

МАРКЕТИНГОВЫЕ АГЕНТЫ

КАК СОЗДАТЬ КОМАНДУ
ИИ-АГЕНТОВ, КОТОРЫЕ РАБОТАЮТ
24/7, ПРИНОСЯТ КЛИЕНТОВ,
ПРОГНОЗИРУЮТ ТРЕНДЫ

НОВЫЕ
ТИПЫ АГЕНТОВ.
НОВЫЕ ВОЗМОЖНОСТИ.
НОВЫЙ УРОВЕНЬ
МАРКЕТИНГА.



ИИ-АГЕНТЫ
ПИШУТ КОНТЕНТ,
ВЕДУТ ПЕРЕПИСКИ,
ДЕЛАЮТ ПРОДАЖИ



ПЕРСОНАЛИЗАЦИЯ
КАЖДОМУ КЛИЕНТУ —
СВОЙ АГЕНТ



ЧАТ-БОТЫ
ОБЩАЮТСЯ,
ПРОДАЮТ,
УДЕРЖИВАЮТ



АНАЛИТИКА
ПРОГНОЗИРУЕТ
СПРОС И ТРЕНДЫ



РЕКЛАМА
ЗАПУСКАЕТ,
ТЕСТИРУЕТ,
МАСШТАБИРУЕТ

*Больше
клиентов,
больше
прибыли!*



СТРАТЕГИЯ
АГЕНТОВ



ИИ
В МАРКЕТИНГЕ



МАСШТАБИРОВАНИЕ
ПРОДАЖ



АВТОМАТИЗАЦИЯ
ПРОЦЕССОВ



УДОВЛЕТВОРЕННЫЕ
КЛИЕНТЫ

ПРАКТИЧЕСКОЕ РУКОВОДСТВО ДЛЯ ТЕХ, КТО ХОЧЕТ РЕКЛАМИРОВАТЬ САМ

Антон Аракчеев

Маркетинговые агенты

<https://litres.ru/74605913>

SelfPub; 2026

Аннотация

Маркетинг больше не ждёт, пока вы спросите. Он сам исследует рынок, запускает кампании, принимает решения и учится на результатах.

«Маркетинговые агенты» — практическое руководство по созданию автономных AI-систем, которые работают как полноценная команда. От Research до Analytics, от Content до Sales. Автор разбирает анатомию агента, цикл AI Marketing Agent Loop, пять уровней автономности и мультиагентные архитектуры. Показывает, как ставить цели, настраивать память, инструменты, guardrails и человеческий контроль — чтобы агент приносил пользу, а не риски.

Внутри: 60 готовых промптов, 30 рабочих шаблонов, сквозные кейсы из ритейла, B2B и услуг, пошаговый план запуска первого агента за 30 дней. Книга продолжает серию «Маркетинг» и опирается на «AI-отдел маркетинга».

Главный тезис: автономность — не самоцель. Цель — система, которая самостоятельно делает полезную работу, оставаясь управляемой, проверяемой и экономически оправданной.

Содержание

Введение. Когда AI начинает действовать	10
Почему генеративный AI был только первым этапом	13
Почему автоматизация ограничена заранее заданными сценариями	14
Почему агенты меняют архитектуру работы	16
Почему автономность создаёт новые риски	17
Почему агентная модель особенно важна для маркетинга	18
Главный вопрос книги	19
Как читать эту книгу	22
Что не является этой книгой	24
Терминологический словарь книги	25
AI-модель (LLM)	25
AI-ассистент	25
Workflow	26
AI-агент	26
Multi-Agent System (MAS)	27
Guardrails	27
Agent Constitution	27
AI Marketing Team	28
AI Marketing Agent Loop	28
Глава 1. От промптов к целям	29

Что нужно агенту: шесть обязательных элементов	31
1. Цель	31
2. Контекст	31
3. Ограничения	32
4. Критерий успеха	33
5. Доступные инструменты	33
6. Правила остановки	34
Чем цель отличается от задачи:	35
четырёхмерная модель	
Переход от промпта к цели: практический пример	37
Цель как контракт между человеком и машиной	39
Иерархия целей: от стратегии к операции	40
Ошибки формулирования цели	41
Глава 2. Чем агент отличается от автоматизации	43
Как работает workflow	44
Как работает агент	45
Сравнительная таблица	46
Когда workflow превращается в агента	48
Гибридная модель: workflow + агент	50
Границы workflow: где он перестаёт работать	52
Экономика выбора: workflow дешевле на старте, агент дешевле в развитии	53
Когда гибрид — лучший выбор	54

Глава 3. Где агент действительно нужен	55
Когда агент особенно полезен	56
Когда агент не нужен	58
Четыре вопроса для принятия решения	59
Матрица «вариативность × стоимость ошибки»	60
Типичные маркетинговые задачи и их соответствие	62
Зрелость команды как фактор выбора	66
Дорожная карта внедрения агентов	67
Сигналы, что агент нужен прямо сейчас	68
Скоринг задач на соответствие агенту	69
Альтернативы агенту: что ещё можно сделать	72
Глава 4. Память агента	73
Шесть слоёв памяти агента	74
1. Краткосрочный контекст	74
2. История взаимодействий	74
3. Долгосрочная память	75
4. База знаний	75
5. Клиентские данные	76
6. Результаты прошлых действий	76
Что хранить и зачем	77
Как обновлять, удалять и контролировать актуальность	79
Доступ к памяти: кто что может видеть	80
Векторная память: новый подход	82

Забывание: что удалять и когда	83
Конфиденциальность и память	84
Контекстное окно и его ограничения	85
Глава 5. Инструменты агента	87
Типовой набор инструментов маркетингового агента	88
CRM	88
Аналитика	88
Рекламные кабинеты	88
Поисковые системы и веб	89
Базы данных и таблицы	89
Email и мессенджеры	89
CMS и системы управления контентом	90
Системы управления задачами	90
BI и внешние API	90
Пять уровней прав доступа к инструментам	91
READ — только чтение	91
ANALYZE — обработка и анализ	91
WRITE — создание данных	92
EXECUTE — изменение состояния системы	92
TRANSACT — финансовые и высокорисковые действия	92
Почему права доступа должны увеличиваться постепенно	95
Tool Permission Matrix — матрица прав	96

доступа	
Аутентификация и управление ключами	100
Версионирование инструментов и обработка изменений API	101
Конец ознакомительного фрагмента.	102

Антон Аракчеев

Маркетинговые агенты

СЕРИЯ «МАРКЕТИНГ». КНИГА 9

Антон Аракчеев

Маркетинговые агенты

Как создавать автономные AI-системы, которые исследуют рынок, запускают маркетинг, принимают решения и постоянно улучшают результат

Антон Аракчеев

Маркетинговые агенты. Как создавать автономные AI-системы, которые исследуют рынок, запускают маркетинг, принимают решения и постоянно улучшают результат.

Девятая книга серии «Маркетинг».

Книга предназначена для маркетологов, предпринимателей, руководителей цифровых команд и всех, кто работает на стыке маркетинга и искусственного интеллекта.

© Антон Аракчеев, 2026

Аннотация

Маркетинг прошёл путь от одиночных AI-промптов к чат-ассистентам, от ассистентов — к автоматизированным сце-

нариям, а от них — к AI-агентам: системам, которые сами ставят подцели, выбирают инструменты, выполняют действия, оценивают результат и корректируют план.

Эта книга — практическое руководство по проектированию, запуску и контролю маркетинговых AI-агентов. Автор последовательно разбирает анатомию агента (память, инструменты, планировщик, исполнитель, оценка, guardrails), цикл AI Marketing Agent Loop, пять уровней автономности и семь ключевых типов агентов — от Research до Analytics. Особое внимание уделено мультиагентным архитектурам, экономике автономных систем, обработке ошибок и человеческому надзору.

Книга содержит более 60 готовых AI-промптов, 30 практических шаблонов, сквозные кейсы из ритейла, B2B и услуг, а также пошаговый план запуска первого маркетингового агента за 30 дней. Она продолжает серию «Маркетинг» и прямо опирается на восьмую книгу — «AI-отдел маркетинга».

Главный тезис автора: автономность — не цель сама по себе. Цель — создать систему, которая способна самостоятельно выполнять полезную работу, оставаясь управляемой, проверяемой и экономически оправданной.

Оглавление

Оглавление будет автоматически обновлено при открытии файла в Word (правая кнопка → «Обновить поле»).

Введение. Когда AI начинает действовать

CHAT → ASSISTANT → AUTOMATION → AGENT

Когда в конце 2022 года ChatGPT стал массовым явлением, маркетологи впервые получили инструмент, который понимает запросы на естественном языке и генерирует осмысленные ответы. Это был момент перехода от поиска к диалогу: вместо того чтобы подбирать ключевые слова и лишать ссылки, можно было задать вопрос и получить связный текст. Первая волна AI-маркетинга состояла в основном из переписывания того, что мы уже делали, — тексты, идеи, заголовки, сценарии, письма. Интеллект машины стал дешевле, но архитектура работы осталась прежней: человек ставит вопрос, машина отвечает, человек действует.

Вторая волна — AI-ассистенты — добавила контекст. Появились диалоги, в которых модель помнит предыдущие реплики, хранит инструкцию и может работать в рамках заданной роли. Ассистент перестал быть одноразовым генератором: он стал собеседником. Маркетологи научились готовить системные промпты, описывать бренд-голос, передавать данные о продукте и аудитории. Но принцип остался прежним: инициатива по-прежнему у человека. Машина отвечает на запрос, но не выполняет задачу до конца. Она

не открывает рекламный кабинет, не анализирует реальную статистику, не корректирует ставки, не отправляет письма и не обновляет CRM. Все эти действия по-прежнему делает человек, используя AI как интеллектуальный усилитель.

Третья волна — автоматизация — добавила сценариев. Появились инструменты, которые связывают AI-модель с внешними системами через API: CRM, рассылки, рекламные кабинеты, аналитика. На этой волне возникла идея AI-отдела маркетинга — предыдущая книга этой серии. AI-отдел подразумевает, что человек проектирует процессы, а AI выполняет их автоматически. Это уже не диалог и не консультация — это исполнение по заданному сценарию. Workflow запускается триггером, проходит заранее заданные шаги и завершается результатом. Архитектура понятная, контролируемая, но жёсткая: каждый шаг прописан человеком заранее, и любое отклонение от сценария требует вмешательства.

