

Безопасный ИИ:

Как пользоваться нейросетями
и не раскрывать лишнее



ИИ
Марк Тьюрин

Марк Тьюрин

Безопасный ИИ: Как пользоваться нейросетями и не раскрывать лишнее

<https://litres.ru/74568368>

SelfPub; 2026

Аннотация

Поле ввода нейросети кажется личным блокнотом. Но вместе с запросом сервису могут уйти имена, документы, рабочая переписка и сведения, которые вы не заметили. Как пользоваться ИИ, не превращая удобный инструмент в источник утечки?

Эта книга учит оценивать риск по чувствительности данных, возможному пути раскрытия и цене ошибки. Вы узнаете, как сократить запрос до необходимого, обезличить материал без самообмана, проверить условия сервиса, настройки аккаунта и файлы перед загрузкой. Разберётесь, когда локальная модель действительно снижает передачу данных, как защитить рабочий контекст и осторожно обращаться со сведениями о здоровье, деньгах, праве и детях. А если чувствительная информация уже отправлена — поймёте, как остановить дальнейшее раскрытие и что делать.

Руководство для тех, кто использует или только осваивает нейросети для работы, учёбы и повседневных задач.

Содержание

Запрос — это тоже передача	5
Не всякая подробность одинаково опасна	19
Куда уходит текст после отправки	32
Своя оценка риска вместо общей тревоги	47
Просить результат, не отдавая исходник	64
Конец ознакомительного фрагмента.	69

Марк Тьюрин

Безопасный ИИ: Как пользоваться нейросетями и не раскрывать лишнее

Запрос — это тоже передача

Поле ввода нейросети похоже на личный блокнот: написал вопрос, получил ответ, закрыл окно. Но сходство обманчиво. Чтобы понять, безопасно ли отправлять запрос, важно смотреть не только на фразу в поле, но и на то, что приложение может к ней приложить, а сервис — сделать с полученными данными.

Начнём с обычной задачи: подготовить ответ клиенту. В запросе написано: «Отредактируй письмо, чтобы оно звучало спокойно и профессионально». Ниже — черновик с именем и фамилией клиента, номером договора, сроком поставки, суммой скидки и внутренней пометкой о том, на какие уступки готова пойти компания. Пользователь просит поправить тон, но передаёт гораздо больше, чем нужно для этой задачи.

Такие случаи не редкость. Так просто удобнее: скопиро-

вать письмо целиком, прикрепить документ, добавить пару пояснений — и не тратить время на подготовку отдельного фрагмента. Поэтому запрос стоит рассматривать не как одну строку текста, а как целый пакет данных.

Текст, который кажется единственным

Самый заметный слой — сообщение, которое пользователь набрал или вставил. В нём могут соседствовать вопрос, инструкция и исходные сведения: «Составь ответ», «сравни два варианта», «объясни результат», «найди противоречия». Чтобы получить точный ответ, к ним нередко добавляют контекст: описание должности, выдержку из договора или всю переписку целиком.

Первое практическое различие — между сведениями, необходимыми для задачи, и теми, что просто оказались рядом. Чтобы улучшить тон письма, обычно не нужны ни номер договора, ни внутренняя оценка переговорной позиции. Для ответа о задержке может хватить причины, согласованного срока и ограничения: не обещать компенсацию. Чем шире контекст, тем больше сведений уходит вместе с просьбой, хотя модель может использовать лишь малую их часть.

Иногда лишнее попадает в запрос не из-за невнимательности, а по привычке копировать текст целиком. Вместе с письмом отправляются подпись, история цепочки, адреса получателей, служебные пометки и ранее вложенные материалы. В документе могут остаться комментарии, исправления и скрытые поля. Имя PDF-файла может содержать фа-

милию клиента или название проекта, а в таблице могут быть дополнительные листы и столбцы, не относящиеся к вопросу. Видимый фрагмент страницы не всегда показывает, что именно входит в файл.

Поэтому полезно перечитать запрос глазами не только автора, но и получателя. Что именно станет доступно сервису, если обработать сообщение буквально? Это может быть одно предложение, а может — письмо, вся переписка, прикреплённый договор и пояснения из предыдущих сообщений. Оценка начинается не с того, хорошо ли задан вопрос, а с понимания границ пакета данных.

История не всегда остаётся за спиной

В диалоге каждое новое сообщение может опираться на предыдущие. Пользователь пишет: «Сделай короче», — и нейросети нужно понять, какой именно текст сократить. Для этого система соотносит новую просьбу с более ранним контекстом. Как именно сервис формирует этот контекст, зависит от его устройства: он может передавать всю историю, часть сообщений, выбранные фрагменты или краткое изложение.

По окну переписки не всегда понятно, какая схема используется. Видимая история и контекст, который модель получает для ответа, могут совпадать, но не обязаны. В длинном диалоге сервис может ограничивать объём или отбирать сообщения; некоторые настройки позволяют сохранять инструкции и сведения между беседами. Не стоит считать, что

каждое новое окно обязательно начинается с чистого листа. Но не следует и думать, что весь архив аккаунта автоматически отправляется с каждым вопросом. Без описания сервиса этого не узнать.

Лишний контекст может появиться и проще — из предыдущих реплик. В одном чате обсуждали рабочий проект, а затем перешли к письму клиенту. Если новый запрос продолжает ту же беседу, прежние сведения могут повлиять на ответ или войти в его контекст. Пользователь уже может не помнить, что сообщил несколько минут назад, но для системы связь между сообщениями сохраняется.

Представим, что специалист сначала попросил разобрать внутреннюю записку, а затем в том же чате написал: «Теперь подготовь нейтральное сообщение по срокам». Для такого сообщения хватило бы двух фактов: поставка задерживается, новый срок уточняется. Но в прежней части беседы остались причины задержки, сведения о запасах, имена сотрудников и оценка клиента. Сам по себе новый вопрос выглядит безопасно, однако соседний контекст может оказаться куда шире.

Некоторые сервисы предлагают постоянные инструкции, сохранённые предпочтения или функцию памяти. Это удобно: не приходится каждый раз объяснять формат ответа. Но появляется и дополнительный вопрос — какие сведения сохраняются и когда используются. Не всякое сохранённое правило чувствительно, однако заметка о должности, компа-

нии, клиентах или личных обстоятельствах может войти в контекст будущих запросов.

Практический вывод прост: если задача относится к другой теме, начните новый чат или проверьте, не добавляли ли история и сохранённые инструкции ненужных сведений. Это не гарантирует удаления старых данных из системы, но помогает ограничить контекст конкретного ответа.

Вложения увеличивают масштаб

Файл — не просто удобный способ передать текст: он может содержать больше, чем пользователь собирался показать. В документе со скопированным отрывком могут остаться комментарии и сведения об авторе. В презентации — заметки докладчика, в таблице — скрытые листы. На изображении могут быть лица, документы, открытые вкладки или детали помещения, не имеющие отношения к вопросу.

Способ обработки вложений тоже бывает разным. Сервис может получать исходный файл, извлечённый из него текст, изображение или несколько производных представлений. Для аудио возможны разные схемы: звук обрабатывается на устройстве или передаётся на распознавание; в запрос могут попасть сам файл, расшифровка либо и то и другое. Фотография может обрабатываться целиком, фрагментами или через распознанный на ней текст. Всё зависит от приложения и его настроек.

Допустим, руководитель просит кратко изложить отчёт. Если прикрепить весь рабочий файл, вместе с выводами мо-

гут уйти черновые расчёты, комментарии коллег и данные, не нужные для резюме. Если скопировать только окончательный раздел с результатами, объём контекста будет меньше. Возможно, придётся проверить, не потерялось ли важное ограничение, но это управляемый выбор, а не неизбежная цена любого ответа.

Проверяйте не только страницу, которую видите на экране, но и сам файл: его название, состав листов, комментарии, историю исправлений, лишние приложения. Если сервис позволяет выбрать фрагмент или предварительно показывает распознанный текст, посмотрите, что именно будет обработано. Если такой возможности нет, безопаснее подготовить отдельную копию с нужным содержимым.

От устройства до ответа

В зависимости от сервиса запрос обрабатывается локально или по сети. При локальной обработке модель запускается на устройстве пользователя либо в контролируемой внутренней среде организации. При сетевой данные передаются сервису, где выполняются вычисления. Возможен и смешанный вариант: часть операций проходит на устройстве, часть — на удалённых системах.

Простейший сетевой маршрут выглядит так: пользователь вводит запрос в приложении или браузере, программа формирует обращение и отправляет его через сеть в инфраструктуру сервиса. Там запрос обрабатывается, после чего пользователь получает ответ. Это общая схема, а не опи-

сание конкретного продукта. Между приложением и моделью могут быть дополнительные этапы: извлечение текста из файла, проверка запроса, выбор модели, обращение к подключённому источнику или инструменту.

