

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Максимов Алексей Борисович

Должность: директор департамента по образовательной политике

Дата подписания: 05.09.2026 14:03:59

Уникальный программный ключ:

8db180d1a3f02ac9e60521a567274273e1b01ca

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДАЮ

Декан факультета

«Информационных технологий»

 / Д.Г. Демидов /

« 26 » февраля 2026 г.

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Инструментальные средства технологий искусственного интеллекта»

Направление подготовки

**10.03.01 «Информационная безопасность»**

Профиль

**«Безопасность компьютерных систем»**

Квалификация

**Бакалавр**

Формы обучения

**Очная**

Москва, 2026 г.

**Разработчик(и):**

Доцент, к.т.н., доцент



/И.В. Калущий/

**Согласовано:**

Заведующий кафедрой «Информационная безопасность»



И.В.Калущий

## Содержание

|      |                                                                                    |    |
|------|------------------------------------------------------------------------------------|----|
| 1.   | Цели, задачи и планируемые результаты обучения по дисциплине .....                 | 4  |
| 2.   | Цели, задачи и планируемые результаты обучения по дисциплине .....                 | 5  |
| 3.   | Структура и содержание дисциплины.....                                             | 5  |
| 3.1. | Виды учебной работы и трудоемкость .....                                           | 5  |
| 3.2. | Тематический план изучения дисциплины .....                                        | 5  |
| 3.3. | Содержание дисциплины .....                                                        | 6  |
| 3.4. | Тематика семинарских/практических и лабораторных занятий .....                     | 8  |
| 3.5. | Тематика курсовых проектов (курсовых работ) .....                                  | 8  |
| 4.   | Учебно-методическое и информационное обеспечение.....                              | 9  |
| 4.1. | Нормативные документы и ГОСТы .....                                                | 9  |
| 4.2. | Основная литература .....                                                          | 9  |
| 4.3. | Дополнительная литература .....                                                    | 10 |
| 4.4. | Электронные образовательные ресурсы.....                                           | 10 |
| 4.5. | Лицензионное и свободно распространяемое программное обеспечение .....             | 10 |
| 4.6. | Современные профессиональные базы данных и информационные справочные системы ..... | 10 |
| 5.   | Материально-техническое обеспечение .....                                          | 11 |
| 6.   | Методические рекомендации .....                                                    | 11 |
| 6.1. | Методические рекомендации для преподавателя по организации обучения .....          | 11 |
| 6.2. | Методические указания для обучающихся по освоению дисциплины .....                 | 11 |
| 7.   | Фонд оценочных средств .....                                                       | 12 |
| 7.1. | Методы контроля и оценивания результатов обучения.....                             | 12 |
| 7.2. | Шкала и критерии оценивания результатов обучения.....                              | 12 |
| 7.3. | Оценочные средства .....                                                           | 13 |

## 1. Цели, задачи и планируемые результаты обучения по дисциплине

К основным **целям** освоения дисциплины «Инструментальные средства технологий искусственного интеллекта» следует отнести:

- изучение современного стека инструментальных средств искусственного интеллекта и их применения на всех этапах разработки моделей
- формирование практических навыков работы с основными библиотеками и фреймворками машинного обучения и глубокого обучения
- освоение инструментов предобработки данных, работы с большими датасетами и векторными хранилищами
- приобретение навыков дообучения, квантизации и локального запуска больших языковых моделей
- изучение средств компьютерного зрения, генеративных моделей и мультимодальных систем
- формирование компетенций в области MLOps: трекинг экспериментов, версионирование, воспроизводимость и мониторинг
- освоение методов деплоя моделей в продакшн и создания демонстрационных интерфейсов
- развитие умений оценки и выбора инструментальных средств по критериям производительности, удобства и совместимости
- подготовка специалистов, способных самостоятельно строить end-to-end пайплайны искусственного интеллекта.

К основным **задачам** освоения дисциплины «Инструментальные средства технологий искусственного интеллекта» следует отнести:

- изучение современных методов и технологий машинного обучения и искусственного интеллекта для решения прикладных задач
- формирование навыков разработки, обучения и оптимизации моделей машинного обучения
- развитие компетенций по выбору, оценке и внедрению алгоритмов искусственного интеллекта в профессиональной деятельности
- подготовка специалистов, способных применять технологии искусственного интеллекта для автоматизации процессов и повышения эффективности цифровых решений.

