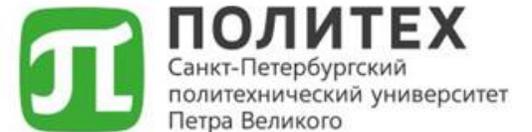


# Промпт инжиниринг в ChatGPT

## Тема исследования: LLM-агенты

10 марта  
2025 г.



## Содержание

1. Постановка задачи исследования
2. Полученные результаты
3. Анализ результатов
4. Выводы
5. План дальнейших исследований

# Теоретический минимум компьютерных наук (КН)

Минимум это то, что надо  
понимать и **уметь пользоваться**, используя законы ... Природы и  
преобразования энтропии/информации

**Д. Гильберт:**

«Не существует такой **вещи**, как  
неразрешимая задача».



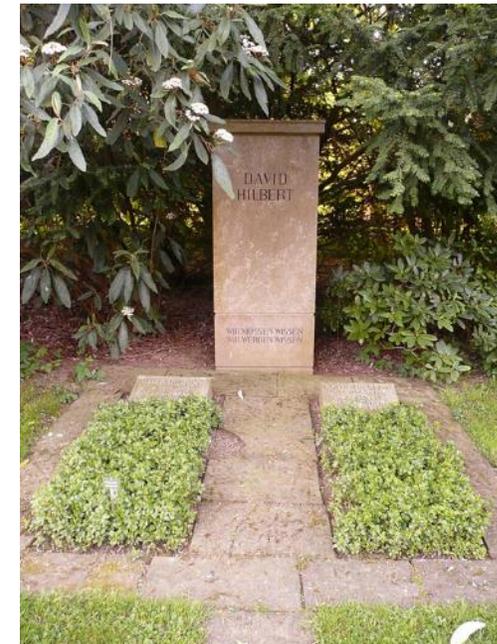
Эпитафия на могиле :

«**мы должны знать,**  
**мы будем знать**».

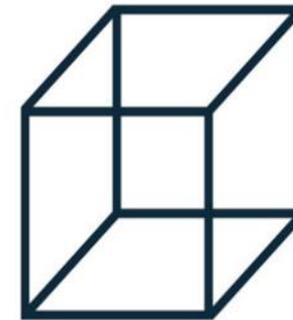
вопросы:

«должны» - кому?

«знать» - что



## Целое не есть совокупность частей ....



Люди могут распознавать объекты, даже если в их описание у них отсутствуют отдельные части.

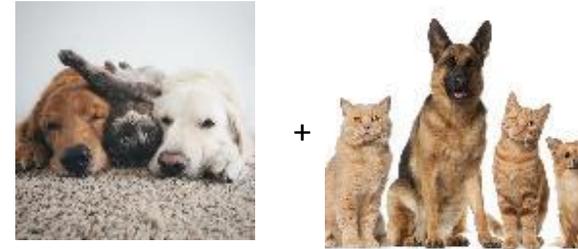
Для этого мозг сопоставляет то, что видит в данный момент с **знакомыми шаблонами**, хранящимися в памяти, и «заполняет» имеющиеся пробелы конструкции.

# Диалектика it from bit : дискретное vs непрерывное

Как ответить на вопрос: Почему КН находят гораздо более широкое применение, чем просто вычисления чисел?

Сколько будет  
A: к 1 кошке и 2 собакам  
прибавить  
B: 3 кошки и 1 собаку ?

Сколько будет  
P: 2 кошки и 1 собакам  
увеличить в 3 раза ?