Если сервис работает по сети, содержимое должно попасть в среду, где выполняются вычисления. Передачу обычно защищают шифрованием. Это снижает риск перехвата данных в пути, но не делает их недоступными самому сервису: чтобы обработать запрос на своей стороне, системе в какой-то момент нужно получить к нему доступ. Шифрование канала и отсутствие доступа у поставщика — разные свойства.

При обработке на устройстве запрос может не передаваться поставщику для генерации ответа. Но это не значит, что приложение вообще не обращается к сети: оно может проверять обновления, отправлять техническую статистику или использовать дополнительные сетевые функции. Такие действия не обязательно включают полный текст запроса — всё зависит от реализации и настроек. Одного слова «локальный» в описании недостаточно, чтобы сделать вывод обо всех потоках данных.

Проверка без сети может дать полезный, но ограниченный сигнал. Если основная функция продолжает работать при отключённом интернете, вероятно, ответ генерируется локально. Но это не доказывает, что при подключении приложение никогда не отправляет диагностические сведения, и не по-

казывает, куда раньше сохранялись запросы. Такая проверка помогает понять маршрут ответа, но не заменяет изучения документации.

В рабочей среде к маршруту добавляются правила организации. Компания может использовать собственную инфраструктуру или одобренный сервис, а администратор — управлять доступом и настройками. Это не означает, что администратор обязательно читает каждое сообщение. Но вопросы о доступе к истории, журналах и управлении учётной записью нужно решать по правилам конкретной системы, а не на основании личных ожиданий пользователя.

Что происходит после отправки

Нажатие кнопки — ещё не конец пути. Между отправкой запроса и появлением ответа могут проходить проверки, необходимые для работы сервиса и защиты от злоупотреблений. Например, система может автоматически оценить запрос и решить, допустимо ли его обрабатывать. Некоторые сервисы допускают ручную проверку в отдельных случаях, другие описывают такой доступ иначе. Нельзя заключить, что запрос обязательно прочитает сотрудник, но не стоит предполагать и обратное, если условия этого не подтверждают.

Сервису могут понадобиться журналы работы. Они помогают поддерживать стабильность, разбирать сбои, выявлять злоупотребления и обеспечивать безопасность. В журнале могут храниться технические события, а иногда — содержа-

ние запросов или часть взаимодействия. Какие именно данные записываются, кто имеет к ним доступ и как долго они хранятся, зависит от практики поставщика и его документов.

История диалогов в интерфейсе — лишь один вид хранения. Видимая переписка может сохраняться в аккаунте для удобства пользователя, а технические журналы — отдельно. Удаление чата из списка не всегда означает, что все копии сразу исчезли из резервных систем или журналов: сроки и порядок зависят от сервиса. Если поставщик обещает удаление, стоит выяснить, что именно удаляется, когда и какие есть исключения.

Отдельно нужно разобраться, могут ли запросы использоваться для улучшения моделей или других функций. Условия различаются в зависимости от продукта, типа аккаунта, настроек и режима работы. Где-то предусмотрен специальный переключатель, где-то правила зависят от рабочего тарифа или соглашения с организацией. Отключение использования данных для обучения не отвечает на вопросы о хранении, проверках безопасности и сроках ведения журналов. Это разные параметры.

Если ответ строится с помощью подключённого источника или инструмента, часть контекста может передаваться дальше. Например, сервис может искать сведения в выбранных пользователем файлах или обращаться к внутренней базе организации. Само наличие такой функции не означает, что информация отправляется куда угодно: маршрут зависит

от конфигурации. Но каждый подключённый источник расширяет перечень участвующих в обработке систем и требует отдельной проверки.

Что можно понять без документов поставщика? Лишь общую схему: сетевой сервис получает необходимые для обработки данные и возвращает результат; приложение может добавить к сообщению контекст; для поддержания сервиса могут вестись журналы. По виду окна нельзя определить, хранится ли весь запрос, передаётся ли он подрядчику, используют ли его для улучшения моделей, каков срок хранения и кто имеет доступ. Для таких выводов нужны настройки и документы конкретного сервиса.

Почему нельзя переносить доверие с одного сервиса на другой

Одинаковое поле ввода ничего не говорит о правилах, которые за ним стоят. Один сервис хранит историю в аккаунте, другой предлагает отдельный режим без её сохранения. В одном запросы могут использоваться для улучшения функций при включённой настройке, в другом действует иной порядок. В рабочем пространстве администратор может управлять сроками хранения, а в другом продукте такие возможности ограничены. Различаться могут даже режимы одного сервиса.

Не стоит ограничиваться рекламным описанием или одним переключателем с удобной формулировкой. Выясните, где обрабатываются данные, сохраняются ли запросы и фай-

лы, на какой срок и могут ли использоваться для улучшения сервиса. Отдельно проверьте, возможен ли доступ сотрудников или подрядчиков, как удаляется история и что остаётся в технических журналах. Если подключены инструменты, уточните, какие ещё системы получают данные.

Имеет значение и тип учётной записи. Личный аккаунт и рабочее пространство могут отличаться настройками, договорами и ролями администраторов. Не считайте рабочий доступ автоматически более закрытым, а личный — более открытым. Проверяйте конкретные условия и правила организации. Если ответ поставщика расплывчатый или его не удаётся найти, разумнее считать этот пункт неизвестным и не передавать данные, безопасность которых зависит от него.

Для российских организаций важно также проверить требования к обработке персональных данных и внутренние правила работы с информацией. Если в запросе есть персональные данные, одной кнопки «отправить» недостаточно, чтобы понять, допустима ли передача. Организации нужно оценить условия обработки с учётом применимых требований, включая Федеральный закон № 152-ФЗ, договоры и локальные документы. Сотруднику следует пользоваться разрешённым рабочим инструментом и не переносить клиентские или кадровые сведения в личный сервис только потому, что так быстрее.

Проверка перед отправкой

Перед отправкой полезно на несколько секунд мысленно

но разложить запрос. Сначала определите, какого результата ждёте и какие факты для него необходимы. Затем проверьте, не расширяют ли контекст история, файл, постоянные инструкции или подключённый источник. Наконец, выясните, куда направляются данные, кто может их обрабатывать и что известно о сроках хранения. Если какой-то слой непонятен, его можно сократить или отложить отправку.

Вернёмся к письму клиенту. Просьба «Отредактируй письмо» не требует обязательно передавать всю переписку. Можно оставить только текст ответа, убрав имя, номер договора и внутреннюю заметку. Если важны точные сроки, замените их нейтральной пометкой: «Новый срок — [дата]». Вместо рассказа о конкретном клиенте достаточно описать задачу: сообщить о задержке поставки, не обещать компенсацию и предложить вернуться с обновлением после подтверждения графика.

Так запрос сохранит условия, от которых зависит качество результата, но не будет содержать лишнего. Например: «Составь спокойный ответ клиенту о задержке поставки. Укажи, что новый срок пока уточняется; не обещай компенсацию; предложи вернуться с подтверждённой датой. Не более 90 слов». Чтобы получить черновик, нейросети не обязательно знать название компании и номер договора.

Если без исходного документа точный анализ невозможен, это ещё не значит, что нужно отправлять файл целиком. Для проверки одного условия можно выделить нужный

пункт, убрав названия сторон, подписи, контактные данные и соседние разделы. Для сравнения двух вариантов — оставить только относящиеся к вопросу фрагменты. Если описание всё равно позволяет узнать человека или сделку, замены имени на инициалы может быть недостаточно.

Когда задача действительно требует полного документа, решение зависит от его содержания и условий сервиса. Для внутреннего материала используйте инструмент, одобренный организацией и соответствующий её правилам. Если такого инструмента нет или условия непонятны, попросите нейросеть подготовить структуру анализа без загрузки документа, а сам анализ выполните вручную. Это медленнее, зато файл не придётся передавать неизвестному сервису.

Перед отправкой спросите себя: можно ли решить задачу без исходных сведений и не попали ли в запрос лишние история, вложение или заметка? Понимаете ли вы, обрабатывается ли он локально или через сеть, и знаете ли правила хранения и использования данных именно в этом режиме? Если на последний вопрос ответа нет, не стоит заполнять пробел догадкой в пользу удобства.

Такой подход не требует отказываться от нейросетей и не превращает каждый запрос в юридическую проверку. Он просто меняет точку приложения усилий: вместо надежды на то, что ненужное останется незамеченным, пользователь заранее убирает лишнее. В коротких задачах это часто быстрее, чем копировать весь материал целиком.

Запрос начинается не с нажатия кнопки, а с решения, какие сведения включить в работу. Поле ввода — часть интерфейса, а не личный блокнот: за видимым текстом могут стоять история, вложения, технические атрибуты, маршрут обработки и правила хранения. Следующий шаг — научиться различать сведения, без которых задачу не решить, и подробности, которые лишь повышают цену ошибки.

