

# ИИ-агенты для юристов: от базовых принципов к пониманию возможностей



*Лектор: Нурлан Даниев*

# План вебинара

ИИ-агенты для юристов: от базовых принципов к пониманию возможностей



1

От чата к агенту: эволюция инструментов



2

Из чего состоит ИИ-агент: модель, инструменты и обязанка



3

Agents.md, Skill.md и MCP: как это работает на практике



4

Безопасность, кейсы и первые шаги внедрения



5

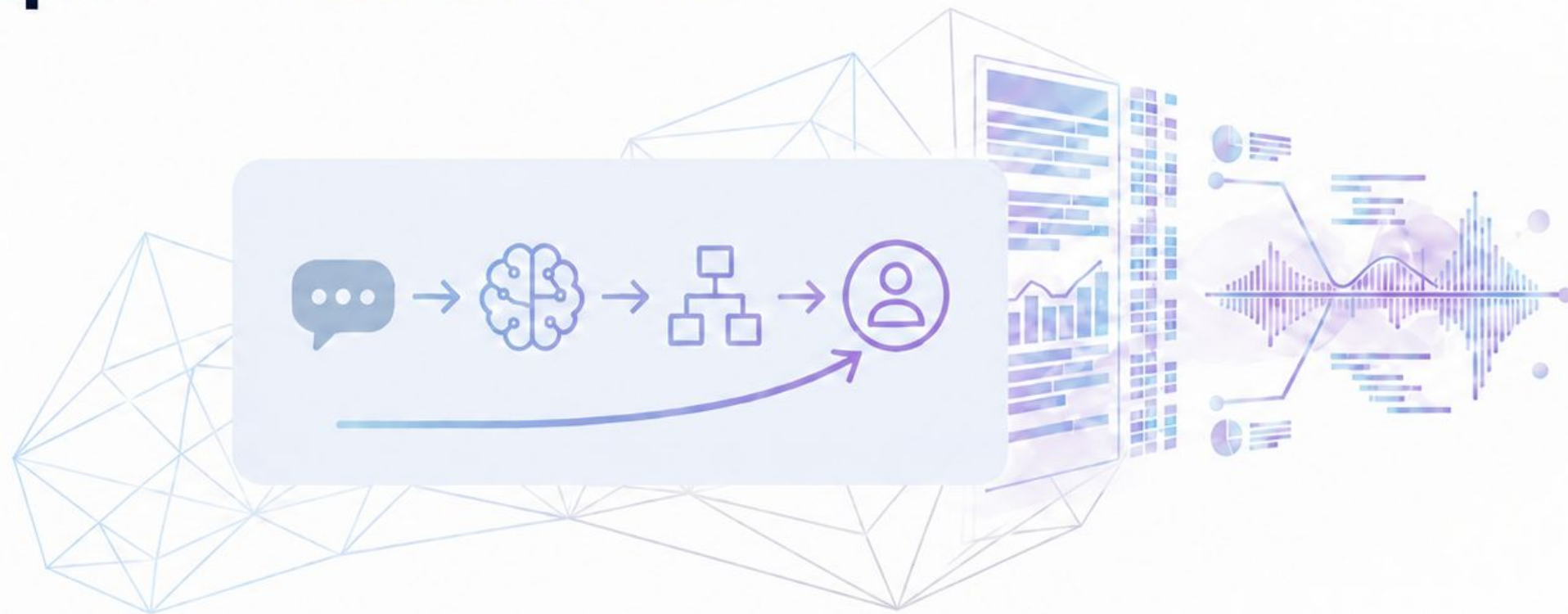
Что уже делают юристы с помощью ИИ



6

Claude/ChatGPT Work и Code как точка входа в агентов

# От чата к агенту: ЭВОЛЮЦИЯ ТЕХНОЛОГИИ



# Движение



Нейросеть



Чат



Поиск



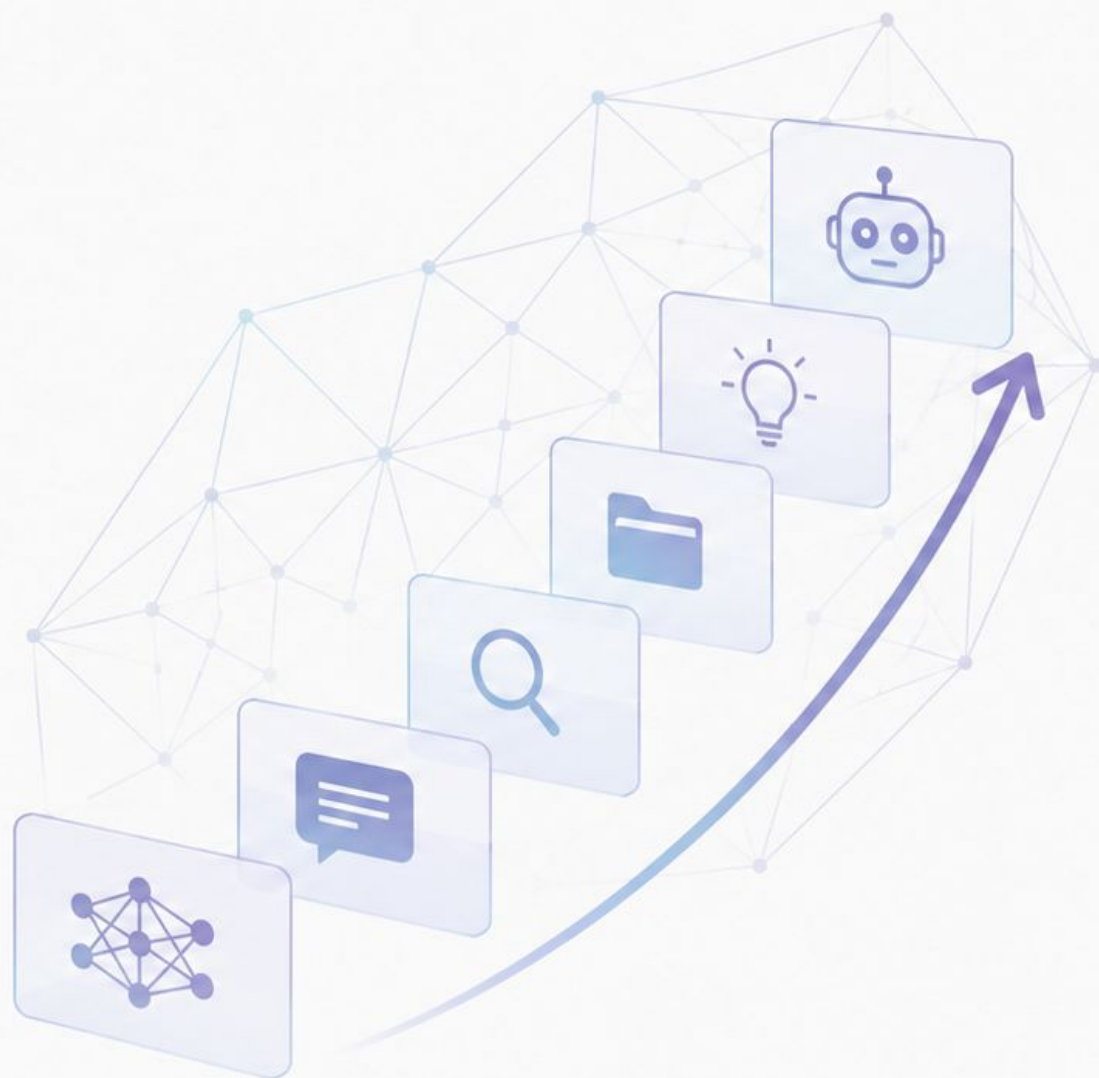
Проект



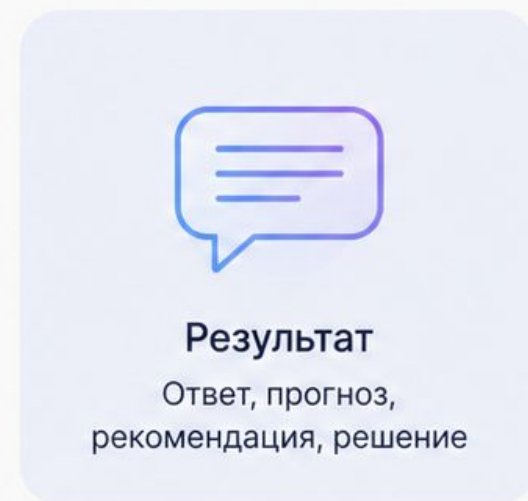
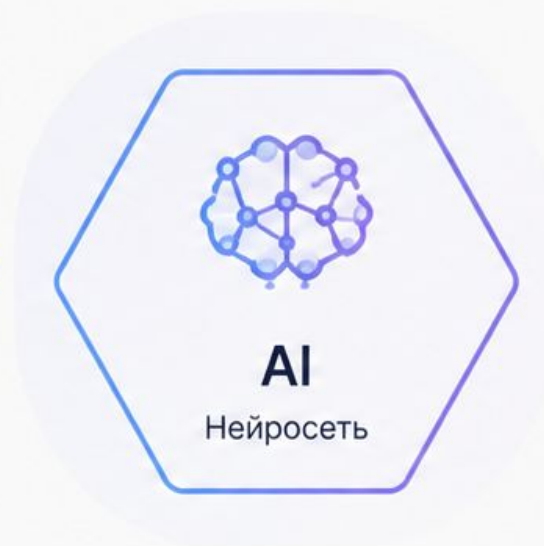
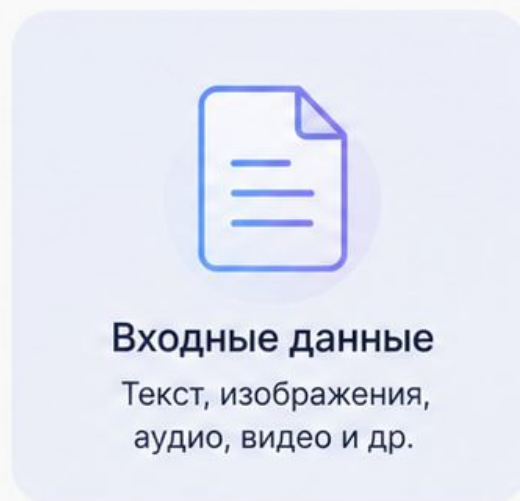
Думающие модели



