Колледж Автономной некоммерческой образовательной организации высшего образования

«Научно-технологический университет «Сириус»

Учебная дисциплина

**«Введение в специальность»**

Реферат

AI-агенты

Выполнил: студент 1 курса, группы К0709-24/1

направления подготовки

«Информационные системы и программирование»

Данилов Антон Витальевич

Проверила:

Яковлева Софья Вячеславовна

# **Оглавление**

**Оглавление** 2

**Введение** 3

**1 ЧТО ТАКОЕ AI-АГЕНТЫ?** 4

**1.1 Определение и основные характеристики** 4

**1.2 Примеры AI-агентов** 4

**2 ГЛАВНОЕ ПРО LLM** 5

**2.1 Большие языковые модели (LLM) как основа** 5

**2.2 Обучение и структура LLM** 7

**2.3 Специальные токены и их роль** 8

**3 КАК РАБОТАЮТ AI-АГЕНТЫ?** 8

**3.1 Инструменты и их роль** 8

**3.2 Цикл "мысль-действие-наблюдение"** 9

**3.3 Шаблоны чата и структурирование диалогов** 10

**4 ПРИМЕНЕНИЕ AI-АГЕНТОВ В БИЗНЕСЕ** 12

**4.1 Автоматизация бизнес-процессов** 12

**4.2 Маркетинг и реклама** 12

**4.3 Креативные задачи** 13

**5 ПЕРСПЕКТИВЫ AI-АГЕНТОВ** 13

**5.1 Технологическое развитие** 13

**5.2 Новые отрасли применения** 14

**5.3 Этика и вызовы** 14

**Заключение** 15

**Список использованных источников** 16

# **Введение**

В современном мире искусственный интеллект (ИИ) стал неотъемлемой частью нашей повседневной жизни, проникая во все сферы — от решения простых бытовых задач до управления сложными бизнес-процессами и научными исследованиями. Сегодня ИИ уже не является лишь инструментом для автоматизации рутинных операций: он кардинально меняет наше взаимодействие с технологиями, делая их более интуитивными, гибкими и способными самостоятельно принимать решения. Особое место среди различный направлений развития ИИ занимают **AI-агенты** — интеллектуальные системы, способные выходить за пределы простого исполнения команд, понимать запросы пользователей, анализировать данные, планировать действия и активно взаимодействовать с окружением для достижения поставленных целей.

Эти агенты олицетворяют собой новый этап эволюции ИИ, во многом благодаря применению **больших языковых моделей (LLM)**, таких как GPT-4 от OpenAI, Llama или Grok от xAI. LLM, обученные на гигантских массивах текстовых данных, LLM демонстрируют уникальные способности: они не только генерируют связный и естественный текст, но также понимают контекст, рассуждают логически и планируют последовательность действий. Благодаря этому AI-агенты решают задачи, которые ранее казались доступными исключительно человеку: от подготовки сложных отчетов до управления проектами и создания креативного контента.

# **1 ЧТО ТАКОЕ AI-АГЕНТЫ?**

## **1.1 Определение и основные характеристики**

AI-агент — это система, использующая модель искусственного интеллекта для взаимодействия с внешней средой для выполнения конкретных задач, заданных пользователем. В отличие от традиционных программ с фиксированными алгоритмами, AI-агенты умеют самостоятельно принимать решения, адаптироваться и обучаться. Они понимают естественный язык, анализируют контекст и применяют различные инструменты для достижения целей.

Представим виртуального помощника, которому дают команду: "Запланируй встречу с командой на завтра". Помощник понимает запрос, составляет план действий (проверить календарь, найти свободное время, отправить приглашения) и выполняет задачу, используя доступные ему инструменты и сторонние сервисы, например Google Календарь и Gmail. Именно в этом заключается суть AI-агента: сочетание "мозга" (модели ИИ) и "тела" (способности взаимодействовать с разными инструментами и сервисами).