Четвёртая волна — AI-агенты — меняет архитектуру принципиально. Агент получает не инструкцию, а цель. Он сам определяет, какие данные нужны, какие инструменты использовать, в каком порядке действовать, как проверить результат и что делать, если что-то пошло не так. Это переход от «выполни шаги А, В, С» к «достигни результата Х, оставаясь в рамках правил Y». Машина впервые получает право не просто отвечать, но и действовать — выбирать следующее действие на основе наблюдаемого результата.

Этот переход меняет всё: и то, как устроена маркетинговая функция, и то, какую роль играет человек, и то, какие риски появляются. Если ассистент может ошибиться в тексте — это неприятно, но локально. Если агент ошибается в действии — он может потратить бюджет, разослать письмо не той аудитории, остановить работающую кампанию или, наоборот, запустить нежелательную. Поэтому автономность без контроля — не зрелая автоматизация, а дополнительный риск. Книга строится вокруг именно этой мысли: полезность агента определяется не его способностью действовать самостоятельно, а балансом между автономностью, контролем, ограничениями и измеримостью.

Почему генеративный AI был только первым этапом

Генеративные модели появились на стыке двух потребностей: дешёвой генерации контента и быстрого доступа к знаниям. Они решили обе задачи — но обнаружили пределы. Первый предел: текст не равен действию. Можно написать отличный рекламный текст, но если его некому опубликовать, протестировать, измерить и скорректировать — ценность ограничена. Второй предел: диалог требует человека. Каждый раз, когда нужно новое действие, человек возвращается в цикл. AI работает только тогда, когда его спрашивают. Третий предел: нет обратной связи. Модель не знает, сработал ли её предыдущий ответ, и не может изменить поведение на основе реального результата.

Эти три предела — отсутствие действия, необходимость человека в каждом цикле и отсутствие обратной связи — и объясняют, почему следующая стадия развития AI неизбежна. Агенты убирают все три ограничения: они могут действовать через инструменты, выполняют последовательность действий без постоянного участия человека и наблюдают результат, чтобы скорректировать план. Это не «более умный чат», а принципиально другая архитектура взаимодействия с AI.

Почему автоматизация ограничена заранее заданными сценариями

Классическая автоматизация — это набор шагов $A \rightarrow B \rightarrow C \rightarrow D$, прописанных заранее. Каждый переход задан условием: если X , то Y . Это работает, пока мир ведёт себя предсказуемо. Но маркетинг по своей природе вариативен: один и тот же рекламный креатив может сработать на одной аудитории и провалиться на другой; одна и та же тема письма может дать открытость 40% в одной рассылке и 12% в другой; один и тот же сегмент может реагировать по-разному в зависимости от дня недели, погоды, контекста конкурентов.

Workflow в таких условиях либо становится слишком простым (и тогда он не решает задачу), либо слишком сложным (и тогда его невозможно поддерживать). На практике большинство автоматизированных сценариев в маркетинге покрывает лишь 60–70% реальных ситуаций; остальное обрабатывается вручную. Это нормально для повторяющихся операций, но не подходит для задач, где путь к результату заранее неизвестен.

Агент отличается тем, что ему не нужно знать весь путь заранее. Он знает цель, ограничения и набор доступных инструментов. Конкретную последовательность действий он определяет сам — на основе наблюдаемого контекста и результата предыдущих шагов. Это не отменяет автомати-

зацию: workflow остаётся оптимальным инструментом для предсказуемых процессов. Агент нужен там, где путь зависит от того, что произойдёт по дороге.

Почему агенты меняют архитектуру работы

Архитектура маркетинговой работы с AI-агентами меняется в трёх измерениях. Первое — источник инициативы. Раньше человек ставил задачу на каждом шаге. Теперь он ставит цель один раз, а агент сам решает, какие подзадачи нужно выполнить. Второе — связь между шагами. Раньше переходы были жёсткими. Теперь они определяются результатом предыдущего действия: агент может попробовать вариант А, увидеть, что он не сработал, и перейти к варианту В. Третье — обратная связь. Раньше результат шага фиксировался в CRM или дашборде, но не влиял на поведение системы. Теперь результат шага становится частью контекста агента и напрямую влияет на следующие действия.

Эти изменения требуют новых инструментов, новых метрик и новых правил. Инструменты — потому что агенту нужен доступ к реальным системам (CRM, рекламные кабинеты, аналитика). Метрики — потому что оценивать надо не качество ответа модели, а достижение бизнес-цели. Правила — потому что действие без ограничений становится риском. Всё это подробно разбирается в книге.

Почему автономность создаёт новые риски

Любое действие в маркетинге имеет последствия: финансовые (бюджет), репутационные (восприятие бренда), правовые (обработка персональных данных), операционные (нагрузка на смежные команды). Когда действие выполняет человек, он в каждый момент удерживает контекст и может остановиться. Когда действие выполняет агент, контекстом управляют правила, заложенные в систему. Если правила неполны, агент может выполнить действие, которое в моменте кажется логичным, но в итоге ведёт к потерям.

Основные категории риска: неверная интерпретация данных (агент делает вывод на основе неполной или устаревшей информации), ошибочный план (агент выбирает стратегию, которая не приводит к цели), конфликт инструментов (агент использует инструмент не по назначению), бесконечный цикл (агент повторяет одно и то же действие, не приближаясь к цели), превышение лимитов (агент тратит больше бюджета, чем предполагалось), утечка данных (агент передаёт чувствительную информацию во внешнюю модель), *prompt injection* (внешний контент, который агент читает, содержит инструкции, меняющие его поведение). Каждый из этих рисков требует отдельного контроля — и каждая глава книги затрагивает те или иные механизмы защиты.

Почему агентная модель особенно важна для маркетинга

Маркетинг — одна из тех функций, где агентная модель раскрывается полнее всего. Причины структурные. Во-первых, маркетинг работает с большим количеством повторяющихся циклов: кампания → анализ → корректировка → новая кампания. Во-вторых, у маркетинга есть измеримый результат: конверсии, стоимость лида, ROAS, CAC, LTV. Это даёт агенту чёткий критерий успеха. В-третьих, маркетинг использует много инструментов, доступных через API: CRM, рекламные кабинеты, системы аналитики, рассылки. Это даёт агенту поле для действий. В-четвёртых, маркетинг работает в условиях постоянных изменений — рынка, конкурентов, поведения потребителей. Это делает жёсткие автоматизированные сценарии быстро устаревающими и создаёт нишу для адаптивных систем.

Вместе эти четыре фактора делают маркетинг идеальным полигоном для агентной модели. Но они же создают и основные ограничения: бюджетные риски (рекламные расходы), репутационные риски (публичный контент), правовые риски (персональные данные клиентов). Поэтому маркетинговый агент — это всегда баланс между полезностью автономии и строгостью контроля. Эта книга — попытка дать практический инструментарий для этого баланса.

Главный вопрос книги

Что произойдёт, если маркетинговая система сможет не только анализировать ситуацию, но и самостоятельно действовать?

Этот вопрос — отправная точка всей книги. Ответ на него не сводится к технологии. Он касается того, как изменится работа маркетолога, какие новые роли появятся, какие навыки станут ключевыми, как будет устроен процесс принятия решений и какой уровень контроля сохранит человек. Книга пытается дать практические ответы: какие агенты существуют, как их проектировать, какие инструменты им нужны, как формировать ограничения, как тестировать и оценивать, как считать экономику, как избегать типичных ошибок.

Книга не обещает футурологического сценария, в котором «через год маркетологи исчезнут». Часть операций действительно может перейти к AI-системам — особенно те, что связаны со сбором данных, формированием гипотез, рутинной корректировкой кампаний, формированием отчётов. Но роль специалиста сместится в сторону постановки целей, проектирования систем, контроля, архитектуры и стратегических решений. Это не конец профессии, а её переосмысление. И язык этой переоценки — язык агентов, циклов, инструментов, ограничений и метрик.

Книга построена вокруг простой формулы: цель → план

→ инструменты → действие → наблюдение → оценка → коррекция → результат. Введении даёт общий контекст. Часть I объясняет, почему агент — это новая парадигма. Часть II разбирает анатомию агента. Часть III описывает семь ключевых типов маркетинговых агентов. Часть IV показывает, как они объединяются в мультиагентную систему. Часть V посвящена автономности, контролю, экономике и практическому плану запуска. В приложениях — 60 готовых промптов и 30 шаблонов для проектирования агентов. Книга построена так, чтобы её можно было читать последовательно или использовать как справочник по конкретным вопросам.

Сквозной кейс: введение

В книге используется несколько сквозных кейсов из разных ниш. Основной — условный российский интернет-магазин товаров для дома «ДомДеко» (ритейл, D2C, средний чек 4 800 #, ~120 000 клиентов в базе). Дополнительные: B2B-сервис аналитики для маркетплейсов «МетрикаПро» (SaaS, длинный цикл сделки, 4 000 активных аккаунтов) и сеть городских кулинарных студий «Вкуснотех» (офлайн-услуги, бронирование, ~30 000 клиентов в год).

Все цифры условные и приведены исключительно для иллюстрации. В каждом кейсе мы будем показывать, как конкретный агент встраивается в существующую инфраструктуру (CRM, рекламные кабинеты, аналитика, сайт), какие права ему выдаются, какие ограничения ставятся и какие KPI отслеживаются. Это позволит увидеть разницу между аген-

тами в разных контекстах: ритейл, B2B и услуги требуют разных уровней автономии, разной скорости реакции и разной глубины человеческого контроля.

Как читать эту книгу

Книга построена так, чтобы её можно было читать двумя способами. Первый — последовательно, от введения до приложений. Это даёт полное понимание архитектуры маркетинговых агентов — от базовой идеи до практического запуска. Второй — как справочник: открыть конкретную главу по мере необходимости. Например, если вы проектируете первого агента — откройте главы 4 (память), 5 (инструменты), 6 (планирование) и 15 (guardrails). Если вас интересует конкретный тип агента — главы 7 (Research), 8 (Content), 9 (Advertising) и т. д. Если экономика — главу 17. Приложения А (промпты) и Б (шаблоны) — для прямого практического применения: берите готовые формы и адаптируйте под свой контекст.

Книга содержит три сквозных кейса из разных ниш: «Дом-Деко» (ритейл товаров для дома, D2C), «МетрикаПро» (B2B SaaS для аналитики маркетплейсов, длинный цикл сделки) и «Вкуснотех» (офлайн-услуги, сеть кулинарных студий). Эти кейсы показывают, как одни и те же принципы агентной архитектуры применяются в радикально разных контекстах: разные средние чеки, разные циклы сделки, разные риски, разные каналы. Цифры во всех кейсах условные и приведены исключительно для иллюстрации логики.

