Режим доступа: <https://www.ijcai.org/>

6. ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD)

ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD) : международная конференция по анализу данных и интеллектуальному анализу больших данных. – Электрон. дан. – Режим доступа: <https://www.kdd.org/>

7. IEEE International Conference on Data Mining (ICDM)

IEEE International Conference on Data Mining (ICDM) : международная конференция по интеллектуальному анализу данных. – Электрон. дан. – Режим доступа: <https://waset.org/data-mining-conference-in-july-2026-in-istanbul>

8. ACM Conference on Economics and Computation (EC)

ACM Conference on Economics and Computation (EC) : международная конференция по экономике вычислений, алгоритмам и мультиагентным системам. – Электрон. дан. – Режим доступа: <https://www.sigecom.org/meetings/winter25/>

3. Предусмотрено участие ИТ-практиков в различных форматах обучения (лекции, семинары с ИТ-практиками, конкурсы, хакатоны, кейс-чемпионаты, мастер-классы, командные проектные задания и др.) и в качестве наставников.

В программе предусмотрено изучение кейсов (кейсы для изучения, практической и проектной работы) и реальных задач (проектов по разработке, внедрению, развитию цифровых технологий, ИТ-разработок и др.) из практического опыта Индустриальных партнеров в объеме не менее 1 кейса на 1 з.е.

Расчётно-графическая работа (РГР)

Цель: Разработка ML-системы для решения задач отрасли, связанных с автоматизацией процессов предприятия, обработкой данных, безопасностью и повышением эффективности производственных и информационных систем.

Студент выбирает **одну** из нижеперечисленных тем и выполняет полный цикл инженерного исследования: анализ задачи и данных, выбор и обоснование алгоритмов, проектирование архитектуры, реализация ключевых модулей, оценка качества, демонстрация интеграции в реальную производственную или корпоративную среду.

Структура выполнения РГР:

- Анализ предметной области и постановка задачи**
 - определение входных данных и сценариев использования;
 - анализ ограничений (ресурсы, корпоративная среда, безопасность, приватность);
 - требования к качеству и метрикам.

Обзор подходов и выбор методов
– анализ классических и современных ML-алгоритмов;
– обоснование выбора модели под задачу, данные и вычислительные ограничения;

- Проектирование архитектуры ML-решения
 - структура пайплайна: от приёма данных до инференса и логирования;
 - взаимодействие подсистем и интеграция с корпоративной инфраструктурой;
 - требования к безопасности, устойчивости и мониторингу.
- Реализация ключевых модулей
 - обработка данных;
 - обучение и оптимизация моделей;

1. – реализация оценки качества и UX для бизнес-пользователей;
– прототип API или pipeline.
2. Эксперименты и оценка
 - сравнение моделей;
 - анализ ошибок;
 - интерпретация модели;
 - тестирование нагрузки, устойчивости, скорости инференса.
3. Интеграционный сценарий (обязательно для всех тем)
 - демонстрация возможности подключения к существующей системе предприятия
 - описание API / веб-сервиса / очереди сообщений / событийной шины;
 - учёт требований реального корпоративного окружения.
4. Выводы и рекомендации
 - инженерные выводы;
 - экономическая и производственная эффективность;
 - риски внедрения;
 - направления улучшения.

Темы курсовых проектов:

Тема 1. Разработка и внедрение NLP-системы для автоматизации внутренних коммуникаций и документооборота предприятия

- | | |
|---|----------------|
| Содержание | работы: |
| – анализ классических методов NLP и современных трансформеров; | |
| – применение open-source моделей (BERT, LLaMA, Mistral и др.); | |
| – адаптация под корпоративные документы (дообучение, LoRA, fine-tuning); | |
| – построение локальной системы инференса без облачных сервисов; | |
| – интеграция с почтой, ServiceDesk, корпоративными базами знаний; | |
| – оценка точности, стабильности, классификации intents, NER, summarization. | |

Тема 2. Создание и тестирование системы распознавания речи для автоматизации набора текста

- | | |
|---|----------------|
| Содержание | работы: |
| – выбор алгоритмов ASR (HMM-based, CTC, transformer-модели); | |
| – шумоподавление и обработка аудиосигналов; | |
| – адаптация к акцентам, диалектам и отраслевой терминологии; | |
| – интеграция с корпоративными системами обработки документов; | |
| – оценка WER, CER, устойчивости к помехам; | |
| – демо API или интерфейса голосового ввода. | |

Тема 3. Применение компьютерного зрения для автоматизации идентификации объектов в производственных процессах

Содержание

работы:

– разработка моделей для распознавания деталей и компонентов:

- CNN, Vision Transformers, YOLO/DETR;
 - создание набора данных (аугментации, синтетические данные);
 - интеграция с ERP/SCADA/системами контроля качества;
 - оценка точности, скорости, устойчивости к освещению и шумам;
 - оценка производственного эффекта: сниженные ошибки и время операций.

Тема 4. Обеспечение безопасности ИИ-систем в промышленной среде

Содержание

работы:

- анализ угроз: data poisoning, model inversion, adversarial attacks, shadow models;
- методы защиты: дифференциальная приватность, защищённые градиенты, шифрование;
- проектирование безопасного ML-pipeline;
- регламент аудита ML-моделей в корпоративной среде;
- имитация атак и оценка устойчивости системы;
- рекомендации по безопасному развёртыванию ИИ-моделей на предприятии.