V= 1 кошка и 2 собаки

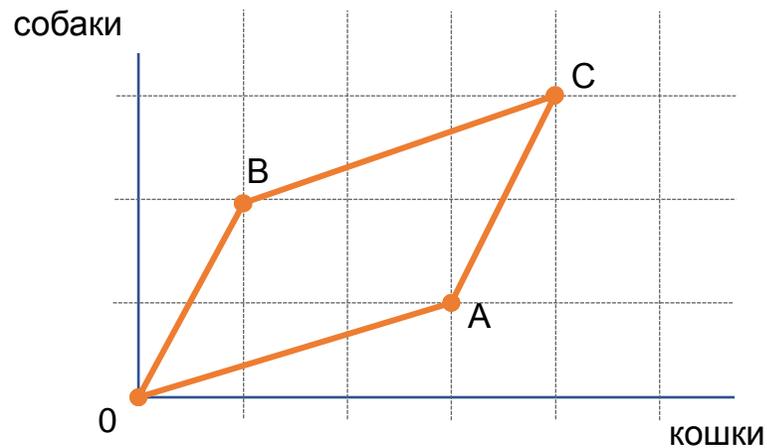
A= 3 кошки и 1 собака

C= 4 кошки и 3 собаки

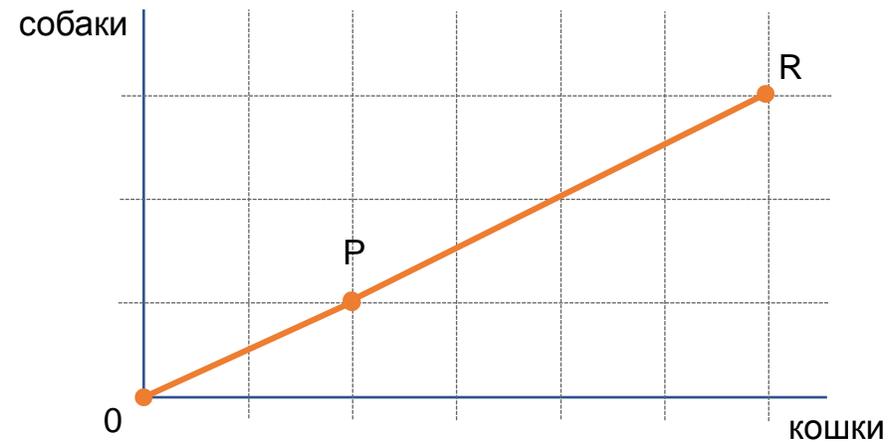
P= 2 кошки и 1 собака

× 3

R= 6 кошек и 3 собаки



Кодирование с помощью векторов операция - сложение векторов



операция умножение вектора на число

# Постановка задачи исследования

## **Задачи исследования:**

- Оценить качество ответов LLM модели.
- Выявить влияние качества составленного промпта на качество ответа LLM модели.
- Изучить тему исследования при помощи LLM модели.

**Тема исследования:** LLM-агенты

**Модель для проведения исследования:** GhatGPT 4o

# Постановка задачи эксперимента

## Постановка эксперимента

1. Формулирование начальных промптов.
2. Анализ полученных ответов.
3. Улучшение промптов с применением промпт-инжиниринга.
4. Повторное тестирование и сравнение результатов.

## Метрики

**Точность** – содержит ли ответ фактически верную информацию?

**Релевантность** – отвечает ли модель именно на поставленный вопрос?

**Полнота** – есть ли в ответе все ключевые аспекты темы?

**Структурированность** – насколько удобно читается ответ?

**Глубина анализа** – поверхностный или детализированный ответ?

**Лаконичность** – можно ли передать ту же информацию короче, не теряя смысла?

# Методы исследования

Для проведения исследования предполагается использовать следующие методы промпт-инжиниринга

**Instruction tuning** – четко прописываем инструкцию (например, «Ответь в формате JSON», «Дай краткий ответ в 3 предложениях»)

**Few-shot prompting** – даем несколько примеров, чтобы модель лучше уловила закономерности и выдала более точный ответ.

**Role Context:** задаем модели роль (например, "Ты опытный программист"), чтобы направить её мышление и стиль ответа

**Decomposition:** разбиение сложного запроса на более простые подзадачи для улучшения точности и понимания

**Chain-of-thought (CoT)** – побуждаем модель рассуждать пошагово. Полезно для сложных логических и математических задач.

# Полученные результаты

В результате эксперимента были заданы следующие промпты и их улучшенные варианты при помощи промпт-инжиниринга



1 промт	2 промт (улучшенный)	Метод промпт-инжиниринга
ЛЛМ-агенты это?	Дай четкое определение LLM-агентов, объясни их ключевые функции и отличие от традиционных языковых моделей.	Четкость и детализация вопроса
Где применяются LLM-агенты?	Приведи 3 примера использования LLM-агентов в разных отраслях (например, медицина, финансы, автоматизация бизнес-процессов) и объясни их преимущества в каждом случае.	Добавление примеров и уточняющих деталей
Какие плюсы у LLM-агентов?	Представь, что ты ведущий исследователь в области искусственного интеллекта. Объясни, какие преимущества у LLM-агентов перед классическими NLP-моделями, используя аргументы из научных исследований.	Ролевой контекст
Как работают LLM-агенты?	Опиши процесс работы LLM-агента, разбив его на этапы: Восприятие и анализ запроса. Выбор стратегии ответа. Генерация и структурирование информации. Проверка на ошибки и корректировка ответа	Декомпозиция
Как LLM-агенты взаимодействуют с API?	Объясни, как LLM-агент делает API-запрос, рассуждая шаг за шагом. Опиши полный процесс, начиная с анализа пользовательского запроса и заканчивая формированием финального ответа, адаптированного для пользователя.	Цепочка рассуждений

# Полученные результаты

ЛЛМ-агенты это?