В книге сознательно используются текстовые ASCII-схе-

мы вместо графических. Это сделано по трём причинам. Во-первых, текстовые схемы универсально читаются в любом редакторе и электронной книге, не требуют рендеринга изображений и не нарушают поток чтения. Во-вторых, они принуждают к простоте: нельзя нарисовать сложную схему в ASCII — приходится выделять самое важное. В-третьих, они легко копируются: если вы захотите использовать схему в своей работе, скопируете и вставьте в свой документ без потери качества.

Что не является этой книгой

Важно явно зафиксировать, чего эта книга не делает. Это не обзор AI-инструментов: здесь нет каталогов «10 лучших AI-сервисов для маркетинга» и сравнений тарифов конкретных платформ. Технологии меняются быстро, и любой такой обзор устаревает за квартал. Книга сосредоточена на принципах, архитектуре и подходах, которые остаются устойчивыми. Это не курс по программированию: здесь нет фрагментов кода на Python или JavaScript, которые можно скопировать и запустить. Книга описывает, что нужно построить, а не как именно писать код. Это не юридический справочник: вопросы обработки персональных данных, согласий и compliance упоминаются, но конкретные правовые требования нужно сверять с актуальной нормативной базой и консультациями юристов.

Также книга не обещает мгновенных результатов. Маркетинговый агент — это не «волшебная кнопка», после нажатия которой выручка вырастет в пять раз. Это инструмент, который требует проектирования, настройки, тестирования, эксплуатации и постепенного совершенствования. Книга даёт методологию, а не заклинание. Реалистичный горизонт внедрения — 3-12 месяцев до первой стабильной системы, 12-24 месяца до полноценной AI Marketing Team. Это не быстро, но это реалистично.

Терминологический словарь книги

Чтобы избежать разночтений, здесь собраны ключевые термины, используемые в книге. Понимание этих терминов в нашем контексте поможет читать книгу без путаницы, особенно если вы знакомы с близкими, но не идентичными определениями из других источников.

AI-модель (LLM)

Большая языковая модель, лежащая в основе интеллекта агента. Сама по себе модель не является агентом — это только «интеллектуальное ядро», способное генерировать тексты и делать выводы. Модель не имеет ни памяти, ни инструментов, ни цели — всё это добавляется архитектурой агента. Когда мы говорим «агент на базе GPT-4o», мы имеем в виду, что ядром агента является модель GPT-4o, но вокруг неё построена система, превращающая модель в действующего агента.

AI-ассистент

AI-система, которая помогает человеку, но не действует автономно. Ассистент отвечает на вопросы, генерирует тексты, предлагает варианты — но человек принимает финаль-

ное решение и выполняет действие. ChatGPT в его базовом использовании — это ассистент. Ассистенты могут иметь контекст (история диалога, настройки, документы), но не имеют инструментов для действий во внешних системах.

Workflow

Заранее описанная последовательность шагов для выполнения задачи. Workflow имеет фиксированную структуру: шаг A $\rightarrow$ шаг B $\rightarrow$ шаг C, с условиями ветвления. Изменения в workflow вносятся разработчиком вручную. Workflow оптимален для повторяющихся, предсказуемых процессов. Workflow не умеет адаптироваться к ситуациям, не предусмотренным в коде.

AI-агент

Система на базе AI-модели, которая получает цель, использует контекст и инструменты, выполняет последовательность действий, оценивает результаты и корректирует своё поведение в рамках заданных полномочий и ограничений. Агент отличается от ассистента наличием инструментов и действий; от workflow — способностью выбирать следующий шаг на основе результатов предыдущих.

Multi-Agent System (MAS)

Архитектура, в которой несколько агентов с разными целями и инструментами взаимодействуют между собой для достижения общей цели системы. MAS отличается от набора независимых агентов наличием координации: либо центральной (Supervisor), либо распределённой (Pipeline, Collaborative).

Guardrails

Явно заданные правила, в рамках которых агент может действовать. Включают допустимые и запрещённые действия, лимиты (бюджет, количество операций, скорость), условия остановки, правила эскалации. Guardrails — основа безопасной эксплуатации агента.

Agent Constitution

Документ, объединяющий все guardrails конкретного агента: цель, полномочия, запреты, критерии успеха и остановки, лимиты, правила эскалации, ответственных. Конституция — это «закон» агента, который технически контролирует его действия.

AI Marketing Team

Зрелая форма MAS, в которой агенты играют роли, аналогичные ролям в реальном отделе маркетинга: директор, исследователь, стратег, контент-мейкер, медийщик, CRM-менеджер, sales, аналитик, оптимизатор. AI Marketing Team — это не «набор ботов», а система с общей целью, единым контекстом и правилами взаимодействия.

AI Marketing Agent Loop

Базовый цикл работы агента: GOAL → CONTEXT → PLAN → TOOLS → ACTION → OBSERVE → EVALUATE → REFLECT → ADJUST → ACTION (повтор) → RESULT → LEARNING. Этот цикл — структурная основа всех агентов в книге, независимо от их типа и сложности.

Глава 1. От промптов к целям

PROMPT → *TASK* → *GOAL*

Промпт — это запрос к модели. Задача — это запрос к исполнителю. Цель — это желаемый результат. Три слова, которые кажутся синонимами, на самом деле описывают три разных уровня взаимодействия с AI. Понимание этой разницы — первый шаг к пониманию того, что такое агент и зачем он нужен.

Промпт: «Напиши рекламный текст для летней распродажи товаров для дома». Модель генерирует текст. Человек публикует его, запускает кампанию, ждёт результат, оценивает. Если текст не сработал — человек пишет новый промпт, и цикл повторяется. Это уровень, на котором большинство маркетологов всё ещё работают с AI.

Задача: «Подготовь три варианта рекламного текста для летней распродажи, протестируй их в рамках бюджета 50 000 # на двух аудиториях, определи победителя по CTR и стоимости клика, составь отчёт с рекомендацией по масштабированию». Здесь уже есть последовательность шагов, есть бюджет, есть критерий выбора, есть результат, который можно передать дальше. Но последовательность всё ещё задаёт человек.

Цель: «Приведи 500 квалифицированных лидов в категории товары для дома за июль при бюджете до 400 000 #,

используя разрешённые каналы (Яндекс Директ, VK Реклама, email по существующей базе), отслеживая стоимость лида и предлагая изменения при отклонении от KPI свыше 15%». Это уже цель в агентном смысле: есть желаемый результат, есть ограничение по бюджету, есть разрешённые каналы, есть критерий успеха, есть правило, когда агент должен вмешаться и предложить изменения. Дальше — агент сам решает, какие креативы сделать, как распределить бюджет между каналами, какие аудитории тестировать, когда остановить неэффективные кампании и как переопределить бюджет.

Что нужно агенту: шесть обязательных элементов

Промпт работает в условиях: модель знает только то, что в неё вложили в момент запроса. Агент работает в условиях: у него есть контекст, который не нужно каждый раз передавать заново, и инструменты, через которые он может добывать недостающую информацию и выполнять действия. Чтобы агент функционировал, ему нужны шесть обязательных элементов.

1. Цель

Цель — это желаемый результат, описанный измеримо. «Увеличь продажи» — не цель, а направление. «Доведите количество квалифицированных лидов до 500 в месяц при САС не выше 2 400 #» — цель. Хорошая цель отвечает на вопросы: что должно измениться, в какой срок, в каком объёме, с какими ограничениями по качеству или стоимости. Без измеримой цели агент не сможет оценить, достигнут ли результат, и не сможет решить, когда остановиться.

2. Контекст

Контекст — это информация, которая нужна агенту для

принятия решений. Сюда входят: данные о продукте (что продаём, по какой цене, какие особенности), данные об аудитории (кто целевая группа, какие сегменты, какие боли), данные о рынке (кто конкуренты, какие цены, какие каналы), исторические данные (что пробовали раньше, что сработало, что нет), текущее состояние (какие кампании активны, какие результаты показывают). Контекст может быть статическим (бренд-бук, описание продукта) и динамическим (статистика кампаний за последние 30 дней). Чем богаче контекст, тем точнее решения агента.

3. Ограничения

Ограничения — это правила, в рамках которых агент действует. Бюджетные лимиты (не более 50 000 # в день). Канальные ограничения (только Яндекс Директ и VK, без Telegram Ads). Временные ограничения (не запускать кампании в выходные). Контентные ограничения (без упоминания конкурентов, без обещаний скидок свыше 15%). Правовые ограничения (не использовать персональные данные без согласия). Ограничения — это «забор», внутри которого агент может свободно выбирать действия. Без ограничений агент либо рискует выйти за пределы дозволенного, либо становится слишком осторожным и не действует.

4. Критерий успеха

Критерий успеха — это измеримое условие, при выполнении которого задача считается выполненной. «500 лидов при $SAC \leq 2\,400$ #». «Увеличение конверсии лендинга на 20% за 4 недели». «Снижение доли корзин без оплаты до 8%». Без критерия успеха агент не знает, достигнут ли результат, и не может решить, нужно ли повторять цикл или можно остановиться. Критерий должен быть измеримым, привязанным ко времени и достижимым при разумных действиях.

5. Доступные инструменты

Инструменты — это интерфейсы, через которые агент читает данные и выполняет действия. CRM (чтение клиентов, обновление статусов), рекламные кабинеты (создание кампаний, корректировка ставок, остановка групп), системы аналитики (просмотр конверсий, воронок, источников трафика), рассылки (отправка писем, сегментация базы), CMS (публикация контента на сайте), поисковые системы (мониторинг видимости), внешние источники (новости рынка, отзывы). Список инструментов определяет, что агент может делать физически. Чем больше инструментов подключено, тем шире пространство возможных действий — и тем выше требования к контролю прав доступа.

6. Правила остановки

Правила остановки — это условия, при которых агент прекращает текущий цикл и возвращает управление человеку. Достигнут критерий успеха. Превышен бюджет. Достигнут лимит количества итераций. Зафиксирована аномалия (CTR резко упал, стоимость клика резко выросла). Обнаружено нарушение ограничений. Истекло время, отведённое на задачу. Без правил остановки агент может работать бесконечно, тратя ресурсы без продвижения к цели. Правила остановки — это техническая реализация здравого смысла: «если что-то идёт не так — остановись и спроси».

Чем цель отличается от задачи: четырёхмерная модель

Полезно различать цель и задачу по четырём параметрам: уровень абстракции, горизонт, мера успеха, степень свободы действий. Задача обычно описывает конкретное действие в коротком горизонте с понятной мерой успеха и небольшой свободой действий. Цель описывает желаемое состояние в более длинном горизонте, с многофакторной мерой успеха и большой свободой действий.