Тема 5. Оптимизация производственных процессов с использованием алгоритмов ML

Содержание

работы:

- прогнозирование потребностей в ресурсах;
- оптимизация маршрутов и планирование;
- анализ производительности сотрудников;
- применение ансамблей, градиентных бустингов, временных моделей;
- оценка экономического эффекта;
- интеграция рекомендаций в корпоративные информационные системы.

Тема 6. Разработка ML-системы для автоматизации анализа больших производственных данных

Содержание

работы:

- обработка структурированных и неструктурированных данных;
- выявление трендов, аномалий, причин отклонений;
- модели anomaly detection, clustering, forecasting;
- интеграция с мониторинговыми системами предприятия;
- визуализация, отчётность, автоматические аналитические сводки.

Тема 7. Создание ИИ-инструментов для автоматизации тестирования и контроля качества продукции

Содержание

работы:

- ML-алгоритмы визуального и функционального контроля;
- обнаружение дефектов: классические CV-методы и глубокие сети;
- интеграция с системами контроля качества и производственной отчётности;
- оценка точности, скорости, устойчивости;
- создание прототипа системы автоматического тестирования изделий.

4. Рекомендованные источники учебно-методической литературы из:

Дополнительные ссылки на источники информации (КРМ)

FC-1:

1. Yandex ML Handbook — Linear Models

Yandex. Linear models // Yandex Education. URL: <https://education.yandex.ru/handbook/ml/article/linear-models>

2. Курс Оселедца по линейной алгебре

Oseledets I. Numerical Linear Algebra Course (2024). GitHub Repository. URL: <https://github.com/oseledets/nla2024>

3. Е. Е. Тыртышников — Матричный анализ и линейная алгебра

Тыртышников Е. Е. Матричный анализ и линейная алгебра. Москва: Физматлит.

4. CUDA Kernels (PyTorch C++ Extensions)

PyTorch. Custom C++ and CUDA Extensions // PyTorch Tutorials. URL: https://docs.pytorch.org/tutorials/advanced/cpp_extension.html

5. NVIDIA CUDA Best Practices

NVIDIA. CUDA C Best Practices Guide. URL: <https://docs.nvidia.com/cuda/cuda-c-best-practices-guide/>

6. Explicit loss asymptotics in the gradient descent training of neural networks // NeurIPS 2021. URL: https://proceedings.neurips.cc/paper_files/paper/2021/file/14faf969228fc18fcd4fcf59437b0c97-Paper.pdf

7. To Stay or Not to Stay in the Pre-train Basin: Insights on Ensembling in Transfer Learning URL: https://proceedings.neurips.cc/paper_files/paper/2023/file/336572db3e99930814d6b328d4220cb6-Paper-Conference.pdf

8. Визуализация ландшафта — классическая статья (NeurIPS 2018)

Li H. et al. Visualizing the Loss Landscape of Neural Nets // NeurIPS 2018. URL: https://proceedings.neurips.cc/paper_files/paper/2018/file/a41b3bb3e6b050b6c9067c67f663b915-Paper.pdf

9. Neuro-Visualizer: An Auto-encoder-based Loss Landscape Visualization Method. URL: <https://arxiv.org/pdf/2309.14601>

10. Репозиторий NeuroVisualizer

Elhamod M. NeuroVisualizer: Loss Landscape Visualization Toolkit. GitHub Repository. URL: <https://github.com/elhamod/NeuroVisualizer>

11. A Survey to Recent Progress Towards Understanding In-Context Learning. URL: <https://arxiv.org/pdf/2402.02212>

12. Модель обучается на одном примере — fast.ai

Howard J. Learning Jumps: How Models Learn from a Single Example // Fast.ai Blog (2023). URL: <https://www.fast.ai/posts/2023-09-04-learning-jumps/>

13. How to Train Data-Efficient LLMs. A Survey. URL: <https://arxiv.org/html/2402.09668v1>

14. А. Безносииков — Методы оптимизации (МФТИ)

Безносииков А. Методы оптимизации. Курс лекций МФТИ. URL: https://vkvideo.ru/playlist/-206078025_72

15. Synthetic-2 Dataset

Prime Intellect. Synthetic-2 Dataset Overview. URL: <https://www.primeintellect.ai/blog/synthetic-2>

16. FATE-LLM

FederatedAI. FATE-LLM Framework. GitHub Repository. URL: <https://github.com/FederatedAI/FATE-LLM>

MF-3:

1. Герасимов, А. В. Оптимизация и улучшение производительности моделей машинного обучения [Электронный ресурс] / А. В. Герасимов, В. Л. Кошкин. — Электрон. дан. — Москва : ДМК Пресс, 2020. — 350 с. — Режим доступа: <https://e.lanbook.com/book/4731>
2. Станкевич, А. В. Методы улучшения качества машинного обучения: подбор гиперпараметров, регуляризация и оптимизация [Электронный ресурс] / А. В. Станкевич. — Электрон. дан. — Санкт-Петербург : Питер, 2018. — 297 с. — Режим доступа: <https://e.lanbook.com/book/3845>
3. Фомина, И. В. Современные методы улучшения качества моделей ИИ [Электронный ресурс] / И. В. Фомина. — Электрон. дан. — Москва : Лань, 2021. — 342 с. — Режим доступа: <https://e.lanbook.com/book/5091>
4. Кузнецов, А. В. Методы улучшения производительности машинного обучения и ИИ: регуляризация, оптимизация гиперпараметров, ускорение обучения [Электронный ресурс] / А. В. Кузнецов. — Электрон. дан. — 2021. — Режим доступа: <https://habr.com/ru/articles/509482/>

Изучение современных технологий по материалам конференций:

1. Современные архитектуры → CNN, RNN, Transformers

Vaswani A., Shazeer N., Parmar N., et al. “Attention Is All You Need.” // NeurIPS, 2017.
<https://proceedings.neurips.cc/paper/2017/file/3f5ee243547dee91fbd053c1c4a845aa-Paper.pdf>

Кратко: Базовая работа, заложившая основу Transformer-архитектур, полностью заменивших RNN/CNN во многих областях — NLP, CV, обработка сигналов.