Обучение по дисциплине «Инструментальные средства технологий искусственного интеллекта» направлено на формирование у обучающихся следующих компетенций:

| Код и наименование компетенций                                                                                                                                                     | Индикаторы достижения компетенции                                                                                                                                                                                                            |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ОПК-8. Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности | <p>знать:</p> <ul style="list-style-type: none"> <li>• необходимые нормативно-методические документы.</li> </ul> <p>уметь:</p> <ul style="list-style-type: none"> <li>• составлять аналитические обзоры по вопросам использования</li> </ul> |

|  |                                                                                                                                                                                                                             |
|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p>технологий искусственного интеллекта;</p> <p>владеть:</p> <ul style="list-style-type: none"> <li>• навыками выбора и обоснования критериев эффективности функционирования выбранных инструментальных средств.</li> </ul> |
|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## 2. Цели, задачи и планируемые результаты обучения по дисциплине

Дисциплина «Инструментальные средства технологий искусственного интеллекта» относится к числу учебных дисциплин блока 1 обязательной части (Б1.1) основной образовательной программы (Б1.1.30).

Дисциплина логически и содержательно-методически взаимосвязана со следующими дисциплинами и практиками ООП: «Программно-аппаратные средства защиты информации» «Основы проектирования информационных систем».

## 3. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 часа).

### 3.1. Виды учебной работы и трудоемкость (по формам обучения)

#### 3.1.1 Очная форма обучения

| №<br>п/п | Вид учебной работы               | Количество<br>часов | Семестры |                    |
|----------|----------------------------------|---------------------|----------|--------------------|
|          |                                  |                     | Семестр  | Неделя<br>семестра |
| <b>1</b> | <b>Аудиторные занятия</b>        | <b>72</b>           | <b>6</b> |                    |
|          | В том числе:                     |                     |          |                    |
| 1.1      | Лекции                           | 18                  | 6        |                    |
| 1.2      | Семинарские/практические занятия | -                   |          |                    |
| 1.3      | Лабораторные занятия             | <b>54</b>           | 6        |                    |
| <b>2</b> | <b>Самостоятельная работа</b>    | <b>72</b>           | 6        |                    |
| <b>3</b> | <b>Промежуточная аттестация</b>  |                     |          |                    |
|          | Экзамен                          |                     | 6        | По расписанию      |
|          | <b>Итого</b>                     | <b>144</b>          |          |                    |

### 3.2. Тематический план изучения дисциплины (по формам обучения)

#### 3.2.1 Очная форма обучения

| № | Разделы/темы | Трудоемкость, час |
|---|--------------|-------------------|
|---|--------------|-------------------|

| п/<br>п      | дисциплины                                                                                                           | Всего      | Аудиторная работа |                                  |                      |                         | Самостоятельная работа |
|--------------|----------------------------------------------------------------------------------------------------------------------|------------|-------------------|----------------------------------|----------------------|-------------------------|------------------------|
|              |                                                                                                                      |            | Лекции            | Семинарские/практические занятия | Лабораторные занятия | Практическая подготовка |                        |
| 1            | Раздел 1. Основы современного стека инструментальных средств ИИ                                                      |            |                   |                                  |                      |                         |                        |
| 1.1          | Тема 1. Обзор ландшафта ИИ-инструментов. Классификация по этапам жизненного цикла моделей                            | 12         | 2                 |                                  | 4                    |                         | 6                      |
| 1.2          | Тема 2. Базовые библиотеки данных и классический ML (NumPy, Pandas, Polars, Scikit-learn, XGBoost/LightGBM/CatBoost) | 12         | 2                 |                                  | 4                    |                         | 6                      |
| 1.2          | Тема 3. Фреймворки глубокого обучения и экосистема Hugging Face (PyTorch, TensorFlow/Keras, Transformers, PEFT)      | 12         | 2                 |                                  | 4                    |                         | 6                      |
| 2            | Раздел 2. Инструменты для больших моделей и прикладных задач                                                         |            |                   |                                  |                      |                         |                        |
| 2.1          | Тема 1. Работа с большими языковыми моделями (LoRA/QLoRA, vLLM, Ollama, LangChain, LlamaIndex, RAG)                  | 18         | 2                 |                                  | 7                    |                         | 9                      |
| 2.2          | Тема 2. Компьютерное зрение и генеративные модели (OpenCV, torchvision, YOLO, Diffusers, Stable Diffusion)           | 18         | 2                 |                                  | 7                    |                         | 9                      |
| 2.3          | Тема 3. Векторные базы данных и демонстрационные интерфейсы (FAISS, Chroma, Gradio, Streamlit, Chainlit)             | 18         | 2                 |                                  | 7                    |                         | 9                      |
| 3            | Раздел 3. MLOps, деплой и готовые продакшн решения                                                                   |            |                   |                                  |                      |                         |                        |
| 3.1          | Тема 1. Трекинг экспериментов и воспроизводимость (MLflow, Weights & Biases, DVC, Hydra)                             | 18         | 2                 |                                  | 7                    |                         | 9                      |
| 3.2          | Тема 2. Деплой, оптимизация и мониторинг моделей (FastAPI, BentoML, Docker, Triton, квантизация, Prometheus)         | 18         | 2                 |                                  | 7                    |                         | 9                      |
| 3.3          | Тема 3. Построение end-to-end production-пайплайнов ИИ                                                               | 18         | 2                 |                                  | 7                    |                         | 9                      |
| <b>Итого</b> |                                                                                                                      | <b>144</b> | <b>18</b>         |                                  | <b>54</b>            |                         | <b>72</b>              |