Не всякая подробность одинаково опасна

Один и тот же запрос может содержать безобидный вопрос, сведения о здоровье и подробности, по которым легко найти конкретного человека. Поэтому перед отправкой важно оценить не только сам вопрос, но и каждую деталь, которая попала в текст. Начнём не с распределения по одному ярлыку, а с оценки нескольких независимых признаков.

Шесть карточек перед отправкой

Представьте, что эти фрагменты лежат перед вами отдельно. Отметьте для каждого, откуда происходят сведения, насколько они чувствительны и можно ли по ним определить человека или организацию. Один фрагмент может получить сразу несколько отметок. Затем решите, можно ли отправить его без изменений.

А. «Объясни простыми словами, чем отличается гарантийный ремонт от платного».

Б. «Я руководитель смены на небольшом производственном предприятии в районном центре».

В. «Помоги составить список вопросов врачу: несколько недель беспокоит такой-то симптом, принимаю такое-то лекарство».

Г. «Проверь письмо: в нём указаны фамилия клиента, его

телефон, адрес и номер документа».

Д. «Подготовь ответ на жалобу: клиент получил заказ с задержкой, в обращении есть номер заказа и дата доставки».

Е. «Оцени план: в документе — внутренний прогноз продаж, планируемая цена и сроки запуска нового продукта».

Единственного верного ярлыка для каждой карточки нет. Например, сведения о клиенте могут одновременно относиться к рабочему процессу, быть персональными данными другого человека и позволять установить его личность. Важно не выучить список запрещённых слов, а понять, что это за сведения, кому они принадлежат, можно ли по ним кого-то определить и к чему приведёт их раскрытие.

В одном случае фрагмент окажется почти безобидным. В другом его стоит сократить или заменить обобщённым описанием. А иногда даже после сокращения сведения нельзя передавать выбранному сервису: они могут быть слишком чувствительными или затрагивать людей, чьи данные вы получили по работе.

Оценка по независимым признакам

Первый признак — контекст и источник сведений. Они могут относиться к вам, к другому человеку, к рабочему процессу или к деятельности компании. Эти отметки не исключают друг друга. Отдельно отметьте, опубликованы ли сведения открыто или относятся к внутренним.

Второй признак — чувствительность. Насколько серьёзными могут быть последствия раскрытия? Сведения о здоро-

вье, финансовых обстоятельствах, доступе к учётной записи или внутренних планах организации обычно требуют особой осторожности. При этом «чувствительность» здесь — практическая оценка риска, а не обязательно юридическая категория.

Третий признак — возможность идентификации. Прямые идентификаторы позволяют установить личность или заметно упрощают эту задачу. К ним относятся фамилия и имя в подходящем контексте, номер телефона, домашний адрес, номер документа. Косвенные признаки сами по себе могут не указывать на конкретного человека, но помогают сузить круг: должность, район, редкая специальность, дата события, небольшой коллектив.

Наконец, оцените возможные последствия. Раскрытие может навредить человеку, клиенту, работодателю или сразу нескольким сторонам. Ущерб бывает финансовым, репутационным, профессиональным или связанным с частной жизнью, безопасностью либо нарушением договорённостей.

Теперь проверим карточки на практике.

А — общий вопрос, не связанный с конкретным человеком или закрытой информацией. Обычно его можно отправить без изменений. Но он перестанет быть общим, если к нему приложить внутреннюю инструкцию, переписку или скриншот с именами.

Б — рабочий контекст и сведения о должности. В крупной организации они могут ничего не говорить о конкретном

сотруднике. Но если предприятие небольшое, а должность редкая, круг возможных людей быстро сужается. Фрагмент может раскрыть и личность, и обстоятельства работы.

В — личные сведения о здоровье, которые могут быть чувствительными. Имя не указано, однако подробности о симптомах и лечении способны сделать человека узнаваемым, особенно в небольшом коллективе или населённом пункте. Раскрытие такой информации может затронуть частную жизнь.

Г — рабочий текст с персональными данными клиента и несколькими прямыми идентификаторами. Фамилия, телефон, адрес и номер документа позволяют установить личность с высокой вероятностью. Для этого не всегда нужна фамилия: сочетания других данных может оказаться достаточно.

Д — рабочая ситуация, в которой есть сведения о клиенте. Номер заказа и детали обращения могут связать жалобу с конкретным человеком. Для подготовки вежливого ответа обычно хватает описания проблемы и желаемого результата, а имя, адрес и номер заказа можно не включать.

Е — внутренняя коммерческая информация. Она может раскрыть планы компании, даже если не содержит данных о конкретных людях. Возможные последствия — потеря конкурентного преимущества, нарушение обязательств перед партнёрами или другой деловой ущерб.

Эта оценка предварительная, а не постоянная. Один и тот

же номер заказа в обезличенном примере может быть просто технической меткой. В переписке с точной датой, товаром, суммой и адресом доставки он уже способен указать на конкретного клиента. Общий прогноз рынка может быть безвредным, а прогноз продаж одной компании до официального объявления — совсем другим по чувствительности.

В разговорной речи слово «личные» может означать сведения о частной жизни. Юридическое понятие персональных данных шире: в российском законодательстве это сведения, относящиеся прямо или косвенно к определённом или определяемому человеку. Поэтому стоит спрашивать не только «Есть ли здесь фамилия?», но и «Можно ли по этому фрагменту вместе с другими доступными сведениями понять, о ком речь?».

Место работы, должность и дата сами по себе не всегда позволяют определить человека. Но в небольшом коллективе должность может указывать на единственного сотрудника. Чем уже круг возможных людей, тем меньше значит отсутствие имени.

Финансовые сведения тоже требуют осторожности, хотя не стоит механически относить их к одной юридической категории. Доход, долги, покупки, реквизиты счёта и история операций могут раскрыть частную жизнь или дать материал для обмана и давления. Риск зависит от точности данных и от того, что можно сделать с их помощью. Номер банковской карты и обобщённое описание бюджета — не одно и то же,

а коды подтверждения и пароли нельзя передавать.

Не всякий внутренний документ автоматически является коммерческой тайной в юридическом смысле. В России для такого статуса важны установленные организацией условия и меры охраны. Но отсутствие формального статуса не превращает внутренний прогноз или план запуска в общедоступный материал. Если раскрытие может повлиять на переговоры, конкуренцию или обязательства перед партнёрами, учитывайте правила организации.

Кто может пострадать

При оценке риска легко сосредоточиться на себе: «Что будет, если увидят мои данные?». Но в рабочем запросе информация часто относится к другим людям. Клиент не отправлял её нейросети; пациент не выбирал сервис; сотрудник мог не знать, что его редкая должность и график окажутся в запросе. Пользователь решает, что включить в текст, но не всегда вправе передавать сведения, полученные по работе.

Поэтому рядом с вопросом «Что это за данные?» стоит задать другой: «Чьи интересы они затрагивают?». Если в тексте есть сведения о клиенте, важно учитывать не только удобство автора запроса, но и возможный ущерб для клиента. Если описан рабочий конфликт, под угрозой могут оказаться несколько сотрудников. Раскрытие внутреннего плана может затронуть компанию, партнёров и покупателей.

В российской организации правила работы с персональ-

ными данными, внутренними документами и сторонними сервисами зависят от роли сотрудника и конкретных процедур. Недостаточно решить, что сведения «не выглядят секретными»: нужно учитывать инструкции работодателя и использовать только разрешённые для задачи инструменты. Требования законодательства, в том числе Федерального закона № 152-ФЗ «О персональных данных», не заменяются личной оценкой «ничего страшного».

Когда имя не требуется

Представим, что нужно составить список вопросов для приёма у врача. Модели могут понадобиться симптомы, их продолжительность и список принимаемых лекарств. Полное имя, адрес, номер полиса, точное место работы и дата рождения обычно не помогают выполнить эту задачу. Их можно убрать, сохранив достаточно информации для полезного ответа.

Вместо полной медицинской выписки можно написать: «Составь нейтральный список вопросов для врача для взрослого пациента с таким-то симптомом, который продолжается около месяца; сейчас он принимает такие-то препараты». Если точный возраст важен, укажите возраст или диапазон, но не добавляйте остальные идентификаторы автоматически.

Сокращая контекст, важно не исказить смысл. Если от дозировки лекарства зависит вопрос, не стоит заменять её произвольным значением только ради видимости безопасности. Если для анализа нужны точные медицинские данные, ре-

шите, допустимо ли использовать этот сервис, а не копируете документ без разбора. Нейросеть не становится лечащим врачом оттого, что ей передали подробную историю.