## **1.2 Примеры AI-агентов**

AI-агенты уже присутствуют в нашей повседневной жизни:

* **Голосовые помощники**: Siri, Яндекс Алиса, Сбер Салют и Google Assistant давно умеют распозновать простые голосовые команды, такие как планирование событий, поиск информации в интернете и управление устройствами. Однако совсем недавно их подключили к большим языковым моделям (LLM), что сделало их умнее и способными отвечать на нестандартные вопросы.
* **Чат-боты для клиентов**: Чат-боты уже долго время помогают крупным компаниям отвечать на типовые вопросы клиентов, решать несложные проблемы и даже завершать транзакции. С подключением к большим языковым моделям (LLM) они стали еще умнее: теперь могут справляться с более сложными запросами, вести естественный диалог и предлагать решения, которые раньше требовали вмешательства человека. Это делает их незаменимыми помощниками в улучшении клиентского опыта.
* **Персонажи в видеоиграх**: Шаблонные персонажи в видеоиграх (NPC) раньше действовали строго по заданным скриптам, но нейросети и большие языковые модели (LLM) вдохнули в них новую жизнь. Теперь они могут быть более динамичными и разговорчивыми, реагировать на действия игрока, поддерживать осмысленные беседы и даже менять поведение в зависимости от ситуации. Это делает игровой мир более живым и затягивающим, побуждая игроков проводить в нём ещё больше времени.

Эти примеры показывают, как AI-агенты адаптируются к различным задачам в зависимости от их "инструментария".

## **2 ГЛАВНОЕ ПРО LLM**

## **2.1 Большие языковые модели (LLM) как основа**

Мозгом AI-агента выступает **большая языковая модель (LLM)**. К числу известных моделей относятся GPT-4 от OpenAI, Llama, YandexGPT 5 Pro от Яндекса и GigaChat Max от Сбера. **Важно отличать сами модели от AI-агентов:**например, GPT-4 — это LLM, способная понимать и генерировать текст, тогда как ChatGPT — это уже полноценный AI-агент, использующий GPT-4 в качестве ядра и дополняющий его интерфейсами, инструментами и логическими функциями для решения конкретных задач.

LLM — это тип модели искусственного интеллекта, которая отлично справляется с пониманием и генерированием человеческого языка.

## **2.2 Как работают LLM?**

LLM обучаются на огромных объемах текстовых данных и умеют предсказывать следующий токен (слово или часть слова) в последовательности. Это дает им возможность понимать и создавать тексты на естественном языке. Основой LLM служит архитектура Transformer, включающая механизм внимания (**attention**), который помогает модели сосредоточиваться на наиболее значимых частях вводимых данных. Это повышает эффективность работы с текстовыми задачами.

Существует три типа моделей на основе трансформеров:

* **Кодеры** (например, BERT) принимают на вход текст и выводят плотное представление этого текста.
* **Декодеры** (например, GPT) преобразует текст в токены и далее предсказывают их для завершения последовательности текста.
* **Модели** **кодер-декодер**(например, T5) они объединяют кодировщик и декодировщик. Кодировщик сначала преобразует входную последовательность в контекстное представление, а затем декодировщик генерирует выходную последовательность. Используются для преобразования текста, такого как перевод.

Для работы с человеческим языком нейросетям нужен особый «переводчик» — им выступает процесс **токенизации**. Так как компьютер воспринимают текст не как смысловую цеопчку, LLM разбивают его на токены — отдельные элементы, которые могут быть целыми словами («кофе»), частями слов («при» - «вет») или отдельными символами. Например, фраза «Как дела?» может разделиться на токены [«Как», «дела», «?»]. Каждому из них присваивается числовой код, что позволяет модели находить закономерности и генерировать ответы. Благодаря токенизации даже сложные запросы становятся «понятными» для ИИ, а обучение моделей — быстрым и эффективным.

LLM работают авторегрессионно: они предсказывают следующий токен на основе предыдущих. Например, в предложении **"Чтобы приготовить омлет, мне нужно ..."** модель понимает, что ключевые слова — "приготовить" и "омлет", и с высокой вероятностью предскажет "яйца" или "разбить яйца". Этот процесс лежит в основе генерации связных и контекстуально правильных ответов.