### 3.3. Содержание дисциплины

**Раздел 1.** Основы современного стека инструментальных средств ИИ

**Тема 1.1.** Обзор ландшафта ИИ-инструментов. Классификация по этапам жизненного цикла моделей

Обзор эволюции инструментального стека ИИ в 2025–2030 годах. Классификация инструментов по этапам: сбор и подготовка данных, обучение и эксперименты, дообучение и fine-tuning, инференс и деплой, мониторинг и поддержка. Основные тенденции: open-weight модели, эффективные архитектуры, локальный запуск, MLOps/LLMOps.

### **Тема 1.2.** Базовые библиотеки данных и классический ML

Работа с данными: NumPy, Pandas, Polars. Классическое машинное обучение: Scikit-learn (пайплайны, метрики, кросс-валидация), градиентный бустинг (XGBoost, LightGBM, CatBoost). Feature engineering, обработка категориальных признаков, борьба с дисбалансом классов, подбор гиперпараметров.

### **Тема 1.3.** Фреймворки глубокого обучения и экосистема Hugging Face

Основы PyTorch и TensorFlow/Keras: тензоры, автодифференцирование, обучение моделей. Экосистема Hugging Face: Transformers (модели, токенизаторы, тренеры), Datasets, Accelerate, PEFT (LoRA, QLoRA, adapters), Hub. Совместная работа с PyTorch и Hugging Face.

## **Раздел 2.** Инструменты для больших моделей и прикладных задач

### **Тема 2.1.** Работа с большими языковыми моделями

Эффективное дообучение и инференс LLM: LoRA/QLoRA, PEFT, vLLM, Ollama, LM Studio. Инструменты для создания приложений: LangChain, LlamaIndex, Haystack. Retrieval-Augmented Generation (RAG): векторный поиск, чанкинг, reranking. Локальный и облачный запуск открытых моделей.

### **Тема 2.2.** Компьютерное зрение и генеративные модели

Библиотеки компьютерного зрения: OpenCV, torchvision, Albumentations. Современные модели детекции и сегментации: YOLOv8–v11, Detectron2. Генеративные модели: Diffusers (Stable Diffusion и производные), ControlNet, ComfyUI. Основы fine-tuning и инференса генеративных моделей.

### **Тема 2.3.** Векторные базы данных и демонстрационные интерфейсы

Векторные хранилища и поиск по сходству: FAISS, Chroma, Pinecone, Weaviate. Создание пользовательских интерфейсов и демо: Gradio, Streamlit, Chainlit. Быстрое прототипирование приложений на базе LLM и мультимодальных моделей.

## **Раздел 3.** MLOps, деплой и готовые продакшн решения

### **Тема 3.1.** Трекинг экспериментов и воспроизводимость

Инструменты трекинга и экспериментов: MLflow, Weights & Biases. Версионирование данных и моделей: DVC. Управление конфигурациями и воспроизводимостью: Hydra, Git + DVC. Логирование метрик, артефактов и сравнение запусков.

### **Тема 3.2.** Деплой, оптимизация и мониторинг моделей

Сервировка моделей: FastAPI, BentoML, TorchServe, Triton Inference Server. Оптимизация инференса: квантизация, ONNX Runtime, Torch.compile. Контейнеризация и оркестрация: Docker basics. Мониторинг: Prometheus + Grafana, drift detection, логирование предсказаний.

### **Тема 3.3.** Построение end-to-end production-пайплайнов ИИ

Интеграция всех этапов: от сбора данных до деплоя и мониторинга. Примеры production-пайплайнов для классических моделей, LLM и мультимодальных систем. Автоматизация переобучения, A/B-тестирование, CI/CD для ML. Лучшие практики построения надёжных и масштабируемых ИИ-решений.