Теперь вернёмся к жалобе клиента. Для ответа обычно нужны суть проблемы, сроки, доступные варианты решения и подходящий тон. Имя, телефон, адрес, номер заказа и скриншот переписки могут оказаться лишними. Часто достаточно написать: «Клиент А», «заказ Б», «доставка задержана на несколько дней». Если номер заказа нужен для внутренней системы, его можно оставить там, но не переносить в запрос к модели без необходимости и разрешения.

Такая замена не гарантирует полной анонимности. Уникальная покупка, точная дата, редкий адрес доставки и необычная жалоба могут помочь узнать человека. Условная метка вместо имени уменьшает прямую узнаваемость, но не устраняет следы, оставленные сочетанием обстоятельств.

Эффект домино

Проведём второй раунд оценки. Возьмём четыре детали, которые по отдельности могут показаться обычными.

Должность — единственный инженер, обслуживающий определённое оборудование.

Место — небольшой населённый пункт или конкретная площадка.

Дата — точный день недавнего происшествия.

Событие — редкий сбой, после которого работа объекта остановилась.

Каждая деталь добавляет свой фрагмент. Должность указывает на профессиональную роль, место сужает географический круг, дата помогает сопоставить описание с сообщениями или внутренними записями, а редкое событие отличает этот случай от повседневной работы. Вместе они могут указать на сотрудника, объект и инцидент — даже если имени в тексте нет.

Это эффект домино: сначала подробность почти ничего не раскрывает, но ведёт к следующей. Инженеров много. Единственный инженер на площадке в небольшом районе — уже более узкий круг. А если известно, кто дежурил в день редкого сбоя, возможен всего один вариант. Точная личность не всегда необходима: иногда достаточно понять, к какой должности относится ошибка, кому направить давление или какую уязвимость использовать.

То же происходит с данными клиента: редкий товар, точная сумма, день покупки и небольшая точка выдачи могут позволить узнать покупателя. В описании здоровья возраст, редкая специальность, клиника, точная дата приёма и необычный диагноз могут указать на пациента в небольшом городе или коллективе.

Проверяя сочетания, спросите себя: если соединить эти фрагменты с тем, что уже известно коллегам, клиенту, жителям района или доступно в открытых источниках, останется ли много возможных людей? Если ответ — «скорее всего, один» или «совсем немного», отсутствие имени ещё не де-

дает текст безопасным.

Для рабочей задачи риск часто можно снизить без потери смысла: обобщить должность, убрать точное место и подробности инцидента, заменить номер заказа условной меткой. В медицинском запросе можно удалить точное название клиники и дату, сохранив необходимые сведения о симптомах. Внутренний прогноз — представить в обобщённом виде или использовать только в инструменте, разрешённом организацией.

Отдельные данные могут быть открыты: должность опубликована на сайте учреждения, событие упомянуто в местных новостях, график размещён в объявлении. Но доступность каждого элемента по отдельности не означает, что их безвредно собрать в один точный портрет. В открытых источниках факты часто разбросаны по разным местам; запрос может связать их и добавить подробности, известные лишь небольшой группе людей.

Это не значит, что кто-то обязательно сопоставит каждый фрагмент. Риск растёт, когда для узнавания требуется не догадка, а простое соединение нескольких подсказок. Для предварительной оценки достаточно заметить, что отдельная деталь перестала быть отдельной.

Как определить достаточный контекст

Полезное правило — оставлять минимум контекста, достаточный для задачи. Это не значит «как можно меньше слов» и не требует превращать запрос в загадку. Речь о са-

мом небольшом наборе сведений, с которым ещё можно получить нужный результат.

Начните с формулировки задачи. Не «разобрать мою переписку», а, например, «предложить спокойный ответ на претензию о задержке». Затем отделите необходимые детали от тех, что просто скопировались вместе с письмом. Для ответа могут быть важны причина задержки и предлагаемый способ решения, но не телефон и домашний адрес клиента.

Измените точность там, где это не повредит результату. Вместо конкретного дня укажите месяц, вместо филиала — тип подразделения, вместо редкой должности — более широкую функцию. Возраст можно обозначить диапазоном, сумму — примерным интервалом, небольшую группу — описанием без названия отдела. Каждое обобщение должно сохранять смысл, важный для ответа.

Затем перечитайте текст и проверьте новые сочетания. Представьте, что его видит человек из той же организации или местности. Остаётся ли единственный кандидат? Не указывают ли должность, место и событие на конкретного сотрудника? Не связывают ли номер, дата или редкая подробность запрос с определённым клиентом?

После этого решите, допустимо ли вообще передавать оставшийся фрагмент. Если сведения относятся к клиенту, пациенту, сотруднику или внутренней деятельности организации, а правила компании не разрешают использовать выбранный сервис, обезличивание «на глаз» не заменит разре-

шения. Если задачу невозможно выполнить без точных данных, нужен подходящий одобренный процесс, а не косметическая замена имён.

Файлы требуют той же проверки, что и текст. В них могут оставаться подписи, комментарии, адреса в колонтитулах, имена в названиях документов, скрытые листы таблиц или данные на скриншотах. Перед загрузкой оцените не только абзац, который хотите показать модели, но и всё содержимое файла.

Три проверки перед отправкой

Чтобы быстро оценить запрос, ответьте на три вопроса.

Что именно я передаю: сведения о себе, данные другого человека, рабочую или общедоступную информацию? В одном фрагменте могут сочетаться сразу несколько признаков.

Можно ли определить человека или организацию по этому фрагменту вместе с соседними деталями? Ищите не только имя и телефон, но и должность, населённый пункт, дату, редкое событие, уникальный заказ или медицинскую подробность.

Что может произойти, если эти сведения окажутся не у того адресата? Достаточно представить правдоподобный ущерб: нарушение приватности, риск обмана, неприятности для клиента или сотрудника, раскрытие плана компании.

Если риск остаётся неясным, сократите контекст или используйте разрешённый рабочий процесс. Рабочая граница проходит не между «личным» и «безопасным», а меж-

ду необходимыми для результата сведениями и лишними. Чем чувствительнее информация и чем вероятнее ущерб для других, тем строже должна быть эта граница.

Куда уходит текст после отправки

Кнопка отправки создаёт впечатление простого обмена: вопрос ушёл, ответ вернулся. Но для сервиса за этим могут стоять несколько операций — от обработки запроса до сохранения истории и проверки безопасности. Важно не только то, какие сведения вы передаёте, но и можно ли связать их с аккаунтом, файлом или другими деталями. Поэтому, оценив сам запрос, стоит проследить и за тем, что происходит с ним дальше.

Один запрос — несколько маршрутов

Пользователь видит поле ввода и готовый ответ. Между ними могут быть интерфейс, серверы сервиса, компоненты для обработки файлов, средства защиты от злоупотреблений и сама модель. Иногда запрос направляется во вспомогательные системы — например, для распознавания текста на изображении. В некоторых продуктах модель работает на устройстве пользователя, и тогда путь данных устроен иначе. Как именно организован конкретный сервис, можно узнать только из его документации.

Даже облачный сервис не обязательно получает лишь строку, которую пользователь набрал в поле ввода. Вместе с ней могут передаваться предыдущие сообщения, загруженные документы, выбранные настройки, данные аккаунта и технические сведения об обращении. Состав и объём дан-

ных зависят от продукта и его настроек.

Представьте запрос: «Составь ответ клиенту на жалобу». К нему приложены переписка, номер заказа и снимок экрана. Сам вопрос звучит нейтрально, но в приложениях могут оказаться фамилия клиента, телефон, адрес доставки и сведения о работе сотрудника. Кроме того, сервис может получить данные, необходимые для работы аккаунта или защиты от сбоев. Это не значит, что каждый продукт собирает всё перечисленное. Это значит, что спрашивать стоит не только о содержимом поля ввода, но и о том, что сервис получает вместе с ним.

Чтобы понять маршрут данных, полезно отдельно выяснить, что происходит при передаче запроса и его обработке, сохраняется ли история, какие технические записи ведутся и используются ли данные для улучшения продукта. Не менее важны вопросы о доступе сотрудников и подрядчиков, сроках удаления, месте обработки и применением прав. Если документация не даёт ответа, это следует считать неизвестностью — а не доказательством того, что сервис хранит всё или, наоборот, ничего не сохраняет.

Отправка и формирование ответа

На первом этапе сервис принимает запрос и подготавливает его к обработке. В зависимости от продукта он может учитывать текущий диалог, сохранённые настройки, прикреплённые файлы или инструкции пользователя. Если вы просите продолжить работу над документом, сервису мо-

жет понадобиться передать не только последнюю фразу, но и часть переписки. Однако объём такого контекста определяется конкретным продуктом, а не общим правилом для нейросетей.