Для AI-агента LLM выполняет роль "мозга", отвечающего за:

* **Понимание естественного языка**: Интерпретация команд и запросов пользователя, включая распознавание смысла даже в свободной или нечёткой форме, что позволяет агенту улавливать намерения и контекст общения.
* **Рассуждение и планирование**: Анализ задачи, её разбиение на логические шаги и принятие решений о том, как лучше выполнить запрос, выбирая подходящие действия или инструменты.
* **Генерация текста**: Формирование ответов, инструкций или команд для инструментов в понятной и связной форме, адаптированной под запрос пользователя или требования системы.

## **2.3 Обучение и структура LLM**

LLM обучаются методом самоконтролируемого обучения на больших текстовых корпусах, где они учатся предсказывать следующее слово в последовательности. После предварительного обучения их можно дообучить для конкретных функций, таких как диалоговое взаимодействие или использование инструментов. В AI-агентах чаще применяются модели, ориентированные на генерацию текста (например, GPT-4, Llama), так как они лучше справляются с созданием связных ответов и поддержанием естественного общения с пользователем.

## **2.4 Специальные токены и их роль**

LLM используют **специальные токены** для структурирования данных. Например, токен конца последовательности (EOS) указывает, когда модель должна остановить генерацию текста. Другие токены обозначают начало и конец сообщений пользователя или помощника. Примеры:

* GPT-4: <|endoftext|>.
* Llama 3: <|eot\_id|>.
* SmolLM2: <|im\_end|>.

Эти токены критически важны для обработки диалогов и структурирования ответов в AI-агентах.

## **3 КАК РАБОТАЮТ AI-АГЕНТЫ?**

## **3.1 Инструменты и их роль**

LLM сама по себе генерирует только текст, но AI-агенты выходят за эти рамки благодаря **инструментам**. Модели предоставляется инструмент, с помощью которого модель может выполнить какое-либо действие, помимо генерации текста. Примеры:

* **Поиск в интернете**: К модели подключают средство выхода в интернет, чтобы она могла получить актуальную информацию из внешних источников.
* **API-интерфейсы**: Подключение к различным API для взаимодействия с внешними системами, такими как отправка писем, управление календарями или бронирование услуг.
* **Генерация изображений**: Для создания визуального контента на основе текстовых описаний, например, с помощью подключения сторонних моделей вроде DALL·E.
* **Распознавание изображений**: Для анализа фотографий или видео, выявления текста, объектов или лиц с использованием технологий компьютерного зрения.

Инструменты описываются в системном сообщении, чтобы агент знал, как их использовать, и мог применять их в зависимости от поставленной задачи.

## **3.2 Цикл "мысль-действие-наблюдение"**

Работа AI-агента строится на трёх ключевых этапах, которые повторяются в цикле, обеспечивая пошаговое выполнение задач:

1. **Мысль**: На этом этапе агент анализирует поступивший запрос, оценивает его суть и определяет, какие шаги нужно предпринять для решения. Например, получив задачу "Узнай текущую погоду", агент решает, что нужно обратиться к внешнему источнику данных, и планирует использовать соответствующий инструмент.
2. **Действие**: Агент переходит к выполнению запланированного шага, применяя доступные инструменты. Это может быть вызов API для получения погодных данных, поиск информации в интернете или запуск другой функции, например, отправка сообщения. Действие — это конкретный шаг, реализующий часть плана.
3. **Наблюдение**: После выполнения действия агент получает результат — обратную связь от инструмента или среды. Например, он видит ответ "солнечно, 20°C" и оценивает, достаточно ли этого для завершения задачи или нужно продолжить цикл, уточнив дополнительные детали, такие как прогноз на день.

Этот процесс, известный как подход **ReAct** (Reasoning + Acting), позволяет агенту гибко решать сложные задачи, адаптируясь к новым данным и корректируя свои действия на основе полученных результатов.