### 3.4. Тематика семинарских/практических и лабораторных занятий

#### 3.4.1 Семинарские/практические занятия

*Не предусмотрены программой.*

#### 3.4.2 Лабораторные занятия

Лабораторная работа 1.1: провести обзор и классификацию инструментов ии по этапам жизненного цикла моделей. Проанализировать документацию 5–7 инструментов (например, scikit-learn, pytorch, mlflow) и создать сравнительную таблицу по критериям удобства, скорости и совместимости.

Лабораторная работа 1.2: реализовать предобработку данных и классическую модель ml с использованием numpy, pandas, polars и scikit-learn. Применить на датасете iris или mnist, обработать дисбаланс, провести feature engineering и подбор гиперпараметров с gridsearchcv.

Лабораторная работа 1.3: создать и обучить простую нейросеть в pytorch или tensorflow/keras. Дообучить модель из hugging face transformers на датасете imdb для классификации текстов, оценить метрики и визуализировать loss/accuracy.

Лабораторная работа 2.1: дообучить llm с lora/qlora с использованием peft и vllm. Применить на датасете squad для question answering, реализовать rag с langchain или llamaindex, оценить точность инференса на ollama.

Лабораторная работа 2.2: реализовать модель компьютерного зрения с openCV и torchvision. Дообучить yolo для детекции объектов на датасете coco subset или pascal voc, сравнить с detectron2. Сгенерировать изображения с diffusers и stable diffusion.

Лабораторная работа 2.3: настроить векторную базу данных с faiss или chroma. Создать демонстрационный интерфейс на gradio или streamlit для поиска по сходству в текстовом датасете (например, wikipedia snippets), интегрировать с chainlit для чат-бота на базе llm.

Лабораторная работа 3.1: настроить трекинг экспериментов в mlflow или weights & biases. Версионировать данные и модели с dvc, провести несколько запусков модели на датасете cifar-10 с hydra для конфигураций, сравнить метрики.

Лабораторная работа 3.2: задеплоить модель с fastapi или bentoml. Оптимизировать инференс с квантизацией и onnx runtime, контейнеризировать с docker, настроить мониторинг с prometheus и grafana, протестировать на локальном сервере.

Лабораторная работа 3.3: построить end-to-end пайплайн от данных до деплоя. Интегрировать предобработку, обучение (pytorch), rag (langchain) и мониторинг (mlflow) для задачи классификации изображений или текстов, провести a/b-тестирование моделей.

### 3.5. Тематика курсовых проектов (курсовых работ)

Темы курсовых работ:

1. Разработка и оптимизация градиентного бустинга (XGBoost, LightGBM, CatBoost) для табличных задач
2. Дообучение предобученных моделей Hugging Face Transformers на русскоязычных текстах

3. Реализация RAG-системы на базе LangChain / LlamaIndex с векторной базой Chroma или FAISS
4. Fine-tuning больших языковых моделей с LoRA/QLoRA для специализированных задач
5. Обнаружение и классификация объектов на изображениях с использованием YOLOv11 и Detectron2
6. Генерация изображений по текстовым описаниям с Stable Diffusion и ControlNet
7. Создание демонстрационного веб-интерфейса для LLM-приложений (Gradio / Streamlit / Chainlit)
8. Построение воспроизводимого ML-эксперимента с MLflow, Weights & Biases и DVC
9. Деплой и оптимизация модели машинного обучения в production (FastAPI, BentoML, Docker, Triton)
10. Квантизация и ускорение инференса больших моделей (ONNX Runtime, vLLM, Torch.compile)
11. Мониторинг и обнаружение data/model drift в production-пайплайнах ИИ
12. Построение end-to-end production-пайплайна от данных до деплоя и мониторинга
13. Сравнение локального и облачного инференса открытых LLM (Ollama vs API-провайдеры)
14. Реализация мультимодальной системы (текст + изображение) на базе CLIP / LLaVA

## **4. Учебно-методическое и информационное обеспечение**

### **4.1. Нормативные документы и ГОСТы**

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»: Текст: электронный // КонсультантПлюс. — URL: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_61801/](http://www.consultant.ru/document/cons_doc_LAW_61801/) (дата обращения: 23.02.2030).
2. Приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований к защите информации, содержащейся в государственных информационных системах, информационных системах государственных органов, органов местного самоуправления, государственных и муниципальных учреждений, иных организаций, создаваемых для выполнения государственных и муниципальных функций» (вступ. в силу 01.03.2030): Текст: электронный // Официальный сайт ФСТЭК России. — URL: <https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/trebovaniya-utverzhdeny-prikazom-fstek-rossii-ot-11-aprelya-2025-g-n-117> (дата обращения: 23.02.2030).

