

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ**

УТВЕРЖДАЮ

Директор/Декан
факультета цифровых технологий
Шлаев Дмитрий Валерьевич

«__» _____ 20__ г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ (ОЦЕНОЧНЫХ МАТЕРИАЛОВ)

Б1.О.12 Проектирование автономных ИИ-агентов

09.04.03 Прикладная информатика

Искусственный интеллект в кибербезопасности

магистр

очная

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих компетенций ОП ВО и овладение следующими результатами обучения по дисциплине:

Код и наименование компетенции	Код и наименование индикатора достижения	Перечень планируемых результатов обучения по дисциплине
ОПК-2 Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач	ОПК-2.1 Понимает методологические основы современных информационных и интеллектуальных технологий для решения профессиональных задач	знает методологические основы современных информационно-коммуникационных и интеллектуальных технологий для решения профессиональных задач
		умеет применять методологические основы современных информационно-коммуникационных и интеллектуальных технологий для решения профессиональных задач
		владеет навыками основами современных информационно-коммуникационных и интеллектуальных технологий для решения профессиональных задач
ОПК-2 Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач	ОПК-2.2 Обосновывает выбор современных информационных и интеллектуальных технологий, методы разработки программных средств, для решения профессиональных задач	знает современные информационнокоммуникационные и интеллектуальные технологии, методы разработки программных средств для решения профессиональных задач
		умеет обосновано выбирать современные информационнокоммуникационные и интеллектуальные технологии, методы разработки программных средств для решения профессиональных задач
		владеет навыками навыками обоснования выбора современных информационнокоммуникационных и интеллектуальных технологий, методы разработки программных средств, для решения профессиональных задач
ОПК-2 Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных	ОПК-2.3 Разрабатывает оригинальные алгоритмы и программные средства, в том числе с использованием	знает алгоритмы и программные средства, в том числе с использованием интеллектуальных технологий, для решения профессиональных задач
		умеет разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием интеллектуальных технологий, для решения профессиональных задач

интеллектуальных технологий, для решения профессиональных задач	м интеллектуальных технологий, для решения профессиональных задач	владеет навыками навыками разработки оригинальных алгоритмов и программных средств с использованием интеллектуальных технологий для решения профессиональных задач
ПК-1 Способен разрабатывать, модернизировать и сопровождать программное обеспечение информационных систем	ПК-1.1 Разрабатывает программный код на современных языках программирования, применяя методы и приёмы формализации и алгоритмизации поставленных задач	знает современные языки программирования, методы и приемы формализации и алгоритмизации поставленных задач
		умеет разрабатывать программный код на современных языках программирования, применяя методы и приемы формализации и алгоритмизации поставленных задач
		владеет навыками навыками разработки на современных языках программирования с применением методов и приемов формализации и алгоритмизации поставленных задач
ПК-3 Способен применять методы машинного обучения и интеллекта для решения задач кибербезопасности	ПК-3.1 Проводит анализ безопасности компьютерных систем с использованием методов машинного обучения для выявления уязвимостей и оценки рисков	знает техническую документацию на компьютерное программное обеспечение с использованием существующих стандартов
		умеет разрабатывать техническую документацию на компьютерное программное обеспечение с использованием существующих стандартов
		владеет навыками навыками разработки технической документации на компьютерное программное обеспечение с использованием существующих стандартов

2. Перечень оценочных средств по дисциплине

№	Наименование раздела/темы	Семестр	Код индикаторов достижения компетенций	Оценочное средство проверки результатов достижения индикаторов компетенций
1.	1 раздел. Проектирование автономных ИИ-агентов			
1.1.	Введение в архитектуру автономных ИИ-агентов	3	ОПК-2.1, ОПК-2.2, ОПК-2.3, ПК-1.1, ПК-3.1	Устный опрос

1.2.	Анатомия агента: память, инструменты и ReAct	3	ОПК-2.1, ОПК-2.2, ОПК-2.3, ПК-1.1, ПК-3.1	Тест
1.3.	Планирование и мультиагентные системы	3	ОПК-2.1, ОПК-2.2, ОПК-2.3, ПК-1.1, ПК-3.1	Устный опрос
1.4.	Агенты в недетерминированных средах	3	ОПК-2.1, ОПК-2.2, ОПК-2.3, ПК-1.1, ПК-3.1	Устный опрос
1.5.	Оценка, безопасность и наблюдаемость	3	ОПК-2.1, ОПК-2.2, ОПК-2.3, ПК-1.1, ПК-3.1	Тест
1.6.	Проектный практикум и управленческие аспекты	3	ОПК-2.1, ОПК-2.2, ОПК-2.3, ПК-1.1, ПК-3.1	Устный опрос
	Промежуточная аттестация			Эк

3. Оценочные средства (оценочные материалы)

Примерный перечень оценочных средств для текущего контроля успеваемости и промежуточной аттестации