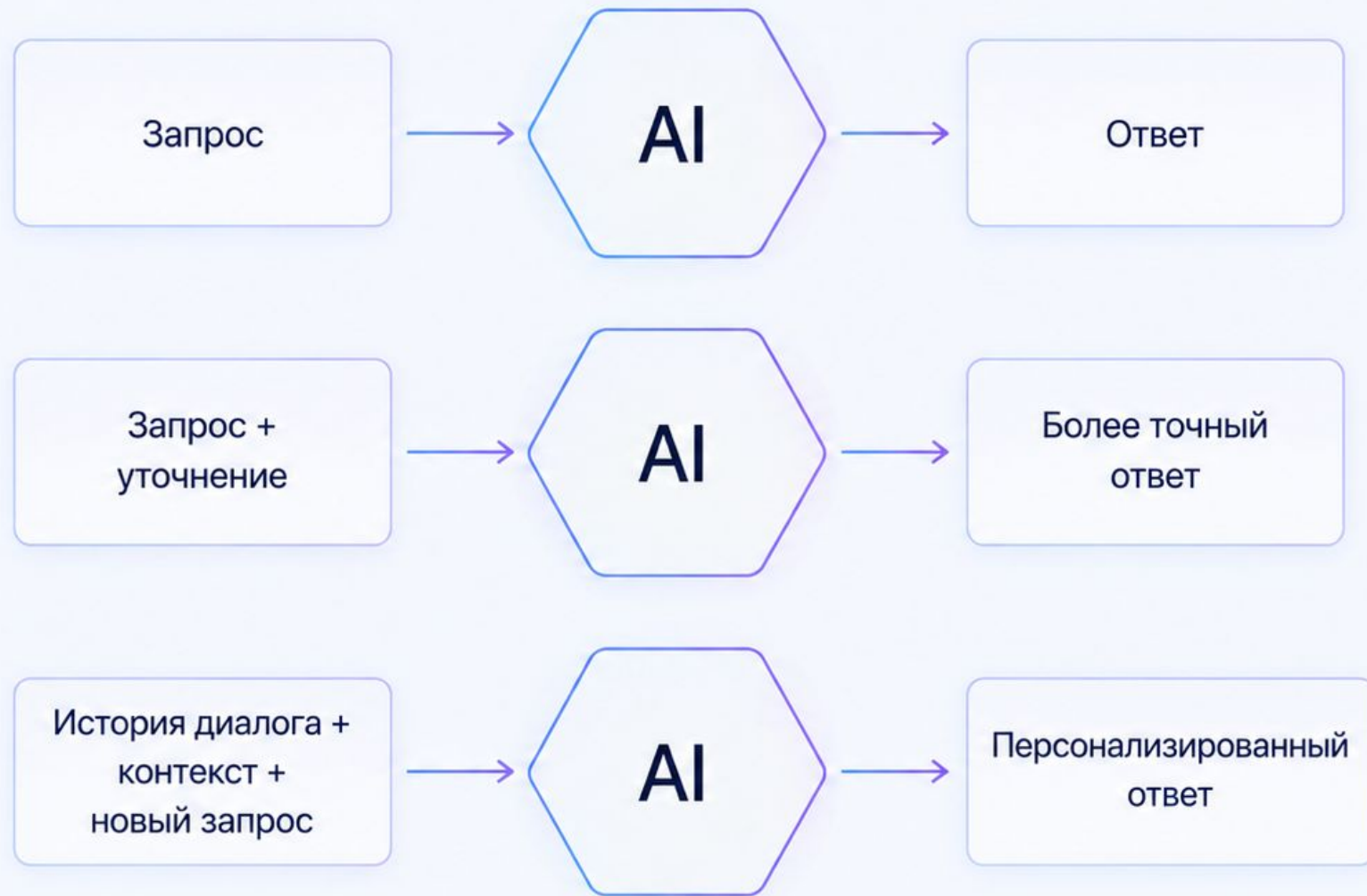
Агенты



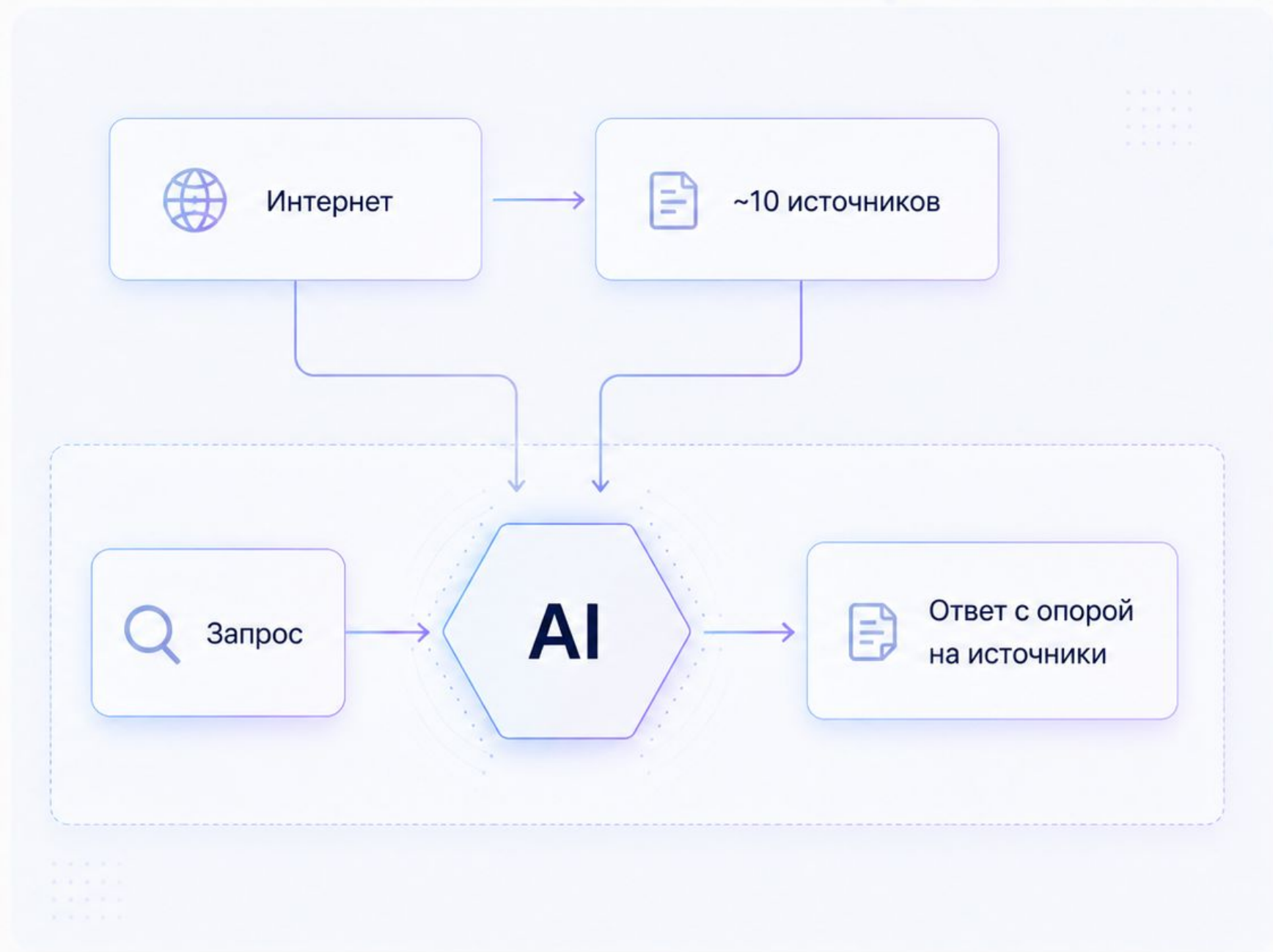
# Нейросеть



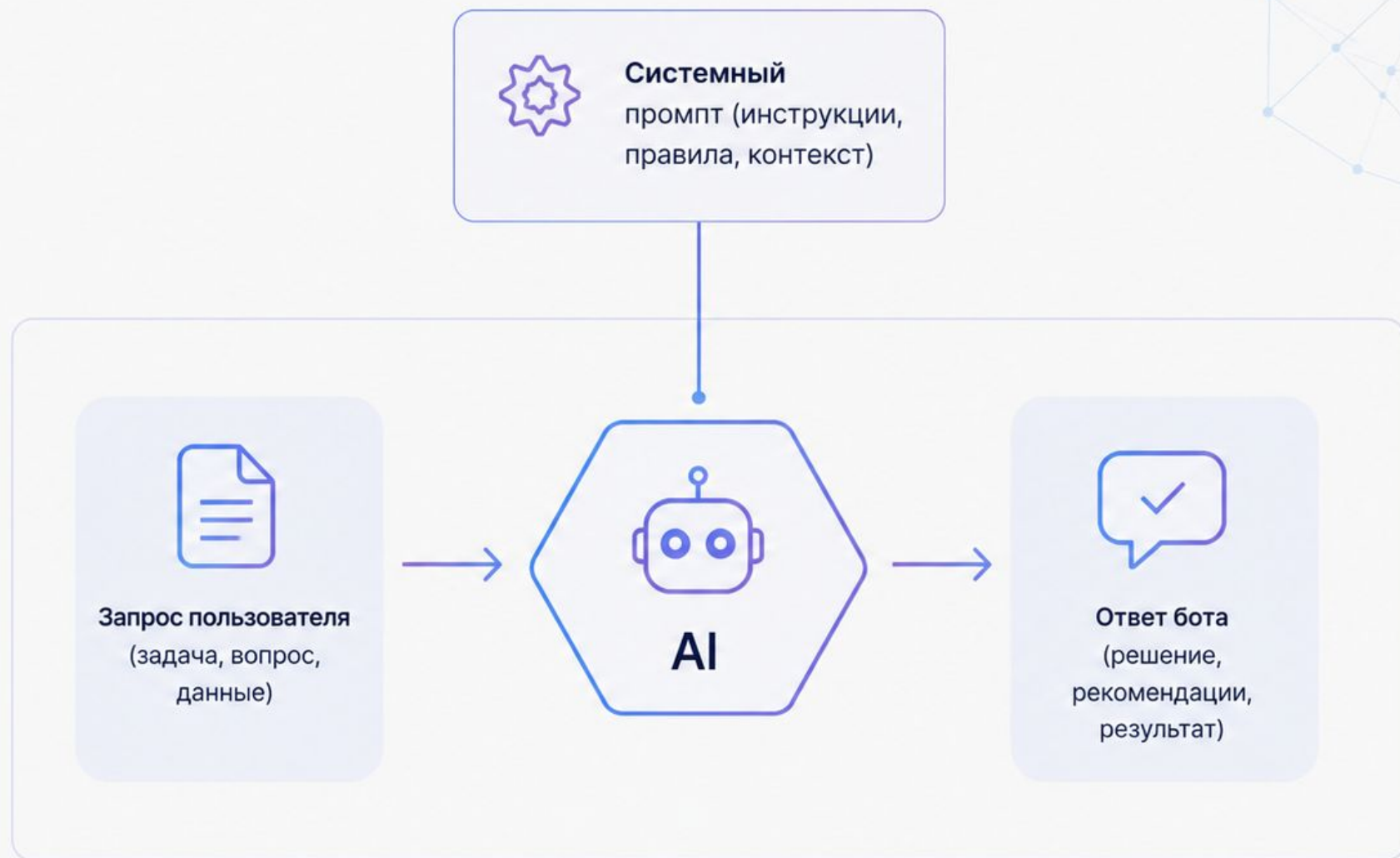
# Чат



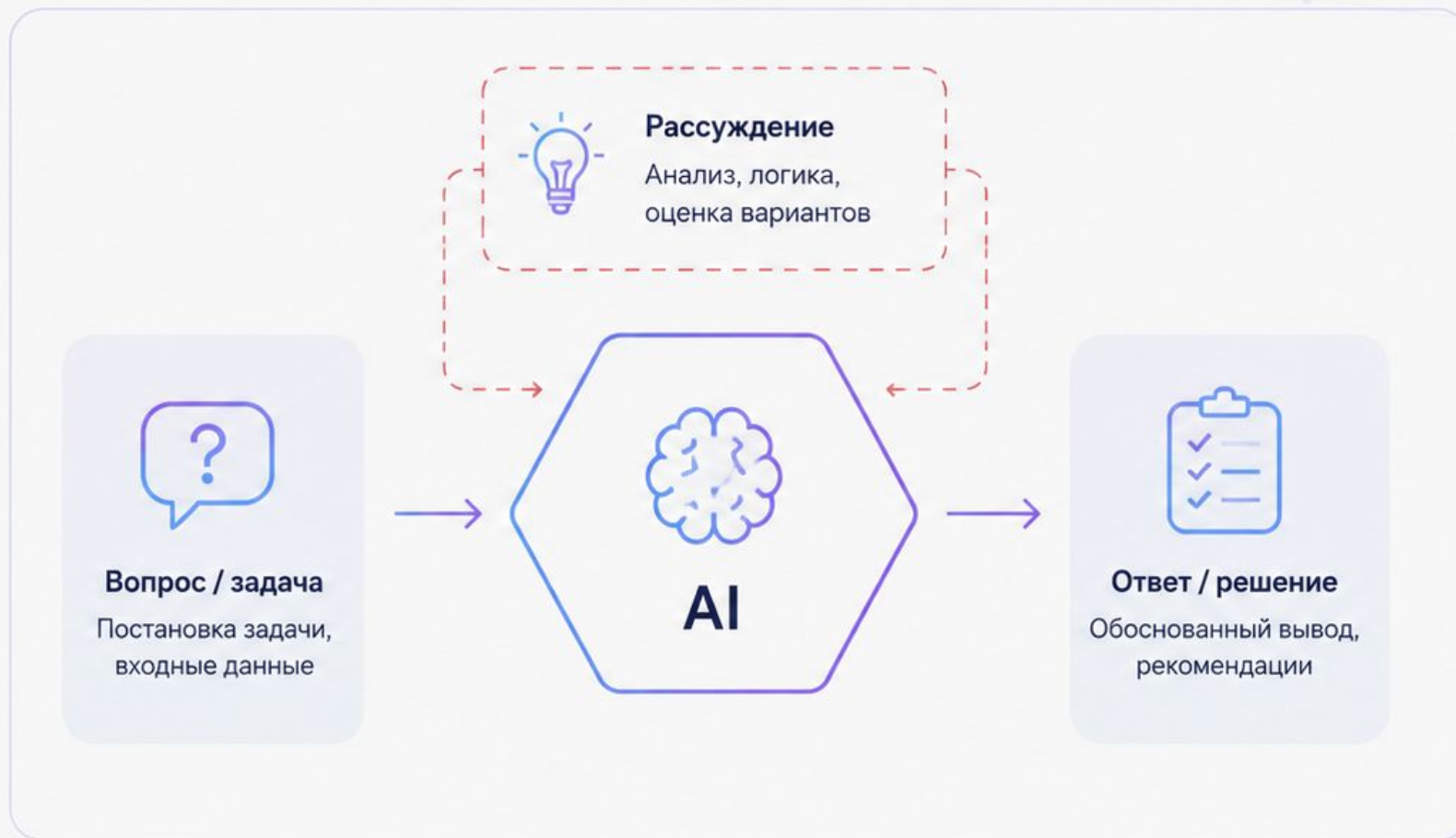
# Поиск



# Проект (бот)



# Рассуждающая модель



# Агенты

## Чат



получает запрос →  
анализирует →  
формирует ответ

## Агент



получает цель → сам определяет  
первый шаг → выполняет действие →  
оценивает результат → выбирает  
следующий шаг → продолжает цикл,  
пока задача не будет выполнена

# Структура агента



## Модель

Думает. Читает задачу и решает, какой шаг сделать следующим. Сама ничего не открывает и не запускает.