2. Self-Supervised Learning и Contrastive Learning: Chen T., Kornblith S., Norouzi M., Hinton G. “A Simple Framework for Contrastive Learning of Visual Representations (SimCLR).” // ICML, 2020.

<https://proceedings.mlr.press/v119/chen20j.html>

Кратко: Метод показывает, как без размеченных данных обучать эффективные эмбединги. Используется в задачах мониторинга QoS, промышленных данных, телеком-поток.

3. Low-Rank Compression / Model Acceleration Li H., Zhang X., Ren J., Sun J. “Pruning Filters for Efficient ConvNets.” // ICLR, 2017.

<https://arxiv.org/abs/1608.08710>

Кратко: Один из первых и наиболее применяемых подходов к структурной компрессии CNN. Полезен для инференса на IoT/SDR-устройствах.

4. Federated Learning и распределённая оптимизация: McMahan H. B., Moore E., Ramage D., et al. “Communication-Efficient Learning of Deep Networks from Decentralized Data (FedAvg).” // AISTATS, 2017.

<https://arxiv.org/abs/1602.05629>

Кратко: Основополагающая статья по федеративному обучению — архитектура FedAvg. Нужна для тем по распределённому обучению в телеком-сетях.

6. Edge AI и оптимизация модели для устройств: Han S., Mao H., Dally W. J. “Deep Compression.” // ICLR, 2016.

<https://arxiv.org/abs/1510.00149>

Кратко: Комбинация pruning + quantization + Huffman coding. Классическая работа для оптимизации моделей под устройство.

7. Методы сжатия и ускорения обучения

Frankle J., Carbin M. "The Lottery Ticket Hypothesis." // ICLR, 2019.

<https://arxiv.org/abs/1803.03635>

Кратко: Показывает, что в больших сетях существуют «подсети-выигрышные билеты», которые можно обучить лучше и быстрее. Полезно для ML-инженерии.

8. Гибридные и самообучающиеся модели (Autoencoders + классификаторы): Kingma D. P., Welling M. "Auto-Encoding Variational Bayes." // ICLR, 2014.

<https://arxiv.org/abs/1312.6114>

Кратко: Основная работа по вариационным автоэнкодерам. Используется для анализа сетевых аномалий, QoE, телеком-трафика.

9. Методы оптимизации (AdamW, Lookahead)

Loshchilov I., Hutter F. "Fixing Weight Decay Regularization in Adam (AdamW)." // ICLR, 2019.

<https://arxiv.org/abs/1711.05101>

Кратко: Улучшает обобщение и стабильность оптимизации глубоких сетей. Один из стандартов для современных нейросетей.

5. Эффективным средством осуществления самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к образовательной программе, рабочей программе дисциплины, к электронным библиотечным системам, профессиональным базам данных и информационным справочным системам. А также рекомендованные ОТКРЫТЫЕ ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ (на платформе LMS Moodle (elearning.volgatech.net), интегрированного с федеральной платформой ГИС СЦОС online.edu.ru открытый образовательный портал (mooped.net) и ресурсы открытых образовательных платформ Яндекс-Практикум, Сберуниверситет.

Рекомендуемые образовательные ресурсы

Курсы по машинному обучению и искусственному интеллекту

1. "Введение в Data Science и машинное обучение" (<https://stepik.org/course/4852/>)

- Основы анализа данных
- Классические алгоритмы ML
- Библиотеки NumPy, pandas, scikit-learn

1. "Нейронные сети и обработка текста" (<https://stepik.org/course/54098/>)

- Архитектуры нейронных сетей
- Natural Language Processing
- Практика на реальных задачах

1. "Введение в глубокое обучение" от HSE (<https://stepik.org/course/135003/>)

- Теория глубокого обучения
- PyTorch и TensorFlow
- Компьютерное зрение и NLP

Специализированные курсы

1. "MLOps: практики и инструменты" (<https://stepik.org/course/181476/>)

- Версионирование моделей и данных
- CI/CD для ML-проектов
- Мониторинг моделей в продакшене

Интерактивные платформы для практики

1. **LeetCode** (<https://leetcode.com/>) — алгоритмические задачи на Python
2. **HackerRank** (<https://www.hackerrank.com/domains/python>) — задачи по программированию и ML

Kaggle Competitions (<https://www.kaggle.com/competitions>) — соревнования по анализу данных

Раздел 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Учебно-методическое обеспечение