Файлы могут обрабатываться отдельно. Из изображения извлекают текст, документ преобразуют в формат, удобный для поиска, а длинный материал делят на фрагменты. Если сервис умеет искать по загруженным файлам или обращаться к дополнительным инструментам, документ может пройти через отдельный компонент системы. Для пользователя это всё равно выглядит как один диалог, хотя внутри происходят разные операции.

При проверке условий сервиса спросите: какие данные он получает вместе с сообщением и какие встроенные функции могут их обрабатывать? Обратите внимание на загрузку файлов, историю диалога, настройки памяти, голосовой ввод, распознавание изображений и внешние инструменты. Перед отправкой снимка экрана проверьте не только нужную область: на нём могут быть видны уведомления, открытые вкладки, имена файлов и другие сведения, не относящиеся к задаче.

Полученные данные используются для формирования ответа. Но обработка запроса и его последующее хранение — разные вопросы. Чтобы ответить, системе нужно принять и обработать сообщение; само по себе это не говорит о том, останется ли его содержание в истории аккаунта или тех-

ническом журнале. И наоборот, сохранение истории ещё не означает, что каждый фрагмент используют для обучения модели.

Отдельно выясните, как работают дополнительные функции. Сохранённые настройки или сведения из прошлых разговоров могут влиять на контекст следующего запроса. Пользователь начинает новый диалог, но сервис, возможно, продолжает учитывать данные из профиля. Это не повод отказываться от удобной функции, но хороший повод проверить, что именно сохраняется, как её отключить и затронет ли отключение уже сохранённые сведения.

Если вы работаете в локальной программе, установленной на устройстве, обработка может проходить без отправки текста на удалённый сервер. Но и в этом случае не стоит автоматически считать все данные локальными. Отдельные функции, синхронизация аккаунта, резервное копирование или отправка сведений о сбоях могут работать по своим правилам. Важно выяснить, где выполняется обработка конкретной функции, а не судить об этом по тому, что приложение установлено на компьютере или телефоне.

История диалога и технический журнал

История диалога — это сообщения, которые пользователь обычно видит в аккаунте и может открыть позднее. Технический журнал фиксирует работу сервиса: например, время обращения, тип ошибки или другие параметры. В нём может сохраняться содержание запроса, его часть или только све-

дения о событии. Точный состав зависит от продукта.

Эти два вида записей могут существовать независимо. Удаление переписки из списка чатов меняет историю в интерфейсе, но не обязательно затрагивает журналы, резервные копии или сведения, нужные для безопасности и устранения неполадок. Возможна и обратная ситуация: диалог не отображается в истории, но технические записи о нём хранятся ограниченное время. Универсального правила здесь нет.

В условиях сервиса ищите не только слово «хранение», но и пояснение, что именно хранится. Текст запросов, загруженные материалы, история аккаунта, отзывы и технические сведения могут быть описаны отдельно. Общая формулировка вроде «мы храним данные для предоставления услуг» сама по себе не раскрывает ни состав данных, ни сроки, ни различия между историей и журналами.

Сроки хранения также нужно соотносить с конкретными категориями. Один срок может относиться к истории чата, другой — к данным, необходимым для защиты сервиса, третий — к сведениям, которые сохраняют по правовым или договорным основаниям. Не переносите срок из одного пункта политики на все данные сразу. Возможность удалить диалог ещё не отвечает на вопрос, когда исчезнут связанные с ним копии.

В рабочем аккаунте важна роль администратора организации. Он может управлять пользователями и настройками

сервиса, но само наличие административных прав не доказывает, что ему видны все диалоги. Нельзя заранее утверждать и обратное. Это зависит от продукта, тарифа, настроек и условий организации. Перед загрузкой внутренних материалов выясните, кто в компании может настраивать доступ, просматривать историю или выгружать данные.

Показателен пример с обращением в поддержку. Чтобы описать сбой, пользователь может приложить весь диалог и снимок экрана. Между тем в условиях сервиса сообщения в поддержку могут рассматриваться отдельно от сведений, которые собираются автоматически. Если для решения проблемы нужен лишь один фрагмент переписки, безопаснее отправить его, удалив лишние личные и рабочие данные, чем прикладывать полный экспорт «на всякий случай».

Когда данные помогают улучшать сервис

Фраза «используем данные для улучшения сервиса» может описывать разные действия: анализ сбоев, оценку качества ответов, тестирование новых функций, работу с обращениями или обучение моделей. Иногда эти цели перечислены отдельно, иногда объединены общей формулировкой. По одному слову «улучшение» нельзя понять, использовали ли конкретный запрос для обучения модели.

Сначала выясните, как обрабатываются данные, необходимые для ответа. Затем проверьте, используются ли они для обслуживания сервиса, безопасности, диагностики, оценки качества или развития продукта. Наконец, ищите прямое

указание на обучение или настройку моделей: включено ли такое использование по умолчанию, можно ли от него отказаться и к каким данным относится настройка. Уточните также, распространяется ли отказ на файлы, отзывы, сообщения в поддержку и уже отправленные материалы.

Настройка с названием вроде «не использовать данные для обучения» может решать только один вопрос. Она не обязательно отключает сохранение истории, ведение технических журналов, проверку на злоупотребления или передачу данных исполнителям, которые обеспечивают работу сервиса. Настройка полезна, но не заменяет проверку остальных условий.

Столь же ошибочно считать любое упоминание улучшения доказательством, что запрос попадёт в обучающую выборку. Сервис может исправлять ошибки или совершенствовать интерфейс на основе статистики, не обучая модель на содержании каждого сообщения. Условия иногда различают данные, связанные с аккаунтом, и агрегированные показатели. Поэтому важны точные определения, а не удобное толкование.

Требует внимания и слово «обезличивание». Удаление имени и телефона снижает риск, но не всегда позволяет исключить повторную идентификацию. Редкая должность, небольшой населённый пункт, дата события и необычная медицинская информация вместе могут указать на конкретного человека. Проверьте, что именно сервис считает обезли-

ченными данными и сохраняется ли связь с аккаунтом до их преобразования.

Отдельный канал передачи — оценка ответа или отзыв о нём. Нажимая кнопку обратной связи, пользователь может отправить не только отметку «полезно», но и связанный с ней запрос, ответ или пояснение. Если хотите сообщить о проблеме, проверьте, какие сведения прикрепляются к отзыву. В рабочей переписке обычно достаточно описать тип ошибки — копировать в комментарий целый документ незначем.

Для профессиональной команды полезно отделять материал, необходимый для ответа, от того, что «может пригодиться для лучшего результата». Если требуется отредактировать пункт договора, зачастую достаточно передать сам пункт и нейтрально описать задачу. Полный договор с реквизитами и приложениями в таком случае не нужен. Чем меньше сведений не по теме отправлено, тем меньше данных придётся проверять на дальнейших этапах.

Кто может получить доступ

Упоминание доступа сотрудников в условиях не означает, что каждый работник сервиса свободно читает переписку. Доступ могут ограничивать конкретными задачами: обработкой обращения в поддержку, расследованием инцидента, проверкой злоупотреблений или контролем качества. Но и уверенность, что человек никогда не увидит текст, требует подтверждения.

Проверьте, в каких случаях допускается доступ к содержанию, кто его может получить и какие ограничения действуют. Важно понять, распространяются ли правила на сотрудников, привлечённых исполнителей и организации, предоставляющие технические компоненты. Условия могут требовать защищать данные или ограничивать доступ, не раскрывая всех внутренних процедур. Если этого недостаточно для оценки чувствительного материала, задайте вопрос поставщику или используйте среду с более понятными договорными условиями.

Подрядчики могут обеспечивать инфраструктуру, поддержку, обработку файлов, защиту от атак или рассылку уведомлений. Их участие не обязательно означает, что каждый из них получает полный текст запросов. Однако при работе с чувствительными материалами стоит выяснить, какие категории исполнителей привлекаются, для каких задач и к каким данным у них есть доступ. Если политика приводит перечень организаций или описывает категории подрядчиков, изучите его. Если подробностей нет, не считайте это доказательством того, что передача исключена.

В России при работе с персональными данными важны роли участников, цели и основания обработки. Федеральный закон о персональных данных устанавливает требования к операторам и обработке, однако распределение обязанностей зависит от конкретной схемы: кто определяет цели, кто действует по поручению, какие сведения используют-

ся и в каком контексте. Одного факта, что пользователь нажал кнопку отправки, недостаточно, чтобы сделать вывод о соблюдении всех требований. Для организации это повод согласовать использование сервиса с ответственными за персональные данные и информационную безопасность, а не считать вопрос юридически решённым.