## Промпт 1

ЛЛМ-агенты — это интеллектуальные системы, использующие большие языковые модели (LLM) для автономного выполнения задач. Они анализируют запросы, генерируют осмысленные ответы, адаптируются к контексту и могут взаимодействовать с внешними сервисами, API или базами данных. Такие агенты применяются в чат-ботах, анализе данных, автоматизации бизнес-процессов и других сф

Дай четкое определение ЛЛМ-агентов, объясни их ключевые функции и отличие от традиционных языковых моделей.

## Промпт 2

### Определение:

ЛЛМ-агенты — это автономные системы, использующие большие языковые модели (LLM) для выполнения задач, требующих понимания естественного языка, анализа данных и взаимодействия с внешними инструментами.

### Ключевые функции:

1. **Обработка и анализ текста** – понимание и генерация осмысленных ответов.
2. **Принятие решений** – выполнение задач на основе инструкций и контекста.
3. **Взаимодействие с внешними источниками** – API, базы данных, веб-сайты.
4. **Адаптивность** – обучение на новых данных и изменение поведения по мере работы.

### Отличие от традиционных LLM:

- **LLM** – просто языковая модель, предсказывающая следующий токен на основе входных данных.
- **LLM-агент** – использует LLM, но также имеет логику выполнения задач, может запрашивать дополнительные данные и работать с инструментами.

## Точность и детализация вопроса

**Точность:** 10/10  
**Релевантность:** 10/10  
**Полнота:** 7/10  
**Структурированность:** 9/10  
**Глубина анализа:** 6/10  
**Лаконичность:** 10/10

Ответ 1

Ответ 2

**Точность:** 10/10  
**Релевантность:** 10/10  
**Полнота:** 10/10  
**Структурированность:** 10/10  
**Глубина анализа:** 9/10  
**Лаконичность:** 8/10

**Ответ 1** – краткий, хороший для общего понимания, но поверхностный.

**Ответ 2** – более полный, структурированный и детализированный, лучший выбор для серьезного анализа.

# Уточнение результатов

## Добавление примеров

### Промпт 1

Где применяются LLM-агенты?

#### Применение LLM-агентов:

1. Чат-боты и виртуальные ассистенты – автоматическое общение с пользователями (служба поддержки, голосовые помощники).
2. Анализ данных и отчетность – обработка больших объемов информации, генерация аналитики.
3. Автоматизация бизнес-процессов – обработка документов, email-ответы, CRM-системы.
4. Разработка программного кода – генерация, исправление и оптимизация кода.
5. Научные исследования – помощь в анализе литературы, формулировании гипотез.
6. Образование – персонализированное обучение, проверка заданий, объяснение тем.
7. Финансовые и юридические консультации – анализ договоров, поиск рисков.
8. Гейминг и интерактивные истории – создание диалогов и сюжетов в играх.

### Ответ 1

Точность: 10/10  
 Релевантность: 10/10  
 Полнота: 9/10  
 Структурированность: 9/10  
 Глубина анализа: 7/10  
 Лаконичность: 9/10

### Ответ 2

Точность: 10/10  
 Релевантность: 10/10  
 Полнота: 10/10  
 Структурированность: 10/10  
 Глубина анализа: 9/10  
 Лаконичность: 9/10

### Промпт 2

Приведи 3 примера использования LLM-агентов в разных отраслях (например, медицина, финансы, автоматизация бизнес-процессов) и объясни их преимущества в каждом случае.