Параметр
Задача
Цель
Уровень абстракции
Действие
Результат
Горизонт
Дни/недели
Недели/месяцы
Мера успеха
Один показатель

Несколько КРІ

Свобода действий

Низкая (заданы шаги)

Высокая (агент выбирает путь)

Контроль

Пошаговый

По####ам

Эта модель — не теоретическая классификация, а практический инструмент. Если вы формулируете запрос к AI как задачу — вам нужен workflow, а не агент. Если как цель — вам нужен агент. Смешение этих уровней — одна из самых распространённых ошибок при внедрении AI в маркетинге: пытаются построить агента там, где нужен workflow, или пишут workflow там, где нужна агентная архитектура.

Переход от промпта к цели: практический пример

Рассмотрим эволюцию одного и того же запроса. Уровень 1 (промпт): «Напиши email для возврата брошенных корзин». Уровень 2 (задача): «Подготовь серию из трёх писем для возврата брошенных корзин, сегментируй базу по давности брошенной корзины (1 час / 24 часа / 72 часа), напиши разные варианты под каждый сегмент, передай готовые тексты и предложения по времени отправки». Уровень 3 (цель): «Снизь долю брошенных корзин, не дошедших до оплаты, с 23% до 17% за 8 недель, работая с сегментами по давности, типу товаров и сумме корзины, используя email и динамические push-уведомления на сайте; бюджет на скидки — не более 180 000 # за период; если за две недели прогресс меньше 15% от цели — предложи пересмотр стратегии».

Разница не в количестве слов. Разница в том, что на уровне 3 исполнитель сам решает, сколько вариантов писем написать, как сегментировать базу, какие скидки предлагать, какие триггеры ставить, как тестировать и когда менять стратегию. Это уже не «помоги мне сделать X», а «сделай X, оставаясь в рамках Y». Этот переход и есть суть агентной модели в маркетинге.

Сквозной кейс: «ДомДеко» — формулировка цели для CRM-агента

Цель: в течение 60 дней снизить долю «зависших» лидов в CRM (статус «в работе» без активности более 14 дней) с 32% до 22% от общего числа активных лидов.

Контекст: текущая база 28 000 активных лидов; средний цикл сделки 18 дней; основные каналы привлечения — Яндекс Директ, VK, органика; 4 менеджера по продажам; в CRM есть поля «последняя активность», «сумма потенциальной сделки», «источник», «категория интереса».

Ограничения: не отправлять более одного автоматического письма в неделю одному контакту; не предлагать скидку выше 10% без подтверждения менеджера; не звонить клиентам без согласия; работать только с сегментом B2C (без корпоративных клиентов).

Критерий успеха: доля зависших лидов $\leq 22\%$ на 60-й день; плюс — рост конверсии в продажу на 4 процентных пункта.

Доступные инструменты: чтение и обновление CRM; отправка email через рассылщик; создание задач менеджерам; аналитика по сегментам.

Правила остановки: если за 2 недели доля зависших лидов не снизилась — приостановить и передать отчёт руководителю продаж; если количество жалоб на спам превысит 0,5% — немедленно остановить все автоматические отправки.

Цель как контракт между человеком и машиной

Полезно рассматривать формулировку цели не как текстовое описание, а как контракт между человеком и машиной. Контракт — это обещание: человек обещает, что если агент достигнет цели, оставаясь в ограничениях, его работа будет считаться успешной. Агент обещает прилагать разумные усилия для достижения цели, не нарушая ограничений. Этот взгляд снимает много проблем. Если цель сформулирована нечётко, контракт не заключён — и агент не понимает, что именно он обещал. Если ограничения слишком жёсткие, контракт невыполним — и агент будет работать только в режиме «безопасных рекомендаций». Если критерий успеха измерим, но нереалистичен, контракт нарушен с самого начала — и агент будет тратить ресурсы впустую.

Контрактный взгляд на цель полезен ещё и тем, что он требует явных границ. Если цель «увеличь продажи» — контракт разорван, потому что нет границы: насколько увеличить, за какой срок, при каком бюджете, с какими ограничениями. Если цель «увеличь продажи на 15% за квартал при бюджете до 1,2 млн #, не снижая маржинальность ниже 22%» — контракт заключён. Каждое слово в этой формулировке — обязательно. Уберите любое — и контракт теряет определённость.

Иерархия целей: от стратегии к операции

В реальном бизнесе цель редко существует одна. Обычно есть иерархия: стратегическая цель (3-12 месяцев) → оперативная цель (1-4 недели) → тактическая цель (1-7 дней). Агент обычно работает на тактическом уровне, но должен «видеть» стратегический контекст. Например, CRM-агент на тактическом уровне снижает долю зависших лидов, но его работа осмысленна только в контексте стратегической цели — роста выручки от базы. Без этого контекста агент может оптимизировать свою тактическую метрику в ущерб стратегической: например, агрессивно «закрывать» лиды в статус «не актуально», что снижает долю зависших, но лишает бизнес потенциальных клиентов, которые могли бы вернуться через месяц.

Поэтому при проектировании агента важно явно связать его тактическую цель со стратегической. Это делается через метрики: тактическая метрика агента (доля зависших лидов) должна коррелировать со стратегической метрикой (выручка от базы). Если корреляция нарушается — значит, либо агент оптимизирует не ту метрику, либо стратегическая метрика зависит от других факторов, которые вне зоны агента. Оба случая требуют пересмотра архитектуры.

Ошибки формулирования цели

Большинство неудач с агентами начинается не с плохой реализации, а с плохой формулировки цели. Типичные ошибки: «улучшить» без числа, «увеличить» без срока, «оптимизировать» без критерия, «расширить» без границ. Все эти формулировки звучат осмысленно, но не дают агенту измеримого критерия успеха. Не менее распространённая ошибка — цель, у которой нет обратной связи. «Повышая лояльность клиентов» — но как именно мы узнаем, что лояльность повысилась? Если метрика не определена, цель не работает. Третья частая ошибка — конфликтующие цели: «увеличь продажи и снизь бюджет на маркетинг» может быть невыполнимым, если текущий ROI уже на пределе.

Чтобы избежать этих ошибок, используйте чеклист при формулировании цели: есть ли число? есть ли срок? есть ли ограничения? есть ли измеримый критерий успеха? есть ли способ проверить прогресс? есть ли обратная связь (как мы узнаем, что близки к цели)? если достигнем цели — будет ли это значить, что бизнесу стало лучше? Если на все вопросы ответ «да» — цель готова к агенту. Если хотя бы на один ответ «нет» — дорабатывайте формулировку, пока все ответы не станут утвердительными.

Сквозной кейс: «МетрикаПро» — формулировка стратегической цели

Бизнес-цель: удвоить количество активных аккаунтов SaaS-сервиса с 4 000 до 8 000 за 12 месяцев.

Стратегические рычаги: (1) увеличение притока новых лидов; (2) повышение конверсии из лида в активацию; (3) снижение оттока существующих клиентов.

Подцели для агентов: Research-агент — отслеживать изменения на рынке маркетинговой аналитики и выявлять новые сегменты; Content-агент — увеличить органический трафик на 30% через контент-маркетинг; Sales-агент — поднять конверсию из лида в демо с 38% до 55%; CRM-агент — снизить отток существующих клиентов с 5,2% до 3,8% в месяц.

Каждая подцель связана с измеримой метрикой и сроком. Каждая привязана к стратегической цели через явную модель: например, рост конверсии с 38% до 55% при неизменном потоке лидов даёт +44% новых активаций.

Контракт между бизнесом и командой агентов: если все четыре подцели достигнуты, суммарный эффект даст ~75-80% прироста активных аккаунтов за 12 месяцев (не 100% — потому что есть взаимные влияния, сезонность и внешние факторы). Это реалистичный контракт, который учитывает, что мир неидеален.

Глава 2. Чем агент отличается от автоматизации

WORKFLOW = A → B → C → D AGENT = A → B → ЕСЛИ X → C → ЕСЛИ Y → D → ПОВТОР

Workflow и агент — это два разных способа организовать выполнение задач. Workflow заранее описывает путь. Агент описывает цель и правила, а путь определяет сам. На первый взгляд разница кажется небольшой, но архитектурно и практически это два разных мира.

Как работает workflow

Классический workflow — это направленный граф шагов. Каждый шаг — это либо действие, либо условие. Действие: «отправить письмо», «создать задачу в CRM», «обновить статус». Условие: «если сумма корзины больше 5 000 #, перейти на шаг А; иначе — на шаг В». Путь от старта к финишу прописан полностью; любые отклонения — это новые ветки, которые тоже нужно прописать заранее. Это даёт две ключевые особенности. Первая: workflow полностью предсказуем — что произойдёт, можно прочитать в его коде. Вторая: workflow полностью негибок — все возможные сценарии должны быть заданы разработчиком.

В маркетинге workflow идеально подходит для таких задач: отправка приветственной серии новому подписчику; активация клиентов, не делавших покупку более 90 дней; еженедельная рассылка дайджеста; постановка задачи менеджеру при достижении лидом определённого скоринга; отправка подтверждения заказа. Все эти процессы имеют фиксированные шаги, понятные триггеры и предсказуемые результаты.

Как работает агент

Агент не имеет заранее прописанного пути от старта к финишу. У него есть цель, набор доступных действий, правила оценки результата и условия остановки. На каждом шаге он выбирает следующее действие на основе текущего состояния. Это может быть простая стратегия: «если текущая конверсия ниже целевой, попробуй новый креатив; если выше — масштабируй текущий». Или сложная: «анализируй весь набор метрик, формируй гипотезу, проверяй её мини-экспериментом, делай вывод, корректируй план». Ключевая разница — в том, что путь не задан, а конструируется в процессе.

Это даёт агенту принципиально другое свойство — адаптивность. Если рынок изменился, агент может изменить стратегию. Если креатив не сработал, он может сгенерировать новый. Если аудитория ведёт себя не так, как ожидалось, он может переопределить сегментацию. Workflow в таких условиях либо ломается (потому что сценарий не предусмотрен), либо требует ручной корректировки.