Возьмём резюме кандидата. В нём могут быть имя, контакты, история работы и другие сведения, по которым человека можно узнать даже после удаления прямых идентификаторов. Если специалист просит нейросеть «оценить кандидата», он передаёт данные не только о себе. До загрузки нужно свериться с внутренними правилами организации, основаниями такой обработки и условиями сервиса. Если задача сводится к улучшению формулировок, часто достаточно убрать имя, контакты и названия конкретных работодателей, оставив нужный фрагмент опыта. Но даже такую версию следует оценивать по сочетанию деталей.

Удалить диалог — не значит уничтожить всё связанное

В интерфейсе удаление выглядит окончательным: строка пропадает, история становится короче, открыть переписку больше нельзя. Для пользователя это важное действие, но оно прежде всего описывает то, что видно в интерфейсе. Чтобы понять, что происходит с данными дальше, нужно выяснить, что именно сервис подразумевает под удалением. Это может быть удаление из списка чатов, запуск проце-

дуры стирания с серверов, ограничение доступа или сохранение части сведений на определённый срок — например, для безопасности и соблюдения требований. Это разные варианты практики, а не описание работы каждого сервиса. В документации нужно искать, какой из них относится к конкретному продукту и конкретным данным.

Удаление не всегда происходит одновременно во всех системах. История и резервные копии могут обновляться по разным графикам, журнал событий может храниться отдельно от текста, а для загруженного файла может действовать собственный порядок удаления. Если документ индексировали для поиска, стоит выяснить, удаляются ли вместе с исходником связанные данные. Технические детали могут быть описаны кратко, но одно нажатие кнопки не следует считать гарантией мгновенного уничтожения всех копий.

Обратите внимание и на исключения. Условия могут предусматривать сохранение сведений, необходимых для защиты сервиса, расследования злоупотреблений, разрешения споров или выполнения правовых обязанностей. Такие оговорки не означают бессрочного хранения. Но если категории данных и сроки не указаны, приписывать им конкретный порядок удаления нельзя. Отсутствие объяснения лучше зафиксировать как неизвестность.

Отдельный вопрос — данные, уже использованные для оценки или обучения. Удаление исходного диалога из аккаунта не обязательно означает удаление всех наборов данных,

результатов анализа или параметров модели, если такое использование происходило. Но и утверждать, что оно происходило, без прямых сведений нельзя. Проверьте, исключает ли отказ от обучения новые запросы, распространяется ли он на прошлые данные и предусмотрена ли отдельная процедура удаления. Не заменяйте ответ догадками о том, можно ли восстановить сведения из модели.

Чтобы понять последствия удаления, выясните, что именно исчезает при действии в интерфейсе и нужен ли для остальных данных отдельный запрос. Уточните, какие категории могут сохраняться, на каком основании и получают ли уведомление привлечённые исполнители или другие системы, которым данные передавались. Иногда сервис подробно описывает эти процедуры, иногда ограничивается общей формулировкой. Чем чувствительнее материал, тем рискованнее полагаться на слова «удалите данные в настройках» без дополнительных пояснений.

Место обработки и применимое право

Страна пользователя, язык интерфейса и место обработки данных — разные обстоятельства. Русскоязычный интерфейс сам по себе не доказывает, что запрос обрабатывается в России. Наличие российского юридического лица тоже не отвечает на вопрос, где находятся все системы и работают ли привлечённые исполнители в других странах. Это нужно выяснять для конкретного продукта и условий обслуживания.

Ищите сведения о том, где данные хранятся, где обраба-

тываются и могут ли передаваться между регионами. Различайте основное хранилище, резервные копии, техническую поддержку и дополнительные компоненты. Если документы содержат только общее географическое описание, расположение каждой системы может оставаться неизвестным. Для обычного запроса это не всегда существенно, но при передаче персональных или корпоративных материалов такой вопрос может повлиять на выбор сервиса.

Применимое право тоже не определяется одним только местом расположения сервера. Значение могут иметь договорные условия, организация, предоставляющая услугу, характер отношений и тип данных. В российском контексте проверьте, кто выступает оператором персональных данных, какие цели и основания обработки указаны, как описана передача сведений другим лицам и куда пользователь может направить запрос. Законодательство меняется, а его применение зависит от обстоятельств. Поэтому общая формулировка в политике не позволяет сделать юридический вывод о конкретной ситуации; при существенном риске потребуются актуальные документы и консультация профильного специалиста.

Для компании важно также понять, какой именно тариф и набор условий применяются. Публичная политика, договор для организаций, настройки администратора и внутренний регламент могут отвечать на разные вопросы. Запрашивайте документы для фактически используемой версии сервиса, а

не для похожего продукта или другого тарифа. Уточните и то, как меняются правила хранения и использования данных при смене настроек или прекращении договора.

Что найти до передачи чувствительного материала

Необязательно читать каждую страницу условий от начала до конца. Сначала определите продукт, тариф, тип аккаунта и актуальную редакцию документов. Затем выясните, что именно сервис получает вместе с запросом: предыдущие сообщения, файлы, настройки, сведения аккаунта и технические данные.

Уточните, для каких целей обрабатываются сообщения и вложения. Нужны ли они только для ответа или также используются для безопасности, диагностики, оценки качества, обучения и других задач? Если данные могут применяться для обучения моделей или улучшения продукта, проверьте, включено ли это по умолчанию, как отказаться и распространяется ли отказ на разные типы данных.

Затем разберитесь со сроками и доступом. Где и как долго хранятся история, файлы, технические журналы и обращения в поддержку? Что именно означает удаление в интерфейсе, какие есть исключения и как запросить удаление остальных данных? В каких случаях к содержанию могут обращаться сотрудники и подрядчики, какие ограничения и меры защиты для них предусмотрены? Если используется рабочий аккаунт, выясните, может ли администратор видеть диалоги или управлять доступом к ним.

Наконец, проверьте, где обрабатываются данные, кто предоставляет сервис, какие документы и нормы регулируют обработку и куда обращаться с вопросами. Записывайте не только ответы, но и источник: условия, настройки продукта, договор или сообщение поддержки. Расплывчатую формулировку отмечайте как неопределённость, а не как гарантию. Если материал очень чувствительный, отсутствие ясного ответа — веская причина не отправлять исходный текст. Можно ограничиться нужным фрагментом, заменить идентификаторы, выбрать одобренную организацией среду или использовать другой способ работы.

Одна и та же кнопка удаления может означать разные вещи в разных сервисах, а слово «улучшение» — описывать разные процессы. Поэтому оценка не сводится ни к общей тревоге, ни к безусловному доверию: она зависит от конкретных условий, настроек и возможных последствий для ваших данных. В следующей главе эта карта станет основой личной оценки риска — с учётом не абстрактных правил, а того, что может произойти с конкретной передачей.

Своя оценка риска вместо общей тревоги

Один и тот же запрос — «сделай текст яснее» — может быть безопасным, сомнительным или недопустимым. Всё зависит от содержания, возможных получателей и последствий раскрытия. Поэтому вместо общего запрета на нейросети нужен способ оценивать каждую задачу отдельно.

Текст не всегда опасен сам по себе. Риск может возникнуть из сочетания деталей: должности, небольшого населённого пункта, редкого события и примерной даты. По отдельности они мало о чём говорят, но вместе могут указать на человека или организацию. Даже если вероятность такого совпадения невелика, последствия бывают серьёзными. И наконец, удаление переписки в интерфейсе не гарантирует, что все связанные с ней данные сразу уничтожены. Условия хранения, использования и доступа стоит проверять для конкретного сервиса.

Предлагаемая модель не вычисляет риск до процента. Она помогает пройти пять шагов: определить, какие данные нужно защитить; понять, кто может их получить; оценить вероятность нежелательного раскрытия; представить возможный ущерб; выбрать решение. Эта последовательность нужна не для того, чтобы оправдать любой запрет или любое разреше-

ние, а чтобы найти способ снизить риск, не отказываясь от полезной задачи.

Сначала выясните, что именно нужно защитить

Фраза «в тексте есть личное» слишком расплывчата, чтобы на её основе принять решение. Лучше уточнить, какой именно ущерб важно предотвратить.

Речь может идти о раскрытии личности — по имени, телефону, адресу, номеру договора или сочетанию косвенных признаков. Или о разглашении частной информации: сведений о здоровье, отношениях, финансах, семейных обстоятельствах. В рабочих материалах под защитой могут быть данные клиента, внутренняя переписка, проект до объявления, коммерческие условия, сведения о сотрудниках или неопубликованные результаты проверки. Иногда важнее не личность, а доступ: пароль, код подтверждения, ключ к рабочей системе. Тогда последствия начнутся не с огласки, а с того, что кто-то воспользуется полученным доступом.

Спросите себя: что именно станет хуже, если эти сведения окажутся у постороннего? Ответ «мне будет неприятно» тоже важен, особенно если речь о личной переписке. Но чем точнее ответ, тем проще выбрать подходящее действие. «Кто-то потеряет конфиденциальность» — общее описание риска. «По документу можно узнать адрес клиента и обстоятельства его обращения» — уже конкретная задача: убрать документ, адрес и уникальные детали, оставив только суть.