№№ п/п	Список используемой литературы	Количество экземпляров печатных изданий, имеющих в библиотеке, или электронный адрес издания (ресурса) в сети Интернет
УЧЕБНЫЕ, УЧЕБНО-МЕТОДИЧЕСКИЕ И НАУЧНЫЕ ИЗДАНИЯ		
1.	Модели и способы взаимодействия пользователя с киберфизическим интеллектуальным пространством [Электронный ресурс] : монография / И. В. Ватаманюк, Д. К. Левоневский, Д. А. Малов [и др.]. Санкт-Петербург: Лань, 2022. - 176 с. ISBN 978-5-8114-3877-8.	https://e.lanbook.com/book/206672
2.	Макшанов, А. В. Большие данные. Big Data [Электронный ресурс] : учебник для вузов / Макшанов А. В., Журавлев А. Е., Тындыкарь Л. Н.; Журавлев А. Е., Тындыкарь Л. Н. 3-е изд., стер. Санкт-Петербург: Лань, 2023. - 188 с. ISBN 978-5-507-46866-9.	https://e.lanbook.com/book/322664
3.	Цехановский, В. В. Архитектор информационных систем: как проектировать большие системы [Электронный ресурс] / Цехановский В. В. Москва, Алматы: Ай Пи Ар Медиа, EDP Hub (Идипи Хаб), 2024. - 284 с. ISBN 978-5-4497-2315-4.	https://www.iprbookshop.ru/133454.html
4.	Сузи, Р. А. Язык программирования Python [Электронный ресурс] / Сузи Р. А. 2-е изд. Москва: ИНТУИТ, 2016. - 350 с. ISBN 5-9556-0058-2.	https://e.lanbook.com/book/100546
5.	Хабаров, С. П. Построение распределенных систем на базе WebSocket [Текст] : учебное пособие для вузов / Хабаров С. П., Шилкина М. Л. 2-е изд., стер. Санкт-Петербург: Лань, 2022. - 216 с. ISBN 978-5-8114-9572-6.	https://e.lanbook.com/book/200510
6.	Борзунов, С. В. Алгебра и геометрия с примерами на Python [Электронный ресурс] / Борзунов С. В., Кургалин С. Д. 3-е изд., стер. Санкт-Петербург: Лань, 2022. - 444 с. ISBN 978-5-8114-9980-9.	https://e.lanbook.com/book/202154
7.	Хахаев, И. А. Практикум по алгоритмизации и	

программированию на Python [Электронный ресурс] / Хахаев И. А. 2-е изд. Москва: ИНТУИТ, 2016. - 178 с.	https://e.lanbook.com/book/100377
--	---

6.2. Материально-техническая база и программное обеспечение

№№ п/п	Аудитории для проведения учебных занятий, самостоятельной работы и проведения государственной итоговой аттестации	Перечень основного оборудования	Программное обеспечение
1.	333б (II)	Комплект учебной мебели (1)	Microsoft Windows Enterprise, Справочная правовая система "Консультант Плюс", Microsoft Office Standard, Агент Dr.Web, Комплект ГАРАНТ-Мастер, Microsoft Access, Microsoft Visio Professional, Microsoft Project Professional, Microsoft Visual Studio Enterprise, Комплект ПО для решения основных пользовательских задач, Mathcad University Classroom Perpetual - 40, LABVIEW
2.	333г (III)	Измерительный прибор "BerCut-E" (1), Комплекс ПАИК/77100/КПВ (1), Комплект дополнит.оборудования к ПАИК/7710/КПВ(автогенератор AnCom и автоответчи (1), Компьютер P4-3.0/2*256Mb/HDD 200Gb/128 6600GT/DVD-RW/KM/FDD/MBi945P/UPS (1), Ксерокс Canon FC-860 (1), Междисциплинарная лабораторная платформа в комплекте с аппаратно-программным кон (10), Монитор 19"Samsung 940N (LKSB) TFT (1), Принтер HP Laser Jet 1100 (1), Систем.блок Core2 DUOE6300/1024Mb*2/320Gb/DVD-RW/клав.мышь.ковр. (1), Комплект учебной мебели (1)	Microsoft Windows Enterprise, Справочная правовая система "Консультант Плюс", Microsoft Office Standard, Агент Dr.Web, Комплект ГАРАНТ-Мастер, Microsoft Access, Microsoft Visio Professional, Microsoft Project Professional, Microsoft Visual Studio Enterprise, Комплект ПО для решения основных пользовательских задач, Mathcad University Classroom Perpetual - 40, LABVIEW
3.	431 (III)	Доска маркерная 120x240 см. ауд.431 (2), Кабель VGA 30.5 М KRAMER (П-П) (1), Проектор мультимедийный Hitachi CP-X8150 (1), Экран настенный с	Microsoft Windows Enterprise, Справочная правовая система "Консультант Плюс", Microsoft Office

		электроприводом 400x300см (1), Комплект учебной мебели (1)	Standard, Агент Dr.Web, Комплект ГАРАНТ- Мастер, Microsoft Access, Microsoft Visio Professional, Microsoft Project Professional, Microsoft Visual Studio Enterprise, Комплект ПО для решения основных пользовательских задач, Mathcad University Classroom Perpetual - 40, LABVIEW
4.	433 (III)	Акустический комплект с микшером CRATE PA 8FX (1), Микшерный пульт компактный мал шумящий Behringer XENYX 1202FX (1), Подавитель шума ALTAIR NG-440 4-х канальный (1), Экран настенный с электроприводом 400*300 Braun (1), Комплект учебной мебели (1)	Microsoft Windows Enterprise, Справочная правовая система "Консультант Плюс", Microsoft Office Standard, Агент Dr.Web, Комплект ГАРАНТ- Мастер, Microsoft Access, Microsoft Visio Professional, Microsoft Project Professional, Microsoft Visual Studio Enterprise, Комплект ПО для решения основных пользовательских задач, Mathcad University Classroom Perpetual - 40, LABVIEW

Раздел 7. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ/ ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Критерии оценивания индикаторов достижения компетенций направлены на:

- усвоение теоретического материала (объем знаний, глубина усвоения), предусмотренного рабочей программой;
- умение излагать материал (четкость, грамотность изложения материала, точность и полнота воспроизведения учебного материала);
- умение применять теоретические знания при решении практических заданий.