## **3.3 Шаблоны чата и структурирование диалогов**

AI-агенты часто взаимодействуют с пользователями через чат-интерфейсы, где общение организовано в виде последовательности сообщений. Для этого используются **шаблоны чата** — специальные структуры, которые преобразуют диалог в единую подсказку, понятную большой языковой модели (LLM). Эти шаблоны применяют **специальные токены**, чтобы четко разделять системные инструкции, запросы пользователя и ответы агента, обеспечивая правильное форматирование и сохранение контекста разговора.

Шаблоны чата включают:

* **Системные инструкции**: Задают поведение агента, например, "Вы — вежливый помощник по планированию".
* **Сообщения пользователя**: Содержат запросы, такие как "Запланируй встречу".
* **Ответы агента**: Результаты обработки запроса, которые модель генерирует.

Токены, такие как <|im\_start|> или <|end|>, обозначают начало и конец каждого элемента, помогая LLM понимать структуру диалога. Это гарантирует, что агент правильно интерпретирует задачу.

Рассмотрим, как это работает на практике. Пользователь говорит: **"Запланируй встречу с командой на завтра".** Агент выполняет задачу в рамках цикла "мысль-действие-наблюдение":

1. **Мысль**: Агент анализирует запрос, понимает, что нужно организовать встречу, и планирует шаги: проверить доступное время в календаре команды, выбрать подходящий час и уведомить участников.

2. **Действие**: Используя инструменты, агент обращается к календарю через API, определяет свободное окно, например, 14:00, и отправляет приглашения по электронной почте или в мессенджер.

3. **Наблюдение**: Получив подтверждение от инструментов (календарь обновлён, письма отправлены), агент формирует ответ: **"Встреча запланирована на завтра в 14:00, приглашения отправлены"**, и отправляет его пользователю.

Шаблон чата структурирует этот процесс, объединяя запрос и ответ в единую последовательность, например:

* <|im\_start|>пользователь: Запланируй встречу с командой на завтра <|im\_end|>
* <|im\_start|>помощник: Встреча запланирована на завтра в 14:00, приглашения отправлены <|im\_end|>.

Это позволяет агенту поддерживать логичный и последовательный диалог, сохраняя контекст и обеспечивая точность ответов.

# **4 ПРИМЕНЕНИЕ AI-АГЕНТОВ В БИЗНЕСЕ**

## **4.1 Автоматизация бизнес-процессов**

AI-агенты трансформируют бизнес, повышая эффективность и открывая новые возможности. Они автоматизируют процессы, улучшают взаимодействие с клиентами и поддерживают креативные задачи, становясь важным инструментом для компаний.

AI-агенты сокращают затраты и ускоряют выполнение рутинных операций, позволяя сотрудникам сосредоточиться на стратегических задачах:

**Управление задачами**: Агенты автоматизируют планирование проектов, распределяют задания по приоритетам и создают отчёты, например, с помощью интеграции с системами вроде ClickUp или Trello.

**Техническая поддержка**: Они обеспечивают быстрые и точные ответы на запросы клиентов, классифицируют обращения и передают сложные случаи людям, как это делает Zendesk AI.

**Рекрутинг**: Агенты анализируют резюме, оценивают соответствие кандидатов требованиям и даже проводят предварительные интервью через видео, ускоряя подбор персонала.

## **4.2 Маркетинг и реклама**

AI-агенты оптимизируют рекламные кампании, делая их более целенаправленными и экономичными:

* **Генерация контента**: Они создают тексты для объявлений, постов в соцсетях или даже изображения для баннеров, как это реализовано в инструментах вроде Bannerbear.
* **Анализ эффективности**: Агенты подбирают ключевые слова, оценивают результаты кампаний и предлагают стратегии улучшения, например, через платформы типа Adzooma.

## **4.3 Креативные задачи**

AI-агенты находят применение в творческих отраслях, ускоряя процессы и вдохновляя команды:

* **Видео и графика**: Они автоматизируют монтаж роликов, удаляют ненужные элементы или создают анимации, как в Runway ML.
* **3D-модели**: Агенты преобразуют 2D-изображения в трёхмерные объекты для дизайна, игр или архитектуры, например, с помощью Kaedim.