## Инструменты

Действуют. Прочитать файл, найти по папке, записать, запустить программу, открыть страницу.



## Обязка

Держит вместе. Выдаёт инструменты, крутит цикл, помнит сделанное, решает, когда остановиться.

Модель — та же самая, что в чате. Агентом её делают инструменты и обязка.

# Агенты



Создаются разработчиками



Строятся с использованием конструктора



Интегрируются с ИИ-сервисами



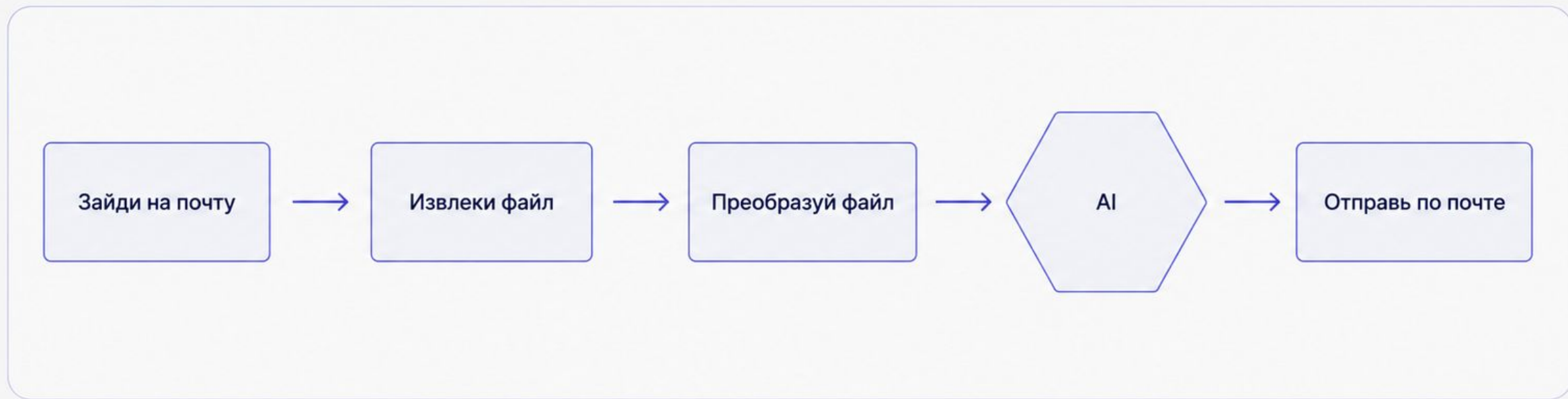
Доступны через веб-браузер



Работают на вашем устройстве



# Начало



# Сейчас



AI на каждом шаге сам определяет следующее действие, опираясь на результат предыдущего этапа

Маршрут гибкий: если что-то идет не по плану — AI перестраивает действия

# От чат-бота к агенту



## Прежний формат: чат-бот

Запрос → обработка → текст или файл в ответ. Возможности ограничены окном диалога.

## Новый формат: агент

Та же модель, но дополненная инструментами.

Самостоятельно открывает почту, документы, обращается к базам данных. Сама определяет, какой инструмент задействовать. Текст + Tools.

☐ Это принципиальный сдвиг. Чат-бот отвечал. Агент действует.

# Возможности агента



## Обрабатывать целые папки

Не отдельный документ в окне чата, а сразу все 100 PDF-файлов по делу.



## Решать задачу пошагово

Изучил, разобрал, отредактировал, сохранил. Ваше участие между этапами не требуется.



## Подключать субагентов

Задача дробится на параллельно идущие процессы.



## Действовать по графику

Открывает папку ежедневно в 09:00 и выполняет назначенную работу.



## Писать код

Как несложный, так и развернутый.



## Многоступенчатые задачи

По одному промпту разработать программу, сгенерировать множество файлов и совершить дополнительные действия.