Сравнительная таблица

Критерий Workflow Агент

Источник пути

Человек прописывает шаги

Агент строит путь сам

Гибкость

Низкая — только заданные ветки

Высокая — выбор на каждом шаге

Предсказуемость

Высокая — путь известен заранее

Средняя — путь зависит от результатов

Стоимость разработки

Высокая на старте, низкая в поддержке

Ниже на старте, выше в поддержке

Контроль

Пошаговый

По###ам и правилам

Подходит для

Повторяющихся, предсказуемых процессов

Вариативных, адаптивных задач

Риск

Низкий — система делает то, что задано

Средний/высокий — система выбирает сама

Скорость внедрения

Медленнее (нужно описать все шаги)

Быстрее (нужно описать цель и правила)

Из этой таблицы видно главное: выбор между workflow и агентом — не вопрос «что современнее», а вопрос «какова природа задачи». Если задача повторяющаяся, предсказуемая и не требует адаптации — workflow лучше, дешевле и надёжнее. Если задача вариативная, требует оценки промежуточных результатов и выбора между альтернативами — агент даёт принципиально другие возможности.

Когда workflow превращается в агента

Между чистым workflow и чистым агентом есть спектр промежуточных состояний. На одном конце — полностью заданный сценарий без ветвлений. На втором — сценарий с условиями и циклами. На третьем — сценарий с параметрами, которые может менять AI-модель, но в рамках заданных шагов. На четвёртом — сценарий, в котором AI-модель сама определяет, какие шаги выполнить. На пятом — агент с полной свободой действий в рамках цели и ограничений. Этот спектр — не теоретическая конструкция, а практический инструмент: переход между уровнями можно делать постепенно, не пытаясь сразу перепрыгнуть от простого workflow к полностью автономному агенту.

Пример постепенного перехода. Шаг 1: workflow отправляет email всем, кто бросил корзину, через 1 час. Шаг 2: workflow добавляет условие — если сумма корзины больше 5 000 #, отправляем письмо с предложением консультации; иначе — с промокодом. Шаг 3: workflow отправляет разные письма в зависимости от сегмента (новый/вернувшийся, тип товара, гео). Шаг 4: AI-модель генерирует содержание письма под каждый контакт на основе его истории. Шаг 5: AI-агент сам определяет, отправлять ли письмо, какому сегменту, с каким предложением и когда, отслеживая конверсию в покупку и корректируя стратегию. На каждом шаге система

становится более адаптивной, но и более сложной в контроле.

Гибридная модель: workflow + агент

На практике большинство систем — гибридные. Workflow используется для надёжных, предсказуемых операций (отправка письма, обновление статуса, постановка задачи). Агент включается там, где нужна адаптация (какое письмо отправить, какой статус поставить, какую задачу сформулировать). Такая гибридная архитектура даёт лучшее из двух миров: предсказуемость workflow и адаптивность агента. Большинство примеров в этой книге — гибридные.

Сквозной кейс: «МетрикаПро» (B2B) — гибридная архитектура

SaaS-сервис для аналитики маркетинговых. Цикл сделки длинный (45–90 дней), средний чек 12 000 #/мес, конверсия из лида в продажу — около 8%. Архитектура: workflow обрабатывает базовый цикл — регистрация → welcome-серия → скоринг → передача в продажи. Агент включается на этапе квалификации лидов.

Workflow: новый лид регистрируется → получает welcome-серию из 4 писем (день 0, 2, 5, 9) → в каждом письме отслеживается активность (открытия, клики, входы в систему) → на основе активности скоринг обновляется → при скоринге 50+ лид передаётся менеджеру.

Агент: при передаче менеджеру агент анализирует дей-

ствия лида в системе — какие отчёты открывал, какие метрики смотрел, какие магазины подключал. На основе этого формирует для менеджера краткую справку: «Лид интересуется аналитикой продаж на Wildberries, подключил два магазина, смотрел отчёты по конкурентам. Рекомендация: предложить тариф Pro с акцентом на анализ конкурентов». Агент не ведёт переговоры — он готовит контекст для менеджера.

Результат: время подготовки менеджера к звонку сократилось с 15–20 минут до 2–3 минут; конверсия из звонка в демо выросла с 38% до 47%.

Границы workflow: где он перестаёт работать

Workflow хорошо работает до тех пор, пока число возможных сценариев остаётся управляемым. На практике это значит: 5-10 ветвлений — нормально, 20-30 — сложно, но поддерживаемо, 50+ — уже не поддерживаемо. Каждый новый сценарий — это новая ветка в коде, новый тест, новый потенциальный баг. В какой-то момент код workflow становится настолько сложным, что любое изменение требует ревизии всех веток. Это и есть граница, за которой нужен агент.

Симптомы того, что workflow достиг своего предела: команда тратит много времени на поддержку существующих сценариев, а не на развитие; новые сценарии добавляются медленно; часто происходят «неучтённые случаи», которые требуют ручного вмешательства; логика workflow разрослась настолько, что никто в команде не помнит все детали. Если вы видите эти симптомы — это сигнал, что для текущей задачи нужен агентный подход, а не дальнейшее усложнение workflow.

Экономика выбора: workflow дешевле на старте, агент дешевле в развитии

Стоимость внедрения — отдельный фактор выбора. Workflow обычно дешевле в момент запуска: чёткие шаги, понятная логика, понятная разработка. Но workflow дорожает в поддержке: каждое новое условие, каждый новый сценарий — это разработка и тестирование. Агент дороже на старте: нужно спроектировать архитектуру, написать конституцию, настроить guardrails, обучить модель. Но агент дешевле в развитии: новые сценарии не нужно «добавлять в код» — агент обрабатывает их через свою логику, нужно только убедиться, что новые сценарии соответствуют правилам.

Эта разница в экономике объясняет, почему небольшие команды чаще выбирают workflow, а зрелые — агентов. На коротком горизонте (3-6 месяцев) workflow почти всегда дешевле. На длинном (12+ месяцев) агент становится выгоднее, особенно если задача вариативная. Для большинства маркетинговых задач горизонт — 1-2 года, и агент обычно выигрывает по совокупной стоимости владения.

Когда гибрид — лучший выбор

В реальности чистые workflow и чистые агенты встречаются редко. Большинство рабочих систем — гибриды: workflow для предсказуемой части процесса, агент — для вариативной. Например, в обработке входящих лидов: workflow принимает лид, проверяет обязательные поля, отправляет welcome-серию, ставит скоринг — это предсказуемая часть. Когда лид достигает определённого скоринга, срабатывает Sales-агент: он анализирует контекст, формирует персональное сообщение, передаёт менеджеру — это вариативная часть.

Гибрид хорош тем, что позволяет внедрять агентов постепенно. Сначала автоматизируете рутину через workflow. Когда workflow достигает предела сложности — добавляете агента на самом сложном участке. Со временем агентов становится больше, и workflow остаётся только там, где он действительно оптимален. Этот эволюционный путь — самый реалистичный для большинства компаний. Сразу построить «всё на агентах» — это риск и дорого; оставить всё на workflow — значит упустить возможности.

Глава 3. Где агент действительно нужен

Если простой workflow решает задачу, не нужен агент.

Это правило — самое важное в этой главе. Любая задача, которую можно решить workflow, должна решаться workflow. Агент имеет смысл только тогда, когда заранее прописать шаги невозможно или неэффективно. Внедрение агента там, где достаточно автоматизации, — это лишние риски, лишние затраты и лишние сложности в поддержке без какой-либо выгоды.

Когда агент особенно полезен

Есть семь признаков, по которым можно понять, что задача подходит для агентного решения. Не обязательно, чтобы присутствовали все семь — но чем больше признаков совпадает, тем сильнее аргумент в пользу агента.

Задача повторяется с определённой частотой. Если задача возникает один раз в год — агент не окупится. Если раз в неделю или чаще — экономика начинает работать.

Задача содержит несколько шагов. Один шаг — это не задача для агента, а просто функция. Несколько шагов с зависимостями — уже кандидат.

Задача требует анализа. Не просто «сделай X», а «посмотри на данные и реши, какой X делать». Это базовое свойство агентного подхода.

Задача использует несколько инструментов. Если всё решается одним вызовом API — это не агент, а интеграция. Агент нужен, когда нужно собрать данные из CRM, рекламного кабинета и аналитики, чтобы принять решение.

Задача имеет измеримый результат. Без измеримого результата нет критерия успеха, и агент не сможет понять, достигнута ли цель.

Задача допускает ограниченную автономию. Не полную свободу, а разумные рамки — например, действовать в пределах бюджета и набора каналов.

Задача содержит множество вариантов пути. Если путь один — workflow. Если возможных путей много и они зависят от результатов промежуточных шагов — агент.

Когда агент не нужен

С другой стороны, есть признаки, при которых агент — плохое решение. Этих признаков меньше, но они важнее, потому что внедрение агента там, где он не нужен, — самая дорогая ошибка.

Задача слишком редкая. Если возникает раз в квартал — дешевле сделать вручную.

Стоимость ошибки очень высокая. Если ошибка может стоить миллионы или навредить репутации — оставьте решение человеку, а агент используйте только как ассистента.

Процесс плохо определён. Если вы не можете объяснить человеку, как выполняется задача, — вы не сможете объяснить это и агенту.

Нет данных. Агент работает с данными. Если данных нет или они низкого качества — агент будет принимать плохие решения.

Нет критериев успеха. Без них невозможно понять, достигнут ли результат, и тем более — оценить качество работы агента.

Обычный workflow решает задачу проще и надёжнее. Это самый частый случай: команда увлекается агентной модой и забывает, что простое решение лучше сложного.

Четыре вопроса для принятия решения

Прежде чем внедрять агента, задайте четыре вопроса. Первый: «Можно ли решить задачу workflow?» Если да — используйте workflow. Второй: «Какова стоимость ошибки агента?» Если ошибка критична — агенту нужны очень жёсткие ограничения, и он, скорее всего, будет работать в режиме рекомендаций. Третий: «Есть ли измеримый критерий успеха?» Если нет — задача не подходит для агента. Четвёртый: «Какой объём данных доступен?» Если данных мало — агент не сможет принимать качественные решения.

Эти четыре вопроса отсекают большинство кандидатов на агентное решение. На практике из 10 задач, которые команда хочет отдать агенту, 6–7 обычно оказываются задачами для workflow, 2–3 — задачами для гибрида (workflow + AI-ассистент), и только 1 — настоящей задачей для агента. Это нормально и даже желательно: меньше агентов — меньше рисков, проще поддержка, понятнее экономика.

Матрица «вариативность × стоимость ошибки»

Полезный инструмент принятия решений — матрица, где по одной оси отложена вариативность задачи (насколько предсказуем путь), по другой — стоимость ошибки (сколько стоит неверное решение). Четыре квадранта дают четыре разных рекомендации.