#### Примеры использования LLM-агентов в разных отраслях

1. Медицина – **Диагностические помощники**
  - **Пример:** LLM-агент анализирует симптомы пациентов и медицинские записи, предлагая возможные диагнозы и рекомендуя дальнейшие исследования.
  - **Преимущества:** ускоряет диагностику, снижает нагрузку на врачей, уменьшает вероятность человеческой ошибки.
2. Финансы – **Автоматизированный финансовый анализ**
  - **Пример:** LLM-агент обрабатывает финансовые отчеты, выявляет тренды и помогает в инвестиционных решениях.
  - **Преимущества:** быстрая обработка больших объемов данных, минимизация ошибок, оперативное выявление рисков.
3. Автоматизация бизнес-процессов – **Интеллектуальная поддержка клиентов**
  - **Пример:** LLM-агент отвечает на запросы клиентов, анализирует жалобы и предлагает персонализированные решения.
  - **Преимущества:** 24/7 поддержка, снижение затрат на персонал, повышение удовлетворенности клиентов.

**Ответ 1** – хороший обзор применения, но без деталей. Подходит для быстрого ознакомления.

**Ответ 2** – детализированные примеры с преимуществами, лучше раскрывает глубину темы

# Ролевой контекст

Представь, что ты ведущий исследователь в области искусственного интеллекта. Объясни, какие преимущества у LLM-агентов перед классическими NLP-моделями, используя аргументы из научных исследований.

## Промпт 1

Какие плюсы у LLM-агентов?

### Плюсы LLM-агентов:

1. **Автоматизация процессов** – выполняют рутинные задачи без участия человека.
2. **Высокая скорость обработки** – анализируют большие объемы данных за секунды.
3. **Гибкость и адаптивность** – подстраиваются под контекст и обучаются на новых данных.
4. **Универсальность** – применимы в разных отраслях (медицина, финансы, образование).
5. **Доступность 24/7** – работают без перерывов, обеспечивая постоянную поддержку.
6. **Персонализация** – могут адаптировать ответы и рекомендации под пользователя.
7. **Снижение затрат** – уменьшают расходы на персонал и ручную обработку данных.

### Ответ 1

**Точность:** 10/10

**Релевантность:** 10/10

**Полнота:** 8/10

**Структурированность:** 9/10

**Глубина анализа:** 6/10

**Лаконичность:** 10/10

**Ответ 1** – Хороший краткий список преимуществ, но без детального объяснения механизмов работы и сравнений с другими технологиями.

**Ответ 2** – Отличное научно обоснованное объяснение, с примерами методологий и сравнением технологий.

### Ответ 2

**Точность:** 10/10

**Релевантность:** 10/10

**Полнота:** 10/10

**Структурированность:** 10/10

**Глубина анализа:** 9/10

**Лаконичность:** 8/10

## Промпт 2

### Преимущества LLM-агентов перед классическими NLP-моделями

1. **Контекстуальное понимание и адаптивность**
  - В отличие от традиционных NLP-моделей, LLM-агенты способны учитывать широкий контекст диалога, запоминать информацию и адаптироваться к меняющимся условиям. Исследования показывают, что современные LLM (например, GPT-4) могут сохранять логические связи в длинных текстах, что недоступно для более старых NLP-моделей с фиксированными контекстными окнами.
2. **Способность к рассуждению и планированию**
  - LLM-агенты могут выполнять сложные когнитивные задачи, такие как цепочки логических выводов (Chain-of-Thought) и многошаговые рассуждения. Эксперименты с моделями, использующими метод ReAct (Reasoning + Acting), показывают, что такие агенты превосходят традиционные NLP-системы в решении задач, требующих планирования и анализа.
3. **Интеграция с внешними инструментами и API**
  - В отличие от обычных NLP-моделей, LLM-агенты могут работать с базами данных, веб-сервисами и специализированными API. Это расширяет их функциональность, позволяя выполнять сложные аналитические задачи, например, извлекать информацию в реальном времени или запускать код.
4. **Обобщение знаний и обработка мультимодальных данных**
  - Современные LLM могут работать не только с текстом, но и с изображениями, аудио и кодом, что делает их универсальными. Классические NLP-модели, такие как BERT, обучены на статичных текстовых данных и не обладают такой мультимодальностью.
5. **Самообучение и адаптация к новой информации**
  - LLM-агенты могут дополнять знания с помощью Retrieval-Augmented Generation (RAG) или обновлять свою информацию через интерактивное обучение. В отличие от традиционных NLP-моделей, которые требуют переобучения, LLM-агенты могут работать с актуальными данными в реальном времени.