Шкала оценивания представлена ниже.

Уровень сформированности элементов компетенции	Критерии оценивания	Шкала оценивания
Пороговый уровень	Обучающийся имеет знания основного материала, проявляет умение логично его излагать, но может допускать неточности в изложении материала, недостаточно правильные формулировки, испытывает затруднения в выполнении практических заданий.	удовлетворительно
Продвинутой	Обучающийся твердо знает программный материал,	хорошо

уровень	излагает его грамотно и по существу, не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения	
Высокий уровень	Обучающийся глубоко и прочно усвоил программный материал, грамотно и логически стройно его излагает, дает исчерпывающие ответы на поставленные вопросы. В ответе тесно увязывается теория с практикой, при этом обучающийся не затрудняется с ответом при видоизменении задания, свободно справляется с задачами, вопросами и другими видами применения знаний, показывает знакомство с монографической литературой, периодическими изданиями, правильно обосновывает принятые решения, свободно владеет разносторонними навыками, приемами выполнения практических работ	отлично

7.1. Текущий контроль успеваемости

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины (модуля) и производится с применением технологии рейтингового контроля в соответствии с технологической картой дисциплины. Порядок составления технологической карты и алгоритм проведения процедуры оценивания видов деятельности обучающихся, направленных на освоение знаний, умений, навыков и/или опыта деятельности, по накопительной системе в баллах устанавливается положением о системе РИТМ в ФГБОУ ВО «ПГТУ»

7.2. Промежуточная аттестация обучающихся

Промежуточная аттестация обучающихся направлена на оценивание результатов обучения по дисциплине (модулю) и проводится с использованием фондов оценочных средств.

Примеры типовых контрольных заданий из базы фонда оценочных средств по образовательной программе.

Семестр №7

Компетенция ML-3: Классические алгоритмы МО для инфокоммуникаций

Множественный выбор

1. Укажите ансамблевые методы, которые снижают дисперсию предсказаний через усреднение независимых моделей.

a) Бэггинг (Bootstrap Aggregating) b) Random Forest с рандомизацией признаков c) Gradient Boosting (AdaBoost, XGBoost) d) Стэкинг разнородных моделей через мета-обучение

2. Определите характеристики временных рядов сетевого трафика, которые требуют специальной обработки в моделях прогнозирования.

a) Множественная сезонность (суточная, недельная, годовая) b) Нестационарность с трендами и структурными сдвигами c) Стационарность с постоянными статистическими свойствами d) Отсутствие автокорреляции между наблюдениями

3. Выберите методы работы с несбалансированными классами в задачах классификации QoS для сетевого трафика.

a) SMOTE для генерации синтетических примеров миноритарного класса b) Class weights в функции потерь для увеличения штрафа за ошибки c) Увеличение общего размера выборки без учёта пропорций d)

Использование ассигасы как единственной метрики качества

4. Укажите проблемы, возникающие при применении линейных моделей к высокоразмерным признаковым пространствам сетевых данных.

a) Мультиколлинеарность между коррелированными сетевыми метриками b) Curse of dimensionality и разреженность данных c) Автоматическое выявление нелинейных зависимостей между признаками d) Гарантированная робастность к выбросам без дополнительных техник

5. Определите модели временных рядов, которые эффективны для краткосрочного прогнозирования нагрузки сетевого оборудования.

a) ARIMA для моделирования автокорреляции и краткосрочных зависимостей b) Экспоненциальное сглаживание (ETS) с адаптивными весами c) Prophet с длинной историей для сложной сезонности d) Наивная модель с предсказанием последнего наблюдаемого значения

6. Выберите статистические свойства байесовских методов, которые делают их полезными для задач с малыми данными в телекоммуникациях.

a) Включение априорных знаний через prior distributions b) Получение апостериорных распределений для оценки неопределённости c) Гарантированная вычислительная эффективность на больших данных d) Отсутствие гиперпараметров для настройки

7. Укажите метрики качества, которые подходят для оценки моделей классификации типов сетевого трафика при несбалансированных классах.

a) F1-score (гармоническое среднее precision и recall) b) Matthews Correlation Coefficient (MCC) c) Accuracy без учёта распределения классов d) Mean Squared Error для категориальных предсказаний

8. Определите ограничения моделей ARIMA/SARIMA при применении к реальным сетевым временным рядам.

a) Предположение о линейных зависимостях ограничивает моделирование нелинейностей b) Необходимость ручного подбора порядков модели через ACF/PACF c) Автоматическая адаптация к структурным сдвигам в данных d) Гарантированная робастность к выбросам и аномалиям

Установление последовательности

9. Расположите этапы построения ансамбля моделей для классификации аномалий сетевого трафика в правильном порядке.

a) Подготовка данных и feature engineering для сетевых признаков b) Обучение разнородных базовых моделей с различными алгоритмами c) Оптимизация весов комбинирования или обучение мета-модели d) Калибровка вероятностей и валидация на тестовой выборке