### **4.2. Основная 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> (дата обращения: 23.02.2030).
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 978-5-534-14916-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/519916> (дата обращения: 23.02.2030).
3. Иванов, В. М. Интеллектуальные системы : учебное пособие для вузов / В. М. Иванов ; под науч. ред. А. Н. Сесекина. — Москва : Издательство Юрайт, 2022. — 91 с. —

(Высшее образование). — ISBN 978-5-534-00551-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/492094> (дата обращения: 23.02.2030).

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 978-5-534-07198-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/494205> (дата обращения: 23.02.2030).

### **4.3. 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> (дата обращения: 23.02.2030).

2. Анализ данных : учебник для вузов / В. С. Мхитарян [и др.] ; под ред. 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> (дата обращения: 23.02.2030).

### **4.4. Электронные образовательные ресурсы**

Электронный образовательный ресурс в разработке

### **4.5 Лицензионное и свободно распространяемое программное обеспечение**

1. Операционная система Microsoft Windows от 7 версии и выше; Microsoft Office или Open Office, браузер (Firefox/Google Chrome /Explorer).
2. Python 3.10–3.12 (устанавливается через официальный сайт [python.org](https://python.org) или через Anaconda/Miniconda)
3. Anaconda / Miniconda
4. Git (для скачивания датасетов и репозиторий с GitHub)
5. Visual Studio Code (бесплатный редактор кода с расширениями Python, Jupyter, Git) или PyCharm Community Edition (бесплатная версия)

### **4.6 Современные профессиональные базы данных и информационные справочные системы**

1. eLIBRARY.RU: Научная электронная библиотека: сайт. - Москва, 2000 -. - URL: <https://www.elibrary.ru> (дата обращения: 23.02.2030). – Текст: электронный.

2. ЛАНЬ: электронно-библиотечная система: сайт. – Санкт-Петербург, 2010 -. - URL: <https://e.lanbook.com> (дата обращения: 23.02.2030). - Текст: электронный.

3. ФСТЭК России: Государственный реестр сертифицированных средств защиты информации. – Москва, 2014. – URL: <https://fstec.ru/tekhnicheskaya-zashchita>

informatzii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii (дата обращения: 23.02.2030). -  
Текст: электронный.

## **5. Материально-техническое обеспечение**

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, ноутбук, экран или интерактивная доска) – 1 комплект.

Для проведения практических занятий необходимо наличие компьютерных классов, оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

## **6. Методические рекомендации**

### **6.1 Методические рекомендации для преподавателя по организации обучения**

При подготовке к лабораторным работам следует предварительно проработать теоретический материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия.

При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

При проверке работ и отчетов следует учитывать правильность выполнения лабораторных работ на всех этапах.

### **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 *лекции*.

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

Лабораторные работы проводятся по наиболее важным темам дисциплины. Осуществляется закрепление знаний, полученных студентами на лекциях и в процессе самостоятельной работы. Особое внимание обращается на развитие умений и навыков установления связи положений теории с профессиональной деятельностью будущего специалиста по ИБ. Лабораторные работы проводятся по теоретическим и проблемным вопросам ИБ. Лабораторные работы предполагает творческие дискуссии, активный обмен мнениями по поставленным вопросам, заслушивание и обсуждение докладов по предложенным преподавателем темам.

Важным обстоятельством является привлечение внимания студентов к обсуждаемой проблеме, стимулирование интереса к ней и организация активного обсуждения, как структуры проблемы, так и составляющих ее наиболее актуальных тем. Для повышения эффективности проведения занятия требуется предварительная подготовка всех его участников. В этой связи рекомендуется заблаговременно (не менее, чем за неделю) оповестить студентов о теме занятия, дать перечень литературы по теме, назначить из числа студентов докладчиков и содокладчиков.

При проведении лабораторной работы преподаватель выполняет, в основном, функции ведущего - следит за регламентом времени, помогает уточнить формулировки, обобщает

результаты дискуссии, подводит итог занятию в целом. При высоком уровне подготовки студенческой группы отдельные функции ведущего можно поручить одному из студентов. В случае необходимости, преподаватель оказывает ему поддержку, а при подведении итогов - дает оценку работе ведущего.