Персональные подробности не всегда одинаково чувстви-

тельны. Для редакции поздравления имя адресата обычно не нужно. Для составления заявления могут иметь значение вид обращения и срок, но не обязательно полный адрес и номер документа. Номер заказа кажется безобидным, однако внутри организации по нему порой можно найти имя, контакты и историю покупок. Оценивать нужно не только сам фрагмент, но и то, с какой другой информацией его можно связать.

Стоит подумать и о том, можно ли решить задачу с меньшим объёмом исходных данных. Чтобы предложить структуру ответа, обычно не нужна вся переписка. Для объяснения сложного термина не требуется скан медицинского заключения с фамилией и датой рождения. А для плана публикации, скорее всего, хватит темы, аудитории и нескольких фактов, уже разрешённых к раскрытию.

Это не просто мера предосторожности. Чем меньше лишних данных попадает в запрос, тем меньше нужно защищать и тем скромнее возможный ущерб.

Кто может получить сведения

Слово «получатель» обычно наводит на мысль об одном конкретном человеке. Но в цифровом сервисе полезнее учитывать разные роли и пути доступа.

Сначала запрос обрабатывают системы самого сервиса. Дальнейшее зависит от условий работы конкретного решения. Сведения могут сохраняться в истории аккаунта; доступ к ним может быть предусмотрен для поддержки, без-

опасности или технического обслуживания; использование запросов для улучшения сервиса может зависеть от настроек и договорных условий. Это не значит, что каждый сотрудник сервиса читает каждый запрос. Но и гарантии, которых нет в условиях, не стоит додумывать самостоятельно.

В рабочей среде могут добавиться другие участники. Например, администратор корпоративного аккаунта может управлять настройками или доступом в пределах своих полномочий. Если к сервису подключены инструменты, расширения или другие платформы, в обработке могут участвовать и они. Схема везде своя: её нужно уточнять по настройкам, внутренним правилам и условиям поставщика, а не переносить с одного сервиса на другой.

Есть и более простой, но частый путь раскрытия — бытовой. Общий аккаунт, открытая вкладка на чужом устройстве, пересланная переписка, демонстрация экрана или копирование текста в общий документ. Сервис может быть настроен приемлемо, но сведения всё равно увидит тот, кому они не предназначались.

Наконец, получателем может стать тот, кому пользователь передаст результат. Ответ нейросети иногда повторяет детали исходного запроса. Если его отправить клиенту, опубликовать или переслать коллеге, риск перейдёт в новый канал. Поэтому контроль не заканчивается нажатием кнопки: нужно проверить и то, что выйдет из сервиса.

Перед передачей текста выясните, сохраняет ли сервис ис-

торию и как ею управлять; используются ли запросы для других целей и можно ли это отключить; кто управляет доступом в выбранном типе аккаунта; что происходит при удалении диалога. Если ответы неясны, это ещё не доказывает, что случится худшее. Но неопределённость становится частью оценки — особенно когда возможный ущерб серьёзен.

Вероятность — не обещание, ущерб — не абстракция

Риск часто пытаются свести к вопросу: «Какова вероятность, что это увидит посторонний?» Точный процент обычно неизвестен. Без данных о конкретном сервисе, его настройках, процессах обработки и возможных инцидентах числовая оценка будет выглядеть точнее, чем она есть. Вместо неё полезнее описать сценарий: что должно произойти для раскрытия данных и насколько этот путь контролируется.

Путь может быть штатным: например, запрос сохраняется в истории аккаунта, доступной пользователю. Он может зависеть от настроек — скажем, от того, разрешено ли использовать переписку для улучшения сервиса. Иногда раскрытие происходит из-за ошибки: человек выбрал не тот аккаунт, открыл общий доступ или случайно приложил файл. Бывают и редкие сбои безопасности. Их нельзя исключить, но оценивать риск только через возможность взлома неверно: обычные настройки и действия пользователя нередко важнее экзотических сценариев.

Для описания вероятности достаточно трёх качественных вариантов. В первом путь раскрытия очевиден или его нельзя ограничить: например, данные уже размещены в общем документе. Во втором такой путь есть, но его вероятность зависит от конкретных настроек и процедур — их можно проверить и изменить. В третьем раскрытие представляется маловероятным, потому что доступ ограничен, а порядок обработки понятен. Однако нулевую вероятность обещать всё равно нельзя. Это не рейтинг сервисов, а способ оценить собственную уверенность в конкретной ситуации.

Затем представьте последствия. Если наружу попадёт обычная формулировка публичного объявления, ущерб может быть небольшим. Если станет известно, кто обращался за помощью и по какому поводу, пострадают частная жизнь, доверие или безопасность человека. Раскрытие пароля может сразу лишить доступа к системе. Утечка ещё не объявленных условий сделки может повлечь финансовые или договорные последствия. Важно оценить не только масштаб ущерба, но и его обратимость: можно ли снять публикацию, заменить пароль, предупредить людей, восстановить доверие? Некоторые последствия уже не исправить после того, как копия разошлась.

Вероятность и ущерб нужно учитывать вместе, но не перемножать в воображаемую оценку по шкале от одного до ста. Даже маловероятный сценарий может быть неприемлем, если последствия тяжёлые, а передача данных легко предот-

вратима. И наоборот, умеренный риск порой оправдан, если сведения малочувствительны, задача действительно полезна, а меры защиты понятны.

Если возможный ущерб велик, спросите не только «насколько это вероятно?», но и «зачем вообще создавать такой путь?». Когда того же результата можно добиться без исходного текста, передача перестаёт быть необходимостью. Это веская причина выбрать другой способ работы.

Три задачи на одном столе

Представим три запроса. Во всех нужно помочь с текстом, но данные и цена ошибки различаются. В каждом случае можно пройти один и тот же путь: понять, что защищаем, кто может получить сведения, насколько вероятно нежелательное раскрытие, к чему оно приведёт и какое решение разумно.

Личный черновик

Человек хочет привести в порядок неотправленное письмо близкому. В нём описан семейный конфликт, названы участники, указаны место работы и обстоятельства, по которым их легко узнать в узком кругу. Письмо нужно не для отправки, а чтобы понять, как выразить просьбу без обвинений.

Здесь важно защитить не только имена и контакты, но и частную историю отношений, эмоциональное состояние, подробности, которые участники могли не соглашаться раскрывать. Если в письме есть угрозы, сведения о насилии,

здоровье, судебном споре или финансовой зависимости, цена ошибки выше: даже косвенное раскрытие может подвергнуть человека опасности или усугубить конфликт.

Текст получит сервис, куда его отправят. Дальше всё зависит от условий, настроек и доступа к аккаунту. Если переписка останется в истории, её могут увидеть люди, у которых есть доступ к устройству или учётной записи. Если ответ затем скопируют в заметки, документ или сообщение, появится ещё один возможный адресат. Не стоит считать, что личный текст обязательно прочитает посторонний, но и отсутствие публичной публикации не гарантирует полной конфиденциальности.

Насколько вероятно раскрытие, зависит от обстоятельств. Если сервис пользователю незнаком, условия не проверены, а аккаунтом пользуются несколько человек, неопределённость заметна. Личный аккаунт на собственном устройстве и изученные настройки сужают некоторые пути доступа. Но даже при понятных условиях остаётся вопрос: зачем передавать узнаваемые подробности, если нужна только помощь с формулировкой?

Последствия могут ограничиться неловкостью и потерей доверия, а могут привести к обострению конфликта, вторжению в частную жизнь или опасности для человека, зависящего от других. Поэтому оценивать текст только по тому, насколько он «секретный», недостаточно: важны контекст и уязвимость участников.

Для обычной редакции целиком передавать письмо не нужно. Можно сформулировать запрос отвлечённо: «Помоги составить спокойную просьбу обсудить распределение домашних обязанностей. Нужно обозначить проблему, не обвиняя человека». Если важны конкретные обстоятельства, их можно обобщить: убрать имена, место работы, точные даты и редкие детали, оставив только то, что влияет на смысл и тон. Если раскрытие может поставить кого-то под угрозу, простого удаления имён недостаточно: сочетание других деталей всё ещё может указать на человека. Тогда лучше попросить общую структуру разговора или обратиться к подходящему специалисту.

Рабочий ответ клиенту

Специалист поддержки готовит ответ на жалобу о задержке доставки. В переписке есть имя клиента, телефон, номер заказа, точный адрес, сведения об оплате, содержание претензии и внутренний комментарий о случившемся на складе. Нужно ответить вежливо, сообщить проверенный статус и не обещать того, на что у специалиста нет полномочий.