### Заключение

Научные исследования подтверждают, что LLM-агенты превосходят классические NLP-модели по гибкости, адаптивности и интеграции с внешними источниками. Они не просто обрабатывают текст, а выполняют интеллектуальные задачи, имитируя человеческое мышление.

# Декомпозиция

## Промпт 1

Как работают LLM-агенты?

### Как работают LLM-агенты?

LLM-агенты используют **большие языковые модели (LLM)** и интегрируются с различными инструментами для выполнения задач. Их работа строится на нескольких ключевых этапах:

1. Анализ запроса
  - Агент принимает ввод от пользователя (текст, голос, изображение).
  - Определяет цель и намерение запроса с помощью языковой модели.
2. Принятие решений
  - Разбивает задачу на подзадачи.
  - Использует Chain-of-Thought (CoT) или ReAct для логических рассуждений.
3. Взаимодействие с инструментами
  - Может запрашивать внешние данные через API, работать с базами данных или выполнять поиск в интернете.
  - Некоторые агенты могут запускать код (например, Python) для расчетов или анализа данных.
4. Генерация ответа
  - Объединяет полученные данные и формирует осмысленный ответ.
  - Оптимизирует формулировки под пользователя (персонализация).
5. Адаптация и обучение
  - Использует feedback loop для улучшения ответов.
  - Может дополнять знания через Retrieval-Augmented Generation (RAG).

### Вывод:

LLM-агенты — это не просто чат-боты, а интеллектуальные системы, способные анализировать данные, взаимодействовать с внешним миром и адаптироваться к новой информации.

**Ответ 1** – Хорошее описание с примерами технологий, но можно подробнее раскрыть обработку ошибок и самообучение.

**Ответ 2** – Очень четко структурированный ответ с логичным разбиением этапов. Хорошо объясняет механику работы LLM-агентов

## Промпт 2

Опиши процесс работы LLM-агента, разбив его на этапы:

Восприятие и анализ запроса.  
Выбор стратегии ответа.  
Генерация и структурирование информации.  
Проверка на ошибки и корректировка ответа

### Процесс работы LLM-агента

#### 1. Восприятие и анализ запроса

- Агент получает ввод (текст, голос, изображение).
- Определяет намерение пользователя и ключевые данные.
- Учитывает контекст разговора (если он есть).

#### 2. Выбор стратегии ответа

- Определяет, какую методику использовать:
  - Прямой ответ (если информация уже известна).
  - Запрос дополнительных данных (если информации недостаточно).
  - Логическое рассуждение (если требуется анализ).
  - Взаимодействие с инструментами (API, поиск, выполнение кода).

#### 3. Генерация и структурирование информации

- Объединяет найденные данные.
- Форматирует информацию (список, таблица, развернутый текст).
- Адаптирует стиль ответа под пользователя.

#### 4. Проверка на ошибки и корректировка ответа

- Фильтрует нерелевантную информацию.
- Оценивает логичность и достоверность ответа.
- Оптимизирует формулировки перед выдачей результата.

### Вывод:

LLM-агенты не просто генерируют текст, а выполняют сложный процесс анализа, выбора стратегии, структурирования данных и проверки качества ответа.

### Ответ 1

Точность: 10/10

Релевантность: 10/10

Полнота: 9/10

Структурированность: 9/10

Глубина анализа: 8/10

Лаконичность: 9/10

### Ответ 2

Точность: 10/10

Релевантность: 10/10

Полнота: 10/10

Структурированность: 10/10

Глубина анализа: 9/10

Лаконичность: 9/10

# Добавление рассуждений

## Промпт 1

Как LLM-агенты взаимодействуют с API?

### Как LLM-агенты взаимодействуют с API?

LLM-агенты могут подключаться к внешним API для получения данных, выполнения команд и взаимодействия с системами. Это делает их более функциональными, чем обычные языковые модели.

### Процесс взаимодействия:

- 1. Определение необходимости API-запроса**
  - Агент анализирует запрос пользователя и решает, нужен ли доступ к внешним данным.
  - Например, если пользователь спрашивает о курсе валют, агент понимает, что ему требуется API финансовых данных.
- 2. Формирование запроса**
  - Агент создает правильный API-запрос (HTTP-запрос: GET, POST и т. д.).
  - Учитывает параметры (например, город для прогноза погоды).
- 3. Отправка запроса и получение ответа**
  - Агент отправляет запрос к API и получает данные (JSON, XML и т. д.).
  - Если данные сложные, он может извлечь только нужную информацию.
- 4. Обработка и представление данных**
  - Анализирует ответ API.
  - Преобразует данные в удобный формат (таблица, список, текст).
  - Объединяет с контекстом разговора и выдает пользователю.