10. Установите последовательность действий при применении SARIMA для прогнозирования нагрузки сетевого канала.

a) Визуализация и декомпозиция ряда на тренд, сезонность и остатки b) Проверка стационарности и определение порядков дифференцирования c) Подбор порядков AR и MA через ACF/PACF или информационные критерии d) Диагностика остатков и валидация прогнозов на hold-out данных

11. Расположите шаги применения байесовской классификации для определения типа сетевого протокола в правильном порядке.

a) Определение априорных распределений классов $P(C)$ b) Моделирование функций правдоподобия $P(X|C)$ для признаков c) Вычисление апостериорных вероятностей $P(C|X)$ через теорему Байеса d) Выбор класса с максимальной апостериорной вероятностью (MAP)

12. Установите последовательность этапов при построении модели Prophet для прогнозирования объёма сетевого трафика с множественной сезонностью.

a) Подготовка данных и определение периодов множественной сезонности b) Создание модели с указанием компонент и настройкой гиперпараметров c) Обучение модели через MAP-оптимизацию аддитивных

компонент d) Генерация прогнозов с доверительными интервалами и валидация

Установление соответствия

13. Установите соответствие между ансамблевыми методами и их ключевыми характеристиками для телеком-задач.

Методы:

1. Бэггинг (Bagging)
2. Бустинг (Boosting)
3. Стэкинг (Stacking)

Характеристики: а) Параллельное обучение на бутстрэп-выборках для снижения дисперсии б) Последовательная коррекция ошибок для снижения смещения с) Комбинирование разнородных моделей через мета-обучение d) Взвешивание примеров для фокусировки на сложных случаях е) Случайный выбор подмножества признаков при каждом разбиении

14. Установите соответствие между моделями временных рядов и их оптимальными применениями в инфокоммуникационных системах.

Модели:

1. ARIMA/SARIMA
2. Prophet
3. Vector Autoregression (VAR)

Применения: а) Краткосрочное прогнозирование одномерных рядов с автокорреляцией и сезонностью б) Долгосрочное прогнозирование с множественной сезонностью и обработкой аномалий с) Моделирование взаимозависимостей между множеством связанных метрик d) Обнаружение структурных сдвигов в нестационарных рядах е) Прогнозирование с учётом экзогенных переменных и внешних факторов

15. Установите соответствие между проблемами при работе с сетевыми данными и методами их решения.

Проблемы:

1. Мультиколлинеарность признаков
2. Несбалансированность классов
3. Выбросы и аномалии

Методы решения: а) Ridge-регуляризация, PCA или анализ VIF с удалением признаков б) SMOTE, class weights или балансировка в ансамблях с) Робастные методы, статистическая фильтрация или модели детекции аномалий d) Увеличение размера обучающей выборки через дубликацию е) Нормализация признаков и стандартизация целевой переменной

16. Установите соответствие между статистическими свойствами моделей и их влиянием на применимость к телеком-задачам.

Свойства:

1. Линейность модели
2. Предположение о нормальности остатков
3. Независимость наблюдений

Влияние: а) Ограничивает моделирование нелинейных зависимостей в трафике б) Нарушается при выбросах, требует робастных методов с) Нарушается в временных рядах, требует учёта автокорреляции d) Обеспечивает автоматическую интерпретируемость результатов е) Гарантирует устойчивость к изменениям распределения данных

Компетенция FC-1: Фронтальные исследования в МО для инфокоммуникаций

Множественный выбор

17. Укажите компоненты self-supervised learning, которые используются для обучения представлений на неразмеченных сетевых данных.

a) Contrastive learning с положительными/отрицательными парами b) Предсказание будущих значений временных рядов (predictive coding) c) Supervised learning с полной разметкой всех образцов d) Transfer learning с предобученными моделями из другой области

18. Определите методы низкоранговой факторизации, которые используются для сжатия весов нейронных сетей в edge-устройствах.

a) SVD (Singular Value Decomposition) для полносвязных слоёв b) Tucker decomposition для свёрточных слоёв c) Pruning для обнуления малозначимых весов d) Quantization для снижения разрядности весов

19. Выберите архитектурные компоненты Transformer, которые обеспечивают эффективную обработку временных рядов сетевого трафика.

a) Multi-head self-attention для захвата долгосрочных зависимостей b) Positional encoding для сохранения временной информации c) Pooling layers для пространственного сжатия признаков d) Batch normalization для стабилизации обучения

20. Укажите методы ускорения обучения глубоких моделей на сетевых данных с ограниченными вычислительными ресурсами.

a) Mixed precision training (FP16/FP32) для ускорения на GPU b) Gradient accumulation для эмуляции большого batch size c) Data augmentation для увеличения разнообразия выборки d) Увеличение batch size до максимально возможного

21. Определите алгоритмы федеративного обучения, которые устойчивы к гетерогенности данных на edge-устройствах.

a) FedProx с проксимальной регуляризацией для стабилизации b) FedAvg с adaptive aggregation по размеру данных c) Простой FedAvg без модификаций для гетерогенных данных d) Централизованное обучение со сбором всех данных

22. Выберите техники защиты приватности в федеративном обучении для телеком-систем.

a) Differential Privacy с добавлением шума к градиентам b) Secure Aggregation через криптографические протоколы c) Простое шифрование канала связи (TLS/SSL) d) Аутентификация edge-устройств через сертификаты

23. Укажите гибридные архитектуры, которые комбинируют классические методы обработки сигналов с нейронными сетями для телеком-задач.