Стоимость ошибки низкая

Стоимость ошибки высокая

Вариативность низкая

Workflow

Workflow + жёсткий контроль

Вариативность высокая

Агент (полная автономия)

Агент (только рекомендации) или гибрид

В квадранте «низкая вариативность + низкая стоимость ошибки» — большинство рутинных операций (рассылки, обновление статусов, базовые отчеты). Workflow здесь оптимален. В квадранте «низкая вариативность + высокая стоимость ошибки» — финансовые операции, изменение

ключевых настроек, отправка коммуникаций VIP-клиентам. Workflow с дополнительными проверками и подтверждениями. В квадранте «высокая вариативность + низкая стоимость ошибки» — генерация контента, тестирование гипотез, мониторинг. Здесь агент может работать с большой автономией. И, наконец, в квадранте «высокая вариативность + высокая стоимость ошибки» — стратегические решения, крупные бюджеты, репутационные вопросы. Здесь агент должен работать в режиме рекомендаций: предлагает варианты, человек выбирает.

Типичные маркетинговые задачи и их соответствие

Рассмотрим типичные задачи маркетинга и то, какой инструмент им соответствует. Это не абсолютная классификация — конкретный выбор зависит от контекста бизнеса. Но как ориентир эта таблица полезна.

Задача

Инструмент

Уровень автономии

Welcome-серия новому подписчику

Workflow

Высокая

Реактивация спящих клиентов

Workflow + AI-сегментация

Средняя

Мониторинг конкурентов

Агент

Высокая

Генерация рекламных креативов

Агент

Средняя (с подтверждением)

Корректировка ставок в рекламе

Workflow + AI-рекомендации

Средняя

Квалификация входящих лидов

Агент

Высокая

Стратегия контент-плана на квартал

Агент-ассистент + человек

Низкая (рекомендации)

Анализ причин падения конверсии

Агент

Высокая

Управление репутацией в отзывах

Гибрид

Средняя

CRM-скоринг и распределение лидов

Workflow + AI-модель

Высокая

Из таблицы видно: чистых агентов в маркетинге меньше, чем кажется. Большинство задач решается гибридами — workflow с AI-компонентами. Это и есть реальная картина внедрения AI в маркетинге 2026 года. Полностью автономные агенты — это скорее исключение, чем правило, и применяются они в основном в задачах с низким риском и высокой вариативностью (контент, исследования, аналитика).

Сквозной кейс: «Вкуснотех» (услуги) — анализ задач на соответствие агенту

Сеть из 8 кулинарных студий в трёх городах. Услуги: групповые мастер-классы, корпоративы, индивидуальные занятия. Бронирование через сайт и по телефону. База клиентов — 30 000 контактов, 60% — повторные.

Команда рассмотрела 12 задач для возможного внедрения агента. Из них: 7 задач переведены на workflow (welcome-серии, напоминания о занятиях, поздравления с днем рождения, базовая реактивация, сбор отзывов, обновление расписания на сайте, отчёты для руководителя). 3 задачи переведены на гибрид (сегментация клиентов для персонализированных предложений, генерация контента для соцсетей, обработка отзывов). 2 задачи отдали агенту: мониторинг конкурентов (сбор и анализ цен, расписания, новых программ) и аналитика загруженности студий с рекомендациями по оптимизации расписания.

Результат: вместо 12 кандидатов в агенты — только 2. Это

позволило сфокусировать внимание на правильной архитектуре двух агентов, а не размазывать ресурсы на 12 полуработорых систем. Экономика двух агентов оказалась положительной уже через 4 месяца.

Зрелость команды как фактор выбора

Даже если задача подходит для агента, есть ещё один фактор — зрелость команды. Агент требует сопровождения: проектирования, настройки, мониторинга, обновления. Если в команде нет человека, способного играть роль архитектора агента, даже идеальный кандидат на агентное решение превратится в неуправляемый эксперимент. Перед запуском агента задайте вопрос: кто в команде будет отвечать за его работу? Этот человек должен понимать и маркетинг, и основы AI, и основы интеграций. Если такого человека нет — сначала растите его, потом запускайте агента.

Минимальный набор ролей для запуска первого агента: бизнес-владелец (формулирует цель и критерии успеха), архитектор (проектирует агента и guardrails), разработчик (реализует интеграции и логику), оператор (следит за работой в продакшене и реагирует на эскалации). В небольших компаниях одна и та же роль может совмещаться в одном человеке — но функции должны быть. Без бизнес-владельца агент оптимизирует не то. Без архитектора агент получается непредсказуемым. Без разработчика — не интегрируется. Без оператора — ломается без присмотра.

Дорожная карта внедрения агентов

Если команда определилась, что ей нужен агент, но не знает, с чего начать, — полезно придерживаться типовой дорожной карты. Месяц 1-2: один Research-агент или Analytics-агент (READ-only) — это безопасный старт, который даёт понимание, как агенты работают в реальном контексте. Месяц 3-4: добавление WRITE-агента (например, CRM-агента для зависших лидов) — это уже более высокий уровень автономии, но всё ещё низкий риск. Месяц 5-6: первый EXECUTE-агент с подтверждением (например, Sales-агент для квалификации лидов). Месяц 7-9: добавление Supervisor-агента для координации двух-трёх агентов. Месяц 10-12: оценка результатов и план дальнейшего расширения.

Эта дорожная карта — ориентир, а не догма. Конкретные сроки зависят от размера команды, сложности интеграций, готовности инфраструктуры. Главное — двигаться постепенно и на каждом шаге оценивать, принёс ли предыдущий агент реальную пользу. Если агент не окупается через 6 месяцев — лучше пересмотреть архитектуру, чем упорствовать в попытках заставить его работать. Если окупается — расширять. Принцип «докажи полезность перед масштабированием» работает и для отдельных агентов, и для всей системы.

Сигналы, что агент нужен прямо сейчас

Есть несколько практических сигналов, что задача прямо сейчас подходит для агентного решения, а не ждёт будущего. Первый: задача не делается, потому что никто не успевает. Если есть функция, которая теоретически нужна, но в команде нет рук — агент может закрыть эту нишу. Второй: задача делается, но плохо и нерегулярно. Если еженедельный анализ конкурентов делается раз в месяц, когда кто-то вспоминает — агент будет делать её каждую неделю. Третий: задача делается, но *inconsistently* — каждый раз по-разному, в зависимости от того, кто из сотрудников её делает. Агент даёт *consistently* — одно и то же действие выполняется одинаково.

Четвёртый сигнал: задача требует синтеза данных из нескольких источников, который человек делает долго. Если анализ рекламных кампаний требует открыть 4 кабинета, выгрузить данные в Excel, сопоставить с CRM — это часы работы, которую делает агент за минуты. Пятый сигнал: задача требует реакции в реальном времени, но человек не успевает. Если нужно реагировать на негативные отзывы в течение часа, но дежурный не всегда успевает — агент может быть «первой линией обороны». Любой из этих сигналов — повод серьёзно рассмотреть агентное решение.

Скоринг задач на соответствие агенту

Чтобы не полагаться на интуицию при выборе задач для агента, полезно использовать количественный скоринг. Каждой задаче даётся оценка по нескольким критериям, и по сумме можно сравнивать кандидатов. Это особенно полезно, когда у команды есть несколько потенциальных задач и нужно выбрать одну-две для начала.

Критерий

0 баллов

1 балл

2 балла

3 балла

Повторяемость

Раз в год

Раз в квартал

Раз в месяц

Еженедельно+

Вариативность

Один путь

2-3 пути

5-10 путей

10+ путей

Стоимость ошибки

Высокая

Средняя

Низкая

Минимальная

Доступные данные

Нет

Ограниченно

Достаточно

Богатые

Измеримость

Нет КРІ

Косвенная

Прямая КРІ

Мульти-КРІ

Срочность

Не срочно

Срочно

Очень срочно

Критично

Задача с суммой 12-18 баллов — отличный кандидат на агента. 8-12 — кандидат, но требует внимательной проработки. Ниже 8 — лучше решать workflow или вручную. Этот скоринг — не догма, но он помогает принимать решение осознанно, а не «по ощущениям». Если разные участники команды дают задаче разные оценки — это повод обсудить разногласия, прежде чем начинать разработку.

Альтернативы агенту: что ещё можно сделать

Если задача не подошла для агента — это не значит, что её нельзя автоматизировать. Есть несколько альтернатив, которые часто недооценивают. Первая: просто не делать. Если задача редкая и не критичная — может быть, проще оставить как есть, чем строить сложную систему. Вторая: workflow. Если задача предсказуема — workflow будет дешевле и надёжнее. Третья: AI-ассистент для сотрудника. Если задача требует человеческого решения, но часть операций рутинная — дайте сотруднику AI-ассистента, который ускорит работу.

Четвёртая альтернатива: аутсорс. Если задача не является ключевой компетенцией бизнеса — может быть, проще отдать её на аутсорс, чем строить сложную систему. Пятая: нанять человека. Иногда это дешевле, чем автоматизация, особенно если задача требует гибкости и нестандартных решений. Шестая: использовать готовый SaaS-продукт, который решает эту задачу. Не всё нужно строить с нуля.

Эти альтернативы упомянуты не для того, чтобы отговорить от агентов, а для того, чтобы агентное решение выбиралось осознанно. Агент — это инструмент, а не религия. Если в каком-то случае лучше другое решение — нужно выбрать его. Это зрелый подход.

Глава 4. Память агента

MEMORY ≠ KNOWLEDGE BASE ≠ DATABASE

Память — один из самых недооценённых компонентов агента. Без памяти агент каждый раз начинает с чистого листа: он не помнит, что пробовал, что сработало, а что нет, какие у клиента были возражения, какие креативы уже использовались. С памятью он может накапливать опыт, не повторять ошибки и постепенно улучшать качество своих действий. Но память — это не просто «склад всего, что когда-либо происходило». Это структурированная система, в которой разные виды информации хранятся по-разному и используются для разных целей.

Прежде чем разбирать типы памяти, важно разделить три понятия, которые часто смешивают: *memory*, *knowledge base* и *database*. *Database* — это база данных: структурированное хранилище транзакционных записей (клиенты, заказы, события). *Knowledge base* — это база знаний: *curated*-хранилище проверенной информации о продукте, рынке, процессах, брендах. *Memory* — это контекст агента: то, что агент помнит о своих взаимодействиях, решениях, результатах, о текущей задаче. База данных — про факты. База знаний — про интерпретацию фактов. Память — про опыт агента.