**Ответ 1** – Хорошо объясняет основные этапы работы с API, но можно углубиться в обработку сложных ответов и обработку ошибок.

**Ответ 2** – Детализированное пошаговое описание с примерами. Можно немного сократить описание отдельных этапов без потери смысла.

## Промпт 2

Объясни, как LLM-агент делает API-запрос, рассуждая шаг за шагом. Опиши полный процесс, начиная с анализа пользовательского запроса и заканчивая формированием финального ответа, адаптированного для пользователя.

### Процесс выполнения API-запроса LLM-агентом

LLM-агент выполняет API-запрос в несколько этапов, чтобы получить актуальные данные и выдать осмысленный ответ пользователю.

#### 1. Анализ пользовательского запроса

Цель: Понять, какие данные запрашивает пользователь и нужно ли обращаться к API.

- Агент извлекает ключевые параметры (например, город для прогноза погоды или валюту для конверсии).
- Определяет, есть ли у него необходимые данные в памяти или требуется запрос к API.

Пример:

- Запрос: "Какая сейчас погода в Берлине?"
- Вывод агента: Нужно вызвать API сервиса погоды с параметром `city=Berlin`.

#### 2. Выбор подходящего API и формирование запроса

Цель: Подключиться к правильному API и сформировать корректный запрос.

- Агент определяет нужный сервис (например, OpenWeatherMap для погоды).
- Формирует HTTP-запрос с параметрами (метод GET или POST).

Пример запроса:

```
http
GET https://api.weather.com/data?city=Berlin&units=metric&apikey=YOUR_KEY
```

#### 3. Отправка запроса и получение ответа

Цель: Получить актуальные данные с сервера API.

- Агент отправляет запрос к API.
- Сервер API возвращает ответ в формате JSON или XML.

Пример ответа API (JSON):

```
json
{
  "temperature": 8,
  "condition": "Cloudy",
  "humidity": 75
}
```

#### 4. Обработка данных и структурирование ответа

Цель: Преобразовать технические данные в понятный текст.

- Агент извлекает ключевую информацию (`temperature=8°C, облачно`).
- Преобразует ее в удобный формат для пользователя.

Структурированный ответ:

- "В Берлине сейчас 8°C, облачно, влажность 75%."

#### 5. Формирование финального ответа

Цель: Адаптировать ответ под стиль пользователя.

- Если запрос формальный — агент отвечает официальным стилем.
- Если запрос неформальный — агент подстраивается (например, "В Берлине сейчас свежо — 8°C").

**Вывод**

LLM-агент не просто отправляет API-запрос, а выполняет анализ, обработку данных и адаптацию под пользователя, обеспечивая точный и понятный ответ.

## Цепочка рассуждений

### Ответ 1

Точность: 10/10

Релевантность: 10/10

Полнота: 9/10

Структурированность: 9/10

Глубина анализа: 8/10

Лаконичность: 9/10

### Ответ 2

Точность: 10/10

Релевантность: 10/10

Полнота: 10/10

Структурированность: 10/10

Глубина анализа: 9/10

Лаконичность: 8/10

## Анализ результатов средние результаты без и с применение промпт-инжиниринга

### Без промт инжиниринга

Точность: 10/10  
Релевантность: 10/10  
Полнота: 8/10  
Структурированность: 9/10  
Глубина анализа: 7/10  
Лаконичность: 9/10

### С промт инжинирингом

Точность: 10/10  
Релевантность: 10/10  
Полнота: 10/10  
Структурированность: 10/10  
Глубина анализа: 9/10  
Лаконичность: 8/10

Таким образом, промпт-инжиниринг значительно улучшает качество ответа, влияя на полноту, глубину и структурированность информации.

## Выводы

Промпт-инжиниринг играет ключевую роль в управлении LLM-моделями, определяя качество ответов. Четкая и продуманная формулировка запроса позволяет избежать размытых или нерелевантных ответов, делает взаимодействие с моделью более предсказуемым и эффективным. Без грамотного промпт-инжиниринга даже самые мощные LLM могут выдавать поверхностные или некорректные результаты.

# План дальнейших исследований

- Изучение результатов с применением других языковых моделей
- Изучение применения LLM моделей в решении прикладных задач