# Почему это важно для юридической работы

Агентный ИИ снимает принципиальное ограничение обычных нейросетей: необходимость вручную готовить и передавать данные. Юрист больше не копирует текст из документа в чат — агент сам читает нужные файлы, находит релевантные фрагменты и работает с ними.



## Что это дает

Это открывает новые горизонты. Теперь вы можете сделать анализ десятков судебных решений за 25 минут по указанным вами параметрам, автоматически проверять десятки договоров по чек-листам.

# MD-файлы: новый стандарт работы



## 1. Создаете MD-файл

Простой текстовый документ  
в формате Markdown.  
Заполняется на обычном  
языке.



## 2. Помещаете в рабочую папку

Агент обнаруживает файл и  
просматривает его перед  
запуском каждой задачи.



## 3. Получаете стабильный результат

Настройка выполняется  
однократно - дальше агент  
действует строго по вашим  
правилам.

# Agents.md - единый стандарт для всех агентов



## Описание

Открытая спецификация.  
Поддерживается Codex,  
Claude Code, Cursor и  
другими агентами.

## Содержимое

Манера работы, требования  
к оформлению, перечень  
рабочих и неприкосновенных  
файлов, схема именования  
итоговых документов.

## Размещение

В корневой директории проекта. Один проект - один файл.

- ☒ Описываете в agents.md → переносится в любого агента.  
Один раз настроили - применяете в любом инструменте.

# Skill.md – отдельный навык агента

## Проверка документа

Чек-лист уязвимостей, режим внесения правок (Track Changes), оформление комментариев.

## Подготовка справки по образцу

Шаблон summary: к примеру, заключение по итогам комплаенс аудита.

## Оформление документа по шаблону

Заголовок, гарнитура, поля, нумерация, формат ссылок на нормативные акты.

- ☐ Один Skill.md = один типовый документ. Помещаете в папку – агент задействует его автоматически



# Инструменты — руки агента

Действия, которые агент умеет совершать.



## Примеры

- прочитать файл, найти нужное в папке
- записать файл, поправить документ
- запустить программу, собрать отчёт
- открыть страницу в интернете



## Что важно знать

- набор выдаёте вы — за его пределы агент не выйдет
- пятнадцать разных инструментов лучше десяти похожих: на похожих модель путается
- на необратимое действие — отдельное разрешение

# MCP - универсальный коннектор для любых сервисов



## В чем сложность

У каждого сервиса собственный API, свой формат и свой «язык». Чтобы связать нейросеть с десятью сервисами, нужно настроить десять отдельных интеграций.

## Что предлагается

MCP — открытая спецификация от Anthropic. Единый коннектор ко всему. Своего рода USB-C для ИИ.

- ☒ Сейчас MCP-сервер есть практически у всех – Notion, Github, Gmail, Google Drive. Список расширяется еженедельно.

# Какие MCP рекомендуется подключить

## Claude in Chrome

Позволяет анализировать НПА, реестры и веб-формы прямо в браузере — без копирования и переключения между вкладками



## Google Calendar

Автоматизация контроля сроков, расследований, обучения и регуляторных обязательств с помощью ИИ и системы напоминаний



## Google Drive и Gmail

Поиск документов и писем по ключевым словам прямо из чата.



## Gamma

Создание презентаций, документов, постов для соцсетей и сайтов с помощью ИИ.



## Zoom for Claude

Поиск по встречам Zoom, подготовка кратких итогов и выполнение действий по материалам встреч.

# Для чего это нужно в юридической работе

MCP превращает разрозненные корпоративные системы в единое рабочее пространство агента. Вместо того чтобы переключаться между интерфейсами и копировать данные вручную, агент сам забирает нужное из каждой системы.



## Практически это означает

агент может: получить задачу из системы управления проектами, открыть нужные документы из корпоративного хранилища, проверить историю переписки по делу, обратиться к базе нормативных актов, сформировать итоговый документ — все в рамках одной сессии.

# Плагины

Плагин — это пакет, который объединяет четыре компонента в одно решение под конкретную задачу:

- **Скиллы** — инструкции под конкретные задачи (анализ NDA, проверка персональных данных, подготовка стенограммы).
- **Команды** — slash-команды для удобного вызова скиллов: /legal:review-nda, /legal:check-pd.

- **Коннекторы** — MCP-интеграции с внешними сервисами: корпоративное хранилище документов, CRM, почта.
- **Субагенты** — параллельные исполнители для сложных задач, когда несколько подзадач можно выполнять одновременно.

# Безопасность: на чем можно обжечься

## Промпт-инъекции

В чужом MCP могут быть зашиты невидимые команды - модель отработает их без вашего ведома.

## Утечка данных

Сервер с правами на файловую систему способен незаметно скопировать ваши документы.

## Ransomware

В наихудшем сценарии - зашифрует папку и затребует выкуп.

## Незрелость технологии

Самописные серверы часто работают со сбоями. Особенно скачанные по ссылке от неизвестного «специалиста».

❗ Устанавливайте MCP только из GitHub проверенных разработчиков и с официальных ресурсов.