Шесть слоёв памяти агента

1. Краткосрочный контекст

Краткосрочный контекст — это то, что агент держит «в голове» во время текущей задачи. Например, при выполнении цикла «проанализируй кампанию → предложи изменения → подготовь отчёт» агент должен помнить промежуточные выводы между шагами. Объём краткосрочной памяти ограничен размером контекстного окна модели. На практике это означает, что агент должен уметь «забывать» то, что уже не нужно для текущего шага, чтобы освободить место для новых данных. Хорошая архитектура агента явно управляет краткосрочным контекстом: что добавить, что убрать, что преобразовать в более постоянное хранилище.

2. История взаимодействий

История взаимодействий — это лог всех действий агента: что он делал, в каком порядке, с какими входными данными, с каким результатом. История нужна для двух целей: отладка (почему агент принял такое решение?) и обучение (какие стратегии работают лучше?). История должна быть структурирована: `timestamp`, `action`, `input`, `output`, `success_metric`. Без

структурированной истории невозможно ни улучшать агента, ни объяснять его поведение.

3. Долгосрочная память

Долгосрочная память — это то, что агент сохраняет между задачами. Например: «для сегмента B2B-клиентов с циклом сделки более 30 дней лучше работают образовательные email, а не промо-предложения». Или: «в прошлой кампании с акцентом на экологичность CTR был выше среднего на 28%». Долгосрочная память формируется из истории взаимодействий через обобщение: агент (или отдельный процесс) периодически анализирует историю и формулирует выводы. Эти выводы должны быть проверяемыми — иначе есть риск, что агент закрепит неверный паттерн.

4. База знаний

База знаний — это curated-хранилище проверенной информации: бренд-бук, описание продуктов, ценовая политика, правила коммуникации, FAQ, регламенты. В отличие от долгосрочной памяти, которая формируется автоматически, база знаний поддерживается человеком (или процессом с человеческим контролем). База знаний — это «тело знаний», на которое агент опирается при принятии решений. Хороший агент не полагается только на то, что модель знает из

своего предобучения; он всегда сверяется с актуальной базой знаний.

5. Клиентские данные

Клиентские данные — это база данных CRM: контакты, сделки, события, история коммуникаций. Эти данные агент не хранит у себя, а читает из CRM по необходимости. Здесь критически важно разграничение: что агент может читать, что может обновлять, что не может видеть вовсе. Клиентские данные — самая чувствительная часть контекста агента, и работа с ними требует отдельного внимания к безопасности и приватности.

6. Результаты прошлых действий

Результаты прошлых действий — это метрики и итоги предыдущих задач агента: «кампания X дала SAC 1 800 #, кампания Y — 3 200 #, кампания Z — 2 100 #». Эти данные позволяют агенту оценивать эффективность своих стратегий и выбирать ту, что лучше сработала в похожих условиях. Без этой памяти агент будет повторять одни и те же эксперименты заново, тратя ресурсы впустую.

Что хранить и зачем

Простой принцип: хранить нужно то, что влияет на будущие решения. Не «всё, что может когда-то пригодиться», а конкретно то, что изменит выбор агента на следующем шаге. Это отсекает 70–80% данных, которые иначе попали бы в память. Чем меньше памяти — тем проще её поддерживать, тем быстрее поиск, тем понятнее, на основе чего агент принял решение.

Тип памяти

Что хранить

Зачем хранить

Краткосрочная

Текущая задача, промежуточные выводы

Связать шаги в цикле

История

Логи действий и результатов

Отладка и обучение

Долгосрочная

Обобщённые выводы из истории

Не повторять ошибки

База знаний

Бренд, продукт, правила

Опора для решений

Клиентские данные

CRM-записи

Персонализация

Результаты

Метрики прошлых задач

Сравнение стратегий

Как обновлять, удалять и контролировать актуальность

Память — не склад навсегда. Она живая система, в которой данные должны обновляться, устаревать и удаляться. Правила обновления зависят от типа памяти. Краткосрочная обновляется при каждом шаге и очищается при завершении задачи. История только добавляется (это append-only лог). Долгосрочная память пересматривается периодически: раз в неделю или месяц. База знаний обновляется при изменении продукта, цен, политики. Клиентские данные синхронизируются с CRM в реальном времени. Результаты прошлых действий хранятся с временными метками, и старые записи постепенно «забываются» — или помечаются как устаревшие, если условия изменились.

Контроль актуальности — отдельная задача. Кто решает, что вывод всё ещё верен? Кто удаляет устаревшие записи? Кто следит, чтобы база знаний соответствовала текущему продукту? На практике это роль, которую можно назвать «архивариус» — либо человек, либо отдельный процесс, который периодически проверяет и обновляет память агента. Без архивариуса память быстро превращается в свалку, и агент начинает принимать решения на основе неактуальных данных.

Доступ к памяти: кто что может видеть

Не весь контекст должен быть доступен агенту в любой момент. Разные типы памяти требуют разного уровня доступа. Краткосрочный контекст — только текущему агенту. История — текущему агенту и администраторам. Долгосрочная память — всем агентам того же типа. База знаний — всем агентам. Клиентские данные — только тем агентам, которые работают с данным клиентом, и только в объёме, необходимом для задачи. Результаты прошлых действий — всем агентам того же типа, плюс возможность поделиться с другими типами агентов при наличии бизнес-цели.

Эта модель доступа — основа безопасности. Чем строже правила, тем меньше риск утечки данных или некорректного использования информации. Например, рекламный агент не должен видеть содержимое переписки менеджера с клиентом — это зона CRM-агента. А CRM-агент не должен видеть детали рекламных кампаний — это зона рекламного агента. Каждый тип агента имеет свой профиль доступа к памяти, и этот профиль должен быть явно задан.

Сквозной кейс: «ДомДеко» — архитектура памяти CRM-агента

Краткосрочный контекст: текущий сегмент лидов, по которому работает агент; последние 50 обработанных контак-

тов; текущая гипотеза (например, «отправка письма с напоминанием о брошенной корзине через 1 час снижает долю незавершённых заказов на 6–9%»).

История взаимодействий: лог всех отправленных писем, обновлений CRM, созданных задач менеджерам. Хранится 90 дней, потом архивируется.

Долгосрочная память: выводы вида «для сегмента покупателей товаров для кухни письмо с рецептом работает на 18% лучше, чем письмо с промокодом»; «клиенты с первой покупкой свыше 5 000 # в три раза чаще возвращаются в течение 60 дней — им нужно особое отношение». Обновляется еженедельно.

База знаний: бренд-бук, каталог товаров с ценами, правила скидок, список запрещённых слов в коммуникациях, FAQ.

Клиентские данные: доступ на чтение к контактам, истории заказов, статусам корзин. Доступ на запись — обновление статуса активности, добавление заметок. Без доступа к платежным данным и персональным документам.

Результаты: конверсия каждого типа письма, средняя сумма восстановленной корзины, доля повторных брошенных корзин после первого письма.

Векторная память: новый подход

Традиционная память агента — это структурированные записи в базе данных: таблицы с полями, связями, индексами. Для многих задач этого достаточно. Но есть класс задач, где структурированная память не работает: когда нужно искать «похожие» случаи, а не точные совпадения. Например: «найди в истории кампании, похожие по динамике на текущую». Точное совпадение не найти, но похожие — можно. Для этого используется векторная память: каждая запись преобразуется в числовой вектор (embedding), и поиск ведётся по близости векторов.

Векторная память особенно полезна для Research-агентов (поиск похожих исследований), Content-агентов (поиск похожих успешных тем), Sales-агентов (поиск похожих клиентов с успешной историей сделки). Технически это реализуется через специализированные базы данных: Pinecone, Weaviate, Qdrant, или через pgvector в PostgreSQL. Выбор зависит от масштаба и существующей инфраструктуры. Главное — понимать, что векторная память не заменяет структурированную, а дополняет её: для точных запросов — структура, для похожих — векторы.

Забывание: что удалять и когда

Память без забывания — это помойка. Чем больше записей, тем сложнее найти релевантные, тем выше риск, что агент опирается на устаревшие данные. Поэтому## — это не потеря, а функция. Что удалять и когда — отдельная задача. Краткосрочная память очищается при завершении цикла. История хранится долго (90+ дней), но периодически архивируется. Долгосрочная память пересматривается: раз в неделю или месяц выводы проверяются, и те, что устарели, помечаются или удаляются. База знаний обновляется при изменении контекста. Клиентские данные хранятся в соответствии с политикой конфиденциальности и регуляторными требованиями.

Правило большого пальца: если данные не использовались в течение 6 месяцев — они, скорее всего, не нужны. Если вывод не подтверждается новыми данными — он устарел. Если запись в базе знаний противоречит текущему состоянию продукта — её нужно обновить. Без периодической чистки память становится балластом, замедляющим работу агента и снижающим качество его решений. Чистка памяти — это такая же обязательная процедура, как аудит конституции или проверка guardrails.

Конфиденциальность и память

Память агента — это потенциальная точка утечки данных. Если агент хранит историю взаимодействий, в этой истории могут быть чувствительные данные клиентов: имена, контакты, история покупок, переписка. Если агент передаёт контекст во внешнюю модель (LLM), чувствительные данные могут попасть «наружу». Это серьёзный риск, и его нужно явно учитывать при проектировании памяти.

Основные меры защиты: минимизация — агент хранит только то, что нужно для работы; обезличивание — имена и контакты заменяются на идентификаторы; маскирование — чувствительные поля маскируются перед передачей модели; шифрование — память шифруется на диске; разграничение — разные агенты имеют доступ к разным частям памяти. Эти меры не «делают память безопасной» — они снижают риск до приемлемого уровня. Полностью безопасной памяти не бывает, как не бывает полностью безопасной любой системы обработки данных. Цель — управлять риском, а не устранить его (что невозможно).

Контекстное окно и его ограничения

Каждая модель имеет ограничение на размер контекста — количество токенов, которое она может «видеть» одновременно. Это ограничение не техническое — оно архитектурное: модель «знает» только то, что помещается в её окно. Если контекста больше, чем окно, модель либо игнорирует часть контекста (обычно — самое старое), либо разбивает обработку на несколько вызовов. Для агента это означает, что он должен явно управлять своим контекстом: что загружать, что выгружать, что резюмировать.

Практические приёмы управления контекстом. Первый: суммирование истории. Если у агента есть история из 50 взаимодействий, он не загружает все 50 в контекст — он загружает резюме первых 40 и последние 10 в полном виде. Второй: релевантная выборка. Если у агента есть база знаний на 1000 документов, он не загружает всю базу — он ищет по релевантности и загружает только топ-3. Третий: приоритизация недавнего. Последние действия важнее для текущего решения, чем события месячной давности — модель должна «помнить» последние лучше.