a) Autoencoder с физическими моделями канала в латентном пространстве b) CNN для признаков + SVM/логистическая регрессия для классификации c) Полностью end-to-end нейросеть без априорных знаний d) Простая pipeline классических методов без нейросетей

24. Определите оптимизаторы, которые эффективны для обучения Transformer моделей на последовательностях сетевых данных.

a) AdamW с decoupled weight decay для правильной регуляризации b) Warmup learning rate schedule для стабилизации начала обучения c) Стандартный SGD без momentum и адаптивных шагов d) Постоянный learning rate без scheduling стратегий

Семестр №8

Установление последовательности

25. Расположите этапы построения гибридной модели (autoencoder + классификатор) для анализа спектральных данных SDR в правильном порядке.

a) Предобучение autoencoder на неразмеченных спектральных данных b) Заморозка encoder и добавление классификационных слоёв c) Fine-tuning классификатора на размеченных данных с замороженным encoder d) Опциональный совместный fine-tuning всей модели и валидация

26. Установите последовательность шагов при применении контрастивного обучения для создания эмбедингов сетевых потоков.

a) Определение стратегии создания положительных/отрицательных пар b) Создание encoder сети для отображения в embedding пространство c) Выбор contrastive loss (InfoNCE, triplet loss, NT-Xent) d) Обучение encoder и валидация эмбедингов на downstream задачах

27. Расположите этапы развёртывания оптимизированной модели на edge-устройстве для мониторинга сетевого оборудования в правильном порядке.

a) Выбор техник компрессии (quantization, pruning, distillation) под устройство b) Конвертация в оптимизированный формат (ONNX, TensorRT, TFLite) c) Профилирование латентности, памяти и энергопотребления на устройстве d) Валидация точности и развёртывание с мониторингом в production

28. Установите последовательность действий при настройке федеративного обучения для распределённой сети базовых станций.

a) Проектирование архитектуры с ролями сервера и edge-устройств b) Выбор федеративного алгоритма с учётом гетерогенности данных c) Реализация локального обучения с балансом качества и коммуникаций d) Настройка защиты приватности и мониторинг сходимости

Установление соответствия

29. Установите соответствие между методами self-supervised learning и их механизмами обучения представлений.

Методы:

1. Contrastive Learning
2. Masked Modeling
3. Predictive Coding

Механизмы: a) Различение положительных/отрицательных пар через contrastive loss в embedding пространстве b) Восстановление замаскированных частей входа для изучения контекстных зависимостей c) Предсказание будущих значений из прошлых для извлечения темпоральной структуры d) Обучение на явных метках классов с supervised loss функцией e) Transfer learning с предобученной моделью из другого домена

30. Установите соответствие между методами компрессии нейронных сетей и их воздействием на модель.

Методы:

1. Quantization
2. Pruning
3. Knowledge Distillation

Воздействие: a) Снижение разрядности весов и активаций для уменьшения размера и ускорения b) Обнуление малозначимых весов для создания разреженной структуры c) Обучение компактной модели имитировать выходы большой модели-учителя d) Добавление регуляризации к функции потерь для предотвращения переобучения e) Увеличение глубины модели для повышения выразительности

31. Установите соответствие между архитектурами глубоких сетей и их оптимальными применениями для телеком-данных.

Архитектуры:

1. CNN (Convolutional Neural Networks)
2. RNN/LSTM (Recurrent Neural Networks)
3. Transformer с self-attention

Применения: а) Обработка спектрограмм и пространственно-временных паттернов через локальные фильтры б) Моделирование последовательных зависимостей с долгосрочной памятью с) Параллельное вычисление глобальных зависимостей на длинных последовательностях д) Обработка табличных данных с категориальными и числовыми признаками е) Генерация синтетических данных через adversarial обучение

32. Установите соответствие между алгоритмами федеративного обучения и их ключевыми особенностями.

Алгоритмы:

1. FedAvg (Federated Averaging)
2. FedProx
3. Secure Aggregation

Особенности: а) Взвешенное усреднение локальных моделей по размеру данных после локальных эпох б) Проксимальная регуляризация для ограничения отклонения от глобальной модели с) Криптографические протоколы для приватной агрегации без раскрытия градиентов д) Адаптивное взвешивание устройств по качеству локальных моделей е) Дифференциальная приватность через добавление шума к агрегированным обновлениям

33. Установите соответствие между оптимизаторами и их преимуществами для обучения глубоких моделей на телеком-данных.

Оптимизаторы:

1. AdamW
2. SGD with Momentum
3. AdaGrad

Преимущества: а) Decoupled weight decay с адаптивными шагами для больших моделей б) Momentum для ускорения и лучшего обобщения при правильной настройке с) Индивидуальная адаптация learning rate для разреженных признаков д) Гарантированная глобальная сходимость для невыпуклых функций потерь е) Автоматический выбор оптимального learning rate без настройки

34. Установите соответствие между типами данных в инфокоммуникациях и рекомендуемыми архитектурами для их обработки.

Типы данных:

1. Спектральные данные (спектрограммы)
2. Временные ряды сетевых метрик
3. Сетевые логи и события

Архитектуры: а) CNN (ResNet, EfficientNet) для извлечения пространственно-частотных паттернов б) RNN/LSTM или Transformer для моделирования последовательных зависимостей с) Transformer/BERT для обработки последовательностей дискретных токенов д) GAN для генерации синтетических сетевых данных е) Graph Neural Networks для анализа топологии сети

35. Установите соответствие между вызовами распределённого обучения в телеком-сетях и методами их решения.