# Что делают юристы



Пакетно обрабатывают файлы

---



Подбирают судебную практику

---



Формируют позицию по спору

---



Проверяют договоры

---

# Первые шаги



## Claude

Агент внутри стандартного окна Claude. Стартовая площадка для тех, кто только пробует.



## Claude Code

Более функциональное решение, но требует чуть больше навыков.



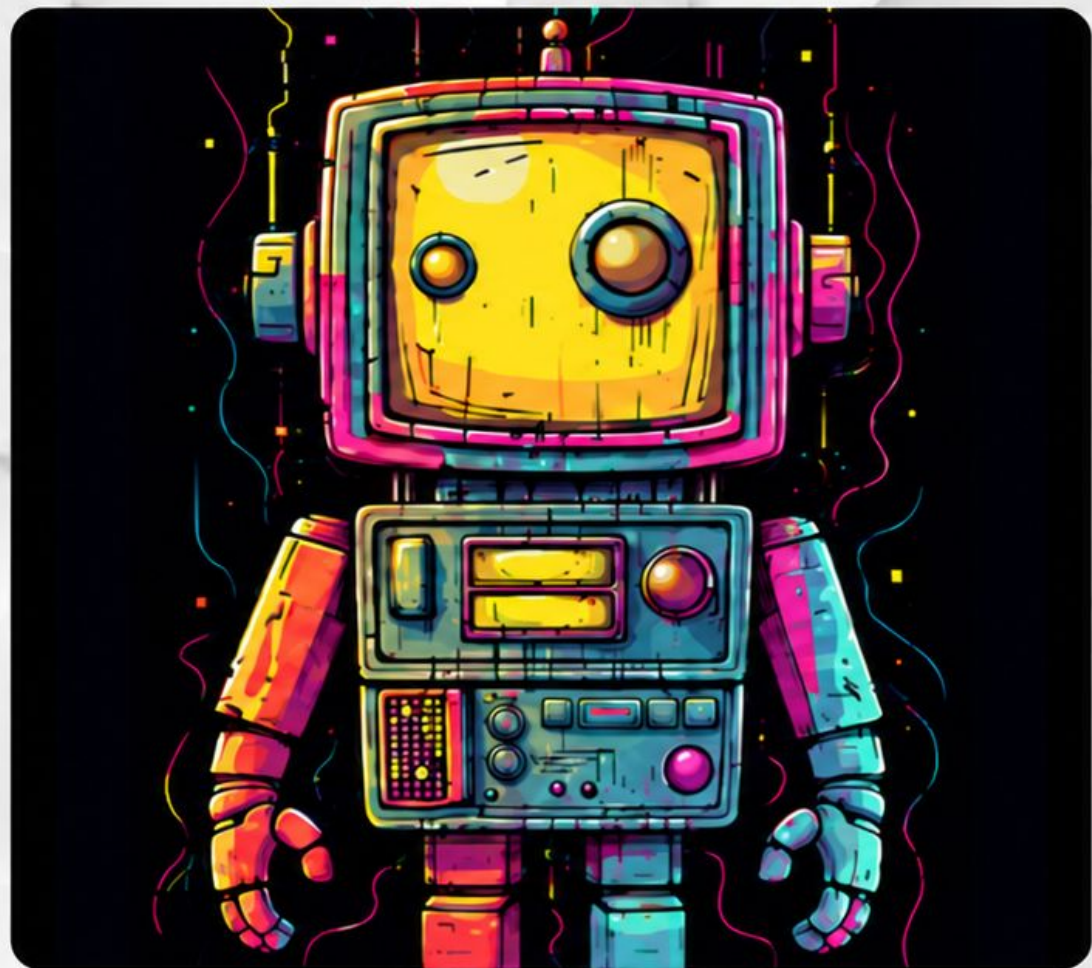
## ChatGPT Codex

Решение от Open AI по аналогичной схеме: агент, работа с файлами, пошаговое исполнение.



## ChatGPT Work (работа)

Рабочий режим для задач и проектов: лучше держит контекст, помогает работать с документами, структурировать шаги и доводить результат до готового вида.



# Claude и ChatGPT Work: точка входа в агентов

## Доступ к проектам

Создаете папку, заполняете ее файлами - агент работает со всем ее содержимым.

## Бережное расходование контекста

Берет из проекта только необходимое. Не загружает в чат сразу 100 PDF-файлов.

## Поэтапное выполнение

Сложная задача решается автономно. Можно отвлечься на кофе и вернуться к готовому результату.

## Субагенты и расписание

Главный агент распределяет части работы между помощниками. Запуск по графику.

# В каких случаях понадобится Code



## Claude Code

Имеет доступ ко всему компьютеру, а не к одной папке. Умеет все то же, что Coder, плюс целый набор дополнительных функций.

## OpenAI Codex

Аналогичный продукт от OpenAI. Удобный выбор для тех, кто уже подписан на платный GPT и не планирует переходить на Claude.

# Контакты

## Нурлан Даниев

Комплаенс-офицер  
РГП «Казаэронавигация»

Электронная почта:  
<mailto:daniyev.nurlan@gmail.com>



LinkedIn:

<https://www.linkedin.com/in/nurlan-daniev>



@NURLAND10



@AICOMPLIANCE