# **5 ПЕРСПЕКТИВЫ AI-АГЕНТОВ**

## **5.1 Технологическое развитие**

AI-агенты обладают огромным потенциалом, который раскроется в ближайшие годы благодаря технологическому прогрессу, расширению сфер применения и решению связанных с ними вызовов.

AI-агенты станут умнее и автономнее благодаря прогрессу в машинном обучении и обработке естественного языка. Улучшение больших языковых моделей (LLM) позволит им быстрее обучаться, точнее понимать сложные запросы и самостоятельно принимать решения с минимальным участием человека.

## **5.2 Новые отрасли применения**

Они проникают в новые сферы, такие как образование, медицина и право, делая передовые технологии доступнее. Например, в образовании агенты смогут выступать персональными репетиторами, в медицине — помогать с диагностикой, а в юриспруденции — автоматизировать анализ договоров и консультации.

## **5.3 Этика и вызовы**

С развитием AI-агентов возникают важные вопросы, которые нужно решить: обеспечение конфиденциальности данных пользователей, устранение предвзятости в решениях моделей и разработка правил регулирования их использования в обществе. Эти аспекты станут ключевыми для безопасного и справедливого применения технологии.

# **Заключение**

AI-агенты представляют собой мощный инструмент, который уже сегодня меняет нашу жизнь, автоматизируя рутинные задачи, повышая эффективность работы и открывая новые горизонты для бизнеса и общества. Их уникальная способность понимать естественный язык, рассуждать, планировать действия и адаптироваться к изменяющимся условиям делает их незаменимыми помощниками в современном мире. Благодаря интеграции с большими языковыми моделями и внешними инструментами, они справляются с задачами, которые раньше требовали исключительно человеческого участия — от управления проектами до создания креативного контента.

Однако успешное внедрение AI-агентов требует вдумчивого подхода: необходимо учитывать не только технологические аспекты, такие как совершенствование моделей и расширение их возможностей, но и этические вопросы — защиту данных, устранение предвзятости и обеспечение прозрачности их работы. Несмотря на эти вызовы, потенциал AI-агентов огромен: они способны не только оптимизировать процессы, но и стать катализатором инноваций в самых разных сферах — от образования до медицины. Мир AI-агентов уже стал реальностью, и сейчас самое время использовать их возможности для личного роста, развития бизнеса и построения более технологически продвинутого будущего.

# **Список использованных источников**

1. Building Effective AI Agents | Anthropic \ Anthropic [Электронный ресурс] // Anthropic. — 2025. — URL: <https://www.anthropic.com/engineering/building-effective-agents> (дата обращения: (09.03.2025).
2. LLM (large language models): языковые модели, их значение, перспективы развития - GigaChat [Электронный ресурс] // Sber. — 2025. — URL: <https://developers.sber.ru/help/gigachat-api/large-language-models> (дата обращения: 09.03.2025).
3. Tips for building AI agents [Видеоролик] // Youtube. — 2025. — URL: <https://www.youtube.com/watch?v=LP5OCa20Zpg> (дата обращения: 09.03.2025).
4. Как AI-агенты меняют бизнес [Электронный ресурс] // Sbermarketing. — 2025. — URL: <https://sbermarketing.ru/news/kak-ai-agenty-meniaiut-biznes-rbc> (дата обращения: 09.03.2025).
5. AI-агенты для бизнеса: от технической поддержки до маркетинга I Блог Napoleon IT [Электронный ресурс] // Napoleon IT. — 2025. — URL: <https://napoleonit.ru/blog/ai-agenty-dlya-biznesa-ot-tehnicheskoy-podderzhki-do-marketinga> (дата обращения: 09.03.2025).
6. What are AI agents? Definition, examples, and types | Google Cloud [Электронный ресурс] // Google Cloud. — 2025. — URL: <https://cloud.google.com/discover/what-are-ai-agents> (дата обращения: 09.03.2025).