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде (Оценочные материалы)
Текущий контроль			
Для оценки знаний			
1	Устный опрос	Средство контроля знаний студентов, способствующее установлению непосредственного контакта между преподавателем и студентом, в процессе которого преподаватель получает широкие возможности для изучения индивидуальных особенностей усвоения студентами учебного материала.	Перечень вопросов для устного опроса
2	Тест	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося.	Фонд тестовых заданий
Для оценки умений			
Для оценки навыков			
Промежуточная аттестация			

3	Курсовые работы (проектов)	Вид самостоятельной письменной работы, направленный на творческое освоение общепрофессиональных и профильных профессиональных дисциплин (модулей) и выработку соответствующих профессиональных компетенций. При написании курсовой работы студент должен полностью раскрыть выбранную тему, соблюсти логику изложения материала, показать умение делать обобщения и выводы.	Перечень тем курсовых работ (проектов)
4	Экзамен	Средство контроля усвоения учебного материала и формирования компетенций, организованное в виде беседы по билетам с целью проверки степени и качества усвоения изучаемого материала, определить необходимость введения изменений в содержание и методы обучения.	Комплект экзаменационных билетов

4. Примерный фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю) "Проектирование автономных ИИ-агентов"

Примерные оценочные материалы для текущего контроля успеваемости

ЗНАНИЯ

1. Вы выкатываете агента в контейнерах. Как безопаснее всего передать ключи моделей и внешних API?

- A) Защитить в исходный код и собрать образ
- B) Передать ключи в пользовательском запросе
- C) Хранить в секрет-менеджере/CI и инжектировать как переменные окружения при деплое
- D) Положить .env в репозиторий

Ответ: C

2. Инструмент «генерация отчёта» занимает 2–3 минуты. Как спроектировать вызов, чтобы не блокировать агента и UI?

- A) Ставить timeout=0
- B) Возвращать job_id и статус; опрос/вебхуки для готовности результата
- C) Повысить температуру
- D) Запретить инструмент

Ответ: B

3. Подключаете send_payment. Что из ниже — две обязательные меры на стороне сервера?

- A) Валидация параметров и бизнес-правил на бэкенде (сумма ≥ 0 , валюта и т. п.)

- В) Логировать токены в явном виде для отладки
- С) Ролевой контроль/allow-list для вызова инструмента (RBAC/ABAC)
- Д Отключить аудит, чтобы ускорить ответы

Ответ: А, С

4. Нужно понять, где теряется производительность. Что вы внедрите?

- А) Структурированные логи с trace-id на шаги: промпт → tool_call → tool_result
- В) Метрики латентности и частоты ошибок по каждому инструменту
- С) Логи только на уровне DEBUG без id
- Д) Скриншоты UI

Ответ: А,В

5. Как застраховаться от регрессий качества до выката?

- А) Регрессионные eval-наборы (golden prompts) + автопроверка
- В) Реплей логов с моками инструментов в CI/CD
- С) Ручной просмотр пары диалогов
- Д) Увеличить окно контекста «на всякий случай»

Ответ: А,В

УМЕНИЯ

6. Соотнесите элементы и описания:

- 1. Векторное хранилище (FAISS/pgvector/...)
- 2. JSON Schema для инструментов
- 3. Поточная выдача (SSE/WebSocket)
- 4. Экспоненциальный бэкофф с джиттером
- А) Инкрементальная доставка токенов пользователю
- В) Валидация и строгая типизация параметров вызова
- С) Устойчивость к временным сбоям/лимитах API
- Д) Поиск ближайших векторов для RAG

Правильный порядок: 1–D, 2–B, 3–A, 4–C.

7. Расставьте шаги:

- А) Описать JSON-схему параметров и зарегистрировать инструмент в рантайме агента
- В) Написать end-point сервера с валидацией/идемпотентностью
- С) Добавить в системный промпт правила вызова и негативные примеры
- Д) Прогнать сквозные тесты/эвал с моками API

Ответ: В → А → С → D

8. Верно ли утверждение: если переменная API_KEY не задана, скрипт упадёт с KeyError и строку missing не напечатает

```
import os
print(os.environ["API_KEY"])
print("missing")
```

Ответ: Верно

9. Верно ли, что программа выведет invalid

```
from pydantic import BaseModel, EmailStr, ValidationError
class Input(BaseModel):
    email: EmailStr
try:
    Input(email="not-email")
    print("ok")
except ValidationError:
    print("invalid")
```

Ответ: Верно

10. Верно ли, что в результате выполнения программы

```
import asyncio
async def long():
```

```
await asyncio.sleep(0.2)
async def main():
    await asyncio.wait_for(long(), timeout=0.1)
asyncio.run(main())
```

произойдёт asyncio.TimeoutError
Ответ: Верно

НАВЫКИ

11. Окно модели — 32 000 токенов. Системные и dev-инструкции — 2 200; новый запрос — 600; вставка из RAG — 5 500; нужно оставить запас на ответ 2 000. В истории — по 1 400 токенов на сообщение, их N штук. Каково максимальное N?