Вызовы:

1. Гетерогенность данных (non-IID)
2. Ограниченная пропускная способность каналов
3. Приватность пользовательских данных

Методы решения: а) FedProx, персонализация или кластеризация устройств по схожести данных б) Gradient compression (sparsification, quantization) или low-rank updates в) Differential Privacy, Secure Aggregation или encrypted updates д) Увеличение частоты коммуникации между сервером и устройствами е) Централизованный сбор всех данных для совместного обучения

36. Установите соответствие между информационно-теоретическими концепциями и их применением в ML для телеком-систем.

Концепции:

1. Взаимная информация (Mutual Information)
2. Энтропия
3. Вариационные нижние границы (ELBO)

Применение: а) Максимизация $I(X;Z)$ для информативных эмбеддингов или feature selection б) Минимизация $H(\text{predictions})$ для уверенных предсказаний или максимизация в latent space в) Максимизация ELBO для обучения генеративных моделей с балансом reconstruction и KL д) Минимизация cross-entropy между предсказаниями и целевыми метками е) Вычисление KL-дивергенции между двумя распределениями для регуляризации

37. Установите соответствие между техниками оптимизации вычислительного графа и их эффектами на производительность.

Техники:

1. Operator Fusion
2. Constant Folding
3. Memory Layout Optimization

Эффекты: а) Объединение последовательных операций для уменьшения memory bandwidth б) Предвычисление операций с константами на этапе компиляции в) Переупорядочивание данных для оптимального доступа к памяти на устройстве д) Увеличение batch size для амортизации накладных расходов е) Параллелизация вычислений на множестве GPU

38. Установите соответствие между низкоранговыми методами и их применением к различным типам слоёв.

Методы:

1. SVD для полносвязных слоёв
2. CP-decomposition для свёрточных слоёв
3. LoRA для Transformer слоёв

Применение: а) Разложение матрицы весов $W = U \cdot \Sigma \cdot V^T$ с аппроксимацией через ранг r б) Разложение 4D тензора ядер на сумму ранг-1 компонент в) Добавление низкоранговых обновлений $\Delta W = BA$ к замороженным весам д) Pruning малозначимых весов на основе величины или градиентов е) Quantization весов с FP32 до INT8 для уменьшения размера

39. Установите соответствие между типами атак на федеративные системы и методами защиты.

Типы атак:

1. Model Poisoning Attack

2. Gradient Leakage Attack
3. Data Poisoning Attack

Методы защиты: а) Robust aggregation (median, Krum) или Byzantine-resilient алгоритмы b) Secure Aggregation или Differential Privacy с зашумлением градиентов c) Anomaly detection обновлений или certified defenses против backdoor d) Увеличение частоты коммуникации для быстрого обнаружения атак e) Централизованная валидация данных на сервере перед агрегацией

40. Установите соответствие между метриками производительности моделей на edge-устройствах и их важностью для телеком-приложений.

Метрики:

1. Latency (задержка inference)
2. Memory Footprint (потребление памяти)
3. Energy Consumption (энергопотребление)

Важность: а) Время отклика для real-time приложений (network slicing, QoS) b) Размер модели и runtime память для устройств с ограниченной RAM c) Батарея и тепловыделение для battery-powered устройств d) Throughput (количество предсказаний в секунду) для batch processing e) Accuracy (точность предсказаний) относительно baseline модели

Перечень вопросов для проведения промежуточной аттестации

Перечень вопросов для проведения зачета	
4.	Объясните принципы работы архитектуры Transformer и механизм внимания (Attention).
5.	Сравните архитектуры RNN, LSTM и GRU по эффективности при анализе временных рядов.
6.	Опишите устройство и функции autoencoder'a. В каких задачах инфокоммуникаций он применяется?
7.	Приведите примеры гибридных архитектур нейросетей и опишите их преимущества.
8.	Что такое contrastive learning и почему этот подход эффективен при недостатке размеченных данных?
9.	Охарактеризуйте методы сжатия нейросетей (quantization, pruning, knowledge distillation).
10.	Объясните назначение low-rank factorization в ускорении обучения глубоких моделей.
11.	Опишите назначение и особенности оптимизаторов AdamW, Lookahead и Lion.
12.	Что означает процедура gradient clipping и зачем она используется?
13.	Объясните принципы распределённого обучения и основные проблемы синхронизации.
Перечень вопросов для проведения БРК	

14. Что такое федеративное обучение (Federated Learning) и какие преимущества оно даёт для IoT-сетей?
15. Опишите роль Secure Aggregation и методов защиты данных в федеративном обучении.
16. Объясните, в чём заключается концепция дифференциальной приватности при обучении моделей.
17. Что означает термин MLOps и какие стадии жизненного цикла ML-моделей он включает?
18. Назовите ключевые компоненты экосистемы MLflow и Kubeflow Pipelines.
19. В чём заключается понятие technical debt в системах машинного обучения?
20. Объясните назначение и принципы проведения A/B-тестирования в ML-проектах.
21. Какие метрики используются для оценки качества моделей в задачах инфокоммуникаций (QoS, QoE,

ROC-AUC и др.)?

22. Что подразумевается под Edge AI, и какие преимущества оно даёт при развёртывании ML-моделей в телеком-средах?
23. Приведите примеры применения Graph Neural Networks в анализе сетевой топологии и маршрутизации.