Без явного управления контекстом агент быстро упирается в ограничения: либо работает медленно (потому что контекст большой), либо теряет важную информацию (потому что контекст маленький). Поэтому архитектура памяти аген-

та — это не «склад», а «активная система управления»: что добавить, что убрать, что преобразовать, что сохранить в долгом хранилище.

Глава 5. Инструменты агента

READ → ANALYZE → WRITE → EXECUTE → TRANSACT

Инструменты — это то, что превращает AI-модель в агента. Без инструментов модель может только отвечать на вопросы. С инструментами — действовать. Чем больше инструментов подключено, тем шире пространство возможных действий агента. Но одновременно растёт и риск: каждое новое подключение — это новая точка отказа, новый канал утечки, новый способ что-то сломать. Поэтому инструментальная архитектура агента — не «дать всё, что есть», а «дать ровно то, что нужно для задачи, с минимально необходимыми правами».

Типовой набор инструментов маркетингового агента

CRM

Доступ к клиентской базе: чтение контактов, истории взаимодействий, статусов сделок, заметок менеджеров; обновление статусов, добавление заметок, создание задач. CRM — центральный инструмент для большинства маркетинговых агентов, потому что именно в ней хранится основная информация о клиентах.

Аналитика

Доступ к системам веб-аналитики (Яндекс Метрика, Google Analytics, внутренние BI-системы): чтение конверсий, источников трафика, воронок, поведения пользователей. Аналитика даёт агенту возможность оценивать результаты своих действий и принимать решения на основе данных, а не предположений.

Рекламные кабинеты

Доступ к Яндекс Директ, VK Рекламе, Telegram Ads и дру-

гим рекламным системам: чтение статистики кампаний, цен, аудиторий; создание и остановка кампаний, корректировка ставок, изменение бюджетов. Это один из самых рискованных инструментов, потому что напрямую связано с деньгами.

Поисковые системы и веб

Доступ к поиску и чтению веб-страниц: мониторинг конкурентов, исследование тем, анализ трендов, сбор отзывов. Этот инструмент позволяет агенту получать актуальную информацию, не заложенную в его обучение.

Базы данных и таблицы

Доступ к внутренним базам данных, Google Sheets, Excel-файлам: чтение справочников, обновление отчётных таблиц, добавление записей. Часто используется как легковесное хранилище для самой памяти агента.

Email и мессенджеры

Доступ к системам рассылок (email, Telegram, WhatsApp): отправка сообщений, управление сегментами, отслеживание открытий и кликов. Один из самых чувствительных инструментов — любая ошибка может привести к массовой рас-

сылке не того контента не той аудитории.

CMS и системы управления контентом

Доступ к сайту, блогу, лендингам: создание, редактирование, публикация контента. Агент может использовать этот инструмент для автоматизации контент-маркетинга.

Системы управления задачами

Доступ к таск-трекерам (Jira, Trello, Asana, Битрикс24): создание задач, обновление статусов, назначение ответственных. Используется для передачи задач из автоматической системы в человеческую.

BI и внешние API

Доступ к BI-системам для построения отчётности; доступ к внешним API для получения рыночных данных, цен конкурентов, новостей, погоды, курсов валют — любого контекста, который может влиять на маркетинговые решения.

Пять уровней прав доступа к инструментам

Все инструменты можно разделить на пять уровней по степени воздействия на систему. Права доступа агента должны увеличиваться постепенно — от чтения к действию — и каждая ступень должна быть явно одобрена.

READ — только чтение

Агент может читать данные, но не может их изменять. Это самый безопасный уровень. Например: агент читает статистику из рекламного кабинета, но не может остановить или изменить кампанию. Подходит для аналитических и исследовательских агентов.

ANALYZE — обработка и анализ

Агент может читать данные и проводить с ними операции: агрегировать, сравнивать, рассчитывать метрики, формировать отчёты. При этом он не изменяет исходные данные — только создаёт производные. Например: агент читает данные из CRM и аналитики, формирует отчёт о воронке продаж. На выходе — новый документ, исходные системы не затронуты.

WRITE — создание данных

Агент может создавать новые записи в системе: добавлять контакты в CRM, создавать задачи, обновлять справочники. При этом он не может удалять или изменять существующие критичные данные. Например: агент добавляет нового лида в CRM, но не может удалить существующего клиента.

EXECUTE — изменение состояния системы

Агент может изменять состояние системы: останавливать рекламные кампании, менять ставки, отправлять рассылки, публиковать контент. Это уровень, на котором агент уже существенно влияет на бизнес-процессы. Каждое такое действие должно быть либо подтверждено человеком (для начала), либо ограничено жёсткими правилами.

TRANSACT — финансовые и высокорисковые действия

Агент может совершать действия, напрямую связанные с деньгами или критичными операциями: изменять бюджеты рекламных кампаний, осуществлять возвраты, списывать средства, отправлять коммерческие предложения. Это уро-

вень максимального риска, и большинство агентов сюда не допускаются. Если агент работает на этом уровне, каждое его действие должно логироваться и требовать двухфакторного подтверждения.

Уровень

Примеры действий

Риск

READ

Чтение CRM, статистики, отзывов

Низкий

ANALYZE

Расчёт метрик, формирование отчётов

Низкий

WRITE

Создание задач, добавление лидов, заметки

Средний

EXECUTE

Остановка кампаний, отправка рассылок

Высокий

TRANSACTION

Изменение бюджетов, возвраты, списания
Очень высокий

Почему права доступа должны увеличиваться постепенно

Принцип постепенного увеличения прав — не формальность, а основа безопасной эксплуатации агентов. Когда агент только запускается, мы не знаем, как он поведёт себя в реальных условиях. Дать ему сразу права EXECUTE — это дать ключи от машины водителю без прав. Правильная последовательность: сначала агент работает в режиме READ, мы смотрим, какие выводы он делает, насколько они корректны. Если всё хорошо — повышаем до ANALYZE и проверяем качество отчётов. Если отчёты полезны — даём WRITE и проверяем, что и как он обновляет. Только после нескольких циклов успешной работы на уровне WRITE можно переходить к EXECUTE — и то с подтверждением каждого действия. TRANSACT — финальная стадия, до которой большинство агентов не доходят никогда.

Эта последовательность не ускоряет, а замедляет внедрение — но именно это замедление и делает систему безопасной. Каждая стадия даёт команде уверенность, что агент ведёт себя предсказуемо. И если что-то идёт не так — проблема обнаруживается на ранней стадии, когда её легко исправить, а не после того, как агент отправил письмо 50 000 клиентам или потратил миллион рублей на неэффективную кампанию.

Tool Permission Matrix — матрица прав доступа

Для каждого агента должна быть явно задана матрица прав доступа к каждому инструменту. Это не формальный документ, а работающее правило, которое контролируется системой. Матрица строится по двум осям: инструменты (строки) и уровни прав (столбцы).

Инструмент

READ

ANALYZE

WRITE

EXECUTE

TRANSACTION

CRM (контакты)

✓

✓

✓

—

—

CRM (финансы)

—

—
—
—
—

Рекламный кабинет

✓
✓
—
✓*
—

Аналитика

✓
✓
—
—
—

Рассылки

✓
✓
✓*
✓*
—

CMS

✓

—

✓*

✓*

—

База знаний

✓

✓

—

—

—

Знак ✓ означает разрешённое действие, ✓* — разрешённое, но с подтверждением человека, — — запрещено. Эта матрица — основа работы системы: при попытке агента выполнить действие система проверяет, есть ли у него права, и если нет — блокирует действие и логирует попытку. Без такой матрицы любые разговоры о безопасности агента остаются разговорами.

Сквозной кейс: «МетрикаПро» — матрица прав Sales-агента

Sales-агент в B2B-сервисе аналитики для маркетплейсов. Задача — квалификация входящих лидов, подготовка контекста для менеджеров, ведение сделок до демо.

Права: READ — все поля в CRM кроме финансовых; ANALYZE — данные из аналитики по действиям пользователя в системе; WRITE — создание задач менеджеру, добавление заметок в карточку лида; EXECUTE — отправка templated-писем из набора одобренных; TRANSACT — нет.

Что особенно важно: агент НЕ имеет права изменять тариф клиента, не видит платёжную историю, не может отправлять произвольные письма (только из заранее одобренного шаблона с подстановкой переменных). Это снижает риск того, что агент отправит клиенту некорректную информацию или предложит условия, которые бизнес не готов выполнить.

Подтверждение: все EXECUTE-действия логируются и ежедневно проверяются руководителем продаж. За первые 3 месяца работы агента не было ни одного инцидента, потребовавшего отката.

Аутентификация и управление ключами

Подключение инструментов требует не только решения «что агент может делать», но и «как он аутентифицируется». Каждый инструмент имеет свой механизм: API-ключи, OAuth-токены, сервисные аккаунты. Эти учётные данные нужно где-то хранить, обновлять при истечении срока, отзывать при компрометации. Управление ключами — отдельная инженерная задача, и её нельзя решать «на скорую руку».

Базовые правила: ключи никогда не хранятся в коде (только в переменных окружения или в секретном хранилище); каждый агент имеет свой набор ключей (не один общий); ключи имеют минимально необходимые права; ключи ротируются раз в 90 дней или чаще; доступ к ключам логируется. Эти правила — не формальность, а основа безопасности. Утечка API-ключа от рекламного кабинета может стоить миллионы; утечка ключа от CRM — подорвать доверие клиентов.

Версионирование инструментов и обработка изменений API

Инструменты меняются. API обновляются: добавляются новые методы, удаляются старые, меняются форматы ответов. Это не редкость, а норма жизни. Агент должен быть устойчив к таким изменениям. Минимальные меры: явная версия API в коде (не «последняя», а «версия 5.2 от октября»); обработка ошибок API с разными стратегиями (повтор, эскалация, fallback); мониторинг изменений в API (подписка на changelog'и). Без этого агент будет работать до первого изменения API, а потом молча ломаться.

Особенно чувствительны к изменениям рекламные API: Яндекс Директ, VK Реклама, Telegram Ads обновляются регулярно, иногда с коротким notice. Если агент критичен для бизнеса, имеет смысл заложить в архитектуру «graceful degradation»: если один инструмент недоступен или изменён, агент должен понять это, сообщить, и продолжить работу с теми инструментами, что доступны. Это сложнее в разработке, но значительно повышает надёжность системы в реальном мире.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.