Расчёт: $32\,000 - (2\,200 + 600 + 5\,500 + 2\,000) = 21\,700$; $21\,700 / 1\,400 = 15.5 \rightarrow$ берём целое вниз.

Ответ: 15

12. За сессию совершено 180 вызовов инструментов, из них 12 завершились ошибкой. Укажите процент успешных вызовов (округлите до целых)

Ответ: 93

13. Название подхода, в котором агент чередует рассуждения и действия с наблюдениями, решая задачу пошагово (одно слово)

Ответ: ReAct

14. Верно ли, что код

```
from concurrent.futures import ThreadPoolExecutor
def f(x): return x*x
with ThreadPoolExecutor(max_workers=1) as ex:
    res = list(ex.map(f, [1,2,3,4]))
print(res)
```

выполняет задачи параллельно и утилизирует несколько потоков

Ответ: Неверно

15. Верно ли, что в результате выполнения программы

```
seen=set()
def create_invoice(req_id):
    if req_id in seen: return "dup"
    seen.add(req_id); return "ok"
print(create_invoice("X")); print(create_invoice("X"))
```

на экран попадут две строки — ok и затем dup

Ответ: Верно

***Примерные оценочные материалы
для проведения промежуточной аттестации (зачет, экзамен)
по итогам освоения дисциплины (модуля)***

1. Понятие искусственного интеллекта. Проблематика задач искусственного интеллекта (ИИ). Основные направления исследований в области ИИ.
2. Моделирование эвристических методов. Биологическое направление ИИ. Генетические алгоритмы и их назначение. Нейроны и их моделирование.
3. Общая схема генетического алгоритма.
4. Моделирование мутации и кроссовера в генетическом алгоритме.
5. Активные и пассивные методы получения знаний. Метод Делфи изучения предметной области.
6. Система знаний. Модели представления знаний: логические модели. Понятие о нечеткой логике.
7. Система знаний. Модели представления знаний: фреймовая и продукционная.
8. Система знаний. Модели представления знаний: семантические сети. Тезаурус и его использование в ИИ. Машинное представление знаний.
9. Задача распознавания образов в ИИ. Лингвистический и геометрический подход.
10. Задача распознавания образов в ИИ. Методы классификации.
11. Задача распознавания образов в ИИ. Методы кластеризации.
12. Представление знаний о предметной области в виде фактов и правил базы знаний Пролога.
13. Язык Пролог, структура и методы построения программ. Среда языка Пролог.
14. Стандартные предикаты Пролога. Разработка интерфейса в программах на Прологе.
15. Списки и их использование в декларативном программировании. Использование списков в программах на Прологе.
16. Основные модели нейронов – модели персептрона и сигмоидального нейрона.
17. Основные модели нейронов – адалайн, инстар-оутстар, WTA, модель Хебба, стохастическая модель.
- 20
18. Понятие нейронной сети. Основные виды нейронных сетей и их использование в системах ИИ. Случайные сети. Байсовские сети и сети Петри.
19. Обучение нейронной сети.
20. Экспертные системы. Общая характеристика, структура и основные элементы экспертных систем.
21. Экспертные системы. Интеллектуальные информационные ЭС. Понятие о ИАД.
22. Экспертные системы. Классификация ЭС по назначению. Основные направления приложения ЭС. Классификация ЭС по методам построения.
23. Инженерия знаний. Метод мозгового штурма.
24. Классификация компьютерных средств разработки систем ИИ. Роль программирования в развитии методов представления знаний. Агентные системы
25. Программирование в языке Пролог. Использование рекурсии в программах на Прологе.
26. Представление о логическом и функциональном программировании. Язык Лисп.

Темы письменных работ (эссе, рефераты, курсовые работы и др.)

ИИ и будущее работы: изменение отраслей и навыков

ИИ и человеческое творчество: компаньоны или конкуренты?

ИИ в сельском хозяйстве: преобразование методов ведения сельского хозяйства для устойчивого производства продуктов питания

Искусственный интеллект на финансовых рынках: возможности и риски

Влияние искусственного интеллекта на занятость и рабочую силу

ИИ в психическом здоровье: возможности, проблемы и этические соображения

Возникновение объяснимого ИИ: необходимость, проблемы и последствия

Этические последствия гуманоидных роботов на основе ИИ в уходе за пожилыми людьми

Пересечение искусственного интеллекта и кибербезопасности: вызовы и решения

Искусственный интеллект и парадокс конфиденциальности: баланс между инновациями и защитой данных

Будущее автономных транспортных средств и роль ИИ в транспорте