Активная работа студента на лабораторной работе учитывается при определении итоговой оценки его знаний по дисциплине на экзамене.

Самостоятельная работа студентов предполагает изучение теоретического и практического материала по актуальным вопросам дисциплины. Рекомендуется самостоятельное изучение учебной и научной литературы, использование справочной литературы и др.

При выдаче заданий на самостоятельную работу используется дифференцированный подход к студентам. Перед выполнением студентами самостоятельной внеаудиторной работы преподаватель проводит инструктаж по выполнению задания, который включает: цель задания, его содержание, сроки выполнения, ориентировочный объем работы, основные требования к результатам работы, критерии оценки. В процессе инструктажа преподаватель предупреждает студентов о возможных типичных ошибках, встречающихся при выполнении задания. Инструктаж проводится преподавателем за счет объема времени, отведенного на изучение дисциплины.

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на экзамене в письменной (устной) форме.

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 практических занятиях, промежуточный контроль осуществляется на экзамене 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**

### **7.1 Методы контроля и оценивания результатов обучения**

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

- проведение лабораторных работ (практических занятий с использованием спецтехники) и их защита;
- самостоятельная подготовка и проведение презентаций по темам дисциплины;
- экзамен.

### **7.2 Шкала и критерии оценивания результатов обучения**

**Форма промежуточной аттестации: экзамен.**

По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

| <b>Шкала<br/>оценивания</b> | <b>Описание</b>                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Отлично                     | 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                      | 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           | 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 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.                           |

### 7.3 Оценочные средства

#### 7.3.1 Текущий контроль

Оценочные средства для текущей аттестации

- Защита отчетов о выполнении лабораторных работ

#### 7.3.2 Промежуточная аттестация

Оценочные средства для промежуточной аттестации

- Экзамен

Список вопросов для экзамена по дисциплине:

1. Какие основные категории инструментальных средств ИИ выделяют по этапам жизненного цикла моделей?

2. Перечислите ключевые тенденции развития инструментального стека ИИ на 2025–2030 годы.
3. В чём основные преимущества и недостатки библиотек Pandas, Polars и Dask при обработке больших данных?
4. Сравните PyTorch и TensorFlow/Keras по удобству разработки, скорости обучения и экосистеме в 2025–2030 годах.
5. Что включает в себя экосистема Hugging Face? Назовите её основные компоненты и их назначение.
6. Что такое LoRA и QLoRA? Когда их используют вместо полного дообучения большой модели?
7. Перечислите популярные инструменты для локального запуска и инференса LLM в 2025–2030 годах и их ключевые особенности.
8. В чём разница между LangChain и LlamaIndex? Для каких задач каждый из них предпочтительнее?
9. Опишите принцип работы Retrieval-Augmented Generation (RAG). Какие инструменты нужны для реализации RAG-пайплайна?
10. Какие современные модели и библиотеки используются для object detection в 2025–2030 годах? Сравните YOLOv11 и Detectron2.
11. Назовите основные компоненты экосистемы Stable Diffusion и их назначение.
12. Перечислите популярные векторные базы данных для задач семантического поиска и RAG. В чём их основные различия?
13. Какие инструменты трекинга экспериментов наиболее распространены? Сравните MLflow и Weights & Biases.
14. Что такое DVC и как оно помогает обеспечить воспроизводимость ML-экспериментов?
15. Перечислите основные способы деплоя моделей в production и их ключевые различия.
16. Какие методы оптимизации инференса больших моделей наиболее актуальны в 2025–2030 годах?
17. Как организовать мониторинг модели в production? Какие метрики и инструменты используются?
18. Что такое data drift и concept drift? Как их обнаруживать и реагировать?
19. Опишите типичный end-to-end production-пайплайн ИИ-решения от данных до деплоя и мониторинга.
20. Какие лучшие практики CI/CD применяются в ML-проектах в 2025–2030 годах?
21. Сравните скорость и качество инференса открытых LLM при локальном запуске (Llama 3.1, Mistral, Qwen2, Gemma-2).
22. Как быстро создать демонстрационный интерфейс для LLM-приложения? Сравните Gradio, Streamlit и Chainlit.
23. В каких случаях предпочтительнее локальный инференс LLM, а в каких облачные API?
24. Как интегрировать векторную базу данных, LLM и пользовательский интерфейс в единую RAG-систему?
25. Назовите типичные ошибки при переходе модели из Jupyter в production и способы их избежать с помощью современного стека инструментов.