Защитить здесь нужно персональные данные клиента, детали заказа и оплаты, а также внутренние сведения о работе компании. Есть и риск случайно переслать клиенту внутренний комментарий или раскрыть данные другого покупателя. Даже привычные на вид детали в сочетании могут открыть доступ к истории заказа или помочь установить личность.

Помимо сервиса, через который обрабатывают запрос, до-

ступ к материалам в рабочем процессе могут иметь администраторы корпоративного аккаунта и участники внутренней системы, если она подключена. Вместо догадок стоит выяснить, одобрена ли нейросеть для работы с клиентскими данными и какие правила действуют в организации. Личный аккаунт сотрудника и инструмент, утверждённый компанией, — не обязательно одно и то же. Но и корпоративная подписка сама по себе не заменяет проверки условий и внутренних ограничений.

Риск зависит от конкретной конфигурации. Если организация проверила сервис, ограничила доступ, установила правила обработки и разрешила использовать данные определённого типа, неопределённость ниже. Если сотрудник копирует переписку в случайно выбранный инструмент и не знает, как долго тот хранит сведения и кто может их увидеть, оценить риск трудно. Рабочее время и должность пользователя сами по себе не делают клиентские данные безопаснее.

Раскрытие может привести к жалобе, потере доверия, нарушению внутренних обязательств и дополнительным правовым последствиям — в зависимости от характера данных, роли организации и обстоятельств обработки. Утечка номера заказа, телефона и адреса опаснее, чем раскрытие обезличенного описания задержки. Если в обращении есть сведения о здоровье, финансовом положении или другие чувствительные детали, цена ошибки становится ещё выше.

Если для ответа достаточно сути, отправлять всю пере-

писку не нужно. Нейросети можно дать обезличенное задание: «Клиент сообщает, что оплаченный заказ задержан на два дня. Нужен спокойный ответ: признать неудобство, сообщить, что статус уточняется, не обещать компенсацию и оставить место для проверенной информации». Здесь нет имени, контактов, номера заказа и точного адреса. Проверенный статус специалист добавит сам.

Это не значит, что любые рабочие материалы нужно обезличивать одинаково. В утверждённой корпоративной среде иногда допустимо работать с данными определённой категории. Но решение должно опираться на правила организации и настройки сервиса, а не на удобство конкретного сотрудника. Если инструмент не разрешён для работы с клиентскими сведениями, сокращение текста снизит риск, но не отменит запрет.

Публичный текст

Сотрудник муниципальной службы редактирует объявление о работе в выходные. Основные сведения уже подготовлены к публикации: часы приёма, адрес учреждения, порядок записи. Черновик написан тяжёлым языком, и автор хочет сделать его понятнее.

Если факты согласованы и предназначены для публикации, конфиденциальность основного текста, вероятно, невысока. Однако в черновик могли попасть неутверждённые сведения, прямой телефон конкретного сотрудника, фамилия заявителя или внутренний комментарий. В публичном доку-

менте нередко остаются непредназначенные для читателей примечания и данные людей, которых никто не собирался упоминать.

Запрос обработает сервис, а после публикации объявление увидит широкая аудитория. Если версия ещё не прошла согласование, передача черновика может преждевременно раскрыть планы. А если в тексте есть личный телефон сотрудника, после публикации он станет доступен неопределённому кругу людей.

Для утверждённых сведений передача обычно несёт меньше риска, чем для закрытого рабочего материала. Но пометка «публичное» не означает, что текст можно отправлять целиком. Проект может раскрыть планы раньше времени, содержать ошибочную дату или указывать на конкретное учреждение и человека благодаря сочетанию открытых деталей. Кроме того, нужно учитывать условия и настройки сервиса, а не только будущую аудиторию объявления.

Если в сервис попадёт общедоступное расписание, последствия могут быть минимальными. Но преждевременное раскрытие изменения режима работы способно вызвать путаницу, увеличить нагрузку на сотрудников или сорвать подготовку. Публикация личных данных затронет частную жизнь. А если нейросеть добавит неподтверждённый факт, проблема возникнет уже после выхода объявления.

Передавать стоит только ту версию, которую разрешено раскрывать и в которой нет лишних личных или внутренних

деталей. Для редакции обычно достаточно самого текста объявления — без черновых комментариев, истории согласования и данных заявителей. После обработки автору нужно перепроверить даты, адреса, условия записи и остальные факты: правдоподобный ответ ещё не означает, что он верен.

Этот пример показывает, что публичная задача не всегда связана с низким риском, а личная — с высоким. Само название категории ничего не решает. Важны содержание, доступ, возможный путь раскрытия и цена ошибки.

Три уровня решения

После разбора не обязательно выставлять задаче числовую оценку. Достаточно выбрать один из трёх вариантов и понимать, почему он подходит.

Можно использовать. Так поступают, если в запросе нет чувствительных, идентифицирующих или конфиденциальных сведений либо их разрешено передавать в выбранной среде. Возможный ущерб невелик, а условия обработки достаточно понятны. Например, можно попросить объяснить сложный термин, придумать структуру выступления на общую тему или отредактировать утверждённое объявление без скрытых комментариев. Но даже в этом случае незачем отправлять лишнее: короткий запрос обычно предпочтительнее.

Можно использовать после сокращения или преобразования данных. Это промежуточный и часто самый полезный вариант. В исходнике есть реальные детали, но для резуль-

тата хватит обобщённого описания. Имена можно заменить ролями, номера убрать, точные даты обозначить диапазоном, адреса и контакты исключить, редкие обстоятельства обобщить. Из письма клиента оставить суть проблемы и желаемый тон ответа, из рабочего отчёта — тип задачи и ограничения, из личного текста — цель сообщения и эмоциональный тон, не раскрывая историю целиком.

Преобразование должно сохранять то, что действительно влияет на результат. Если убрать всё значимое, нейросеть начнёт додумывать контекст, и пользы станет меньше. Поэтому сначала сформулируйте задачу, а затем оставьте минимальный набор необходимых для неё фактов. Просьбы «напиши ответ клиенту» недостаточно, если важны срок, статус и допустимые обещания. «Составь нейтральный ответ о поддержке на два дня, не обещая компенсацию» — уже подходящее задание для черновика, если проверенные данные сотрудник добавит сам.

Лучше не передавать. Такой вариант нужен, когда возможный ущерб серьёзен, данные нельзя надёжно обезличить или передача запрещена правилами организации. Это могут быть пароли и коды доступа, не обработанные документы с данными клиентов, особо чувствительные материалы, закрытая информация о безопасности или сведения о человеке, чьё положение может ухудшиться в случае раскрытия. Конкретные границы зависят от содержания и обстоятельств: редкое сочетание деталей тоже может сделать чело-

века узнаваемым.

«Лучше не передавать» не обязательно означает «отказаться от задачи». Нейросеть можно попросить описать общий порядок действий, подготовить пустой шаблон, составить список вопросов для внутренней проверки или отредактировать искусственный пример без реальных данных. Если у организации есть утверждённый инструмент и регламент для такой информации, следует действовать по ним. Но подменять установленную процедуру личной уверенностью в том, что «ничего не случится», нельзя.

Если решение сомнительно, пройдите короткий путь: назовите данные, которые собираетесь отправить; определите возможные роли получателей; уточните, от чего зависит раскрытие; представьте худшее реалистичное последствие; проверьте, получится ли выполнить задачу с меньшим объёмом сведений. Если вы не можете уверенно сказать, кто и на каких условиях обработает текст, это не автоматический запрет на любой запрос. Но это повод сократить исходник или выбрать способ, который не требует передачи.

Личные границы вместо общей тревоги

У каждого могут быть собственные правила, но лучше, чтобы они были не набором случайных запретов, а понятной системой. Какие данные я не отправляю ни при каких обычных обстоятельствах? Какие передаю только в проверенной рабочей среде? Что могу обобщить, если задача личная?

Для одного человека разумным правилом будет не загру-

жать личные документы и переписку, а просить помощь на основе краткого описания. Для специалиста поддержки — не передавать клиентские сообщения в неутверждённый сервис и не вводить идентификаторы даже в рабочем чате. Для автора публичных материалов — использовать только согласованные факты и проверять, не остались ли в черновике заметки для внутренней команды. Такие правила помогают принять решение в тот момент, когда нужно отправить запрос.

Границы можно устанавливать не только по чувствительности данных, но и по цене ошибки. Опечатка в публичном черновике и раскрытие пароля требуют разного подхода. В первом случае достаточно вычитать текст перед публикацией. Во втором нельзя рассчитывать на исправление после факта: пароль нужно вообще не передавать. Чем сложнее отменить последствия, тем меньше причин полагаться на удачу.

Не нужно добиваться абсолютной уверенности — её часто невозможно получить. Достаточно понимать, на каком основании вы принимаете решение. «Организация одобрила этот сервис для таких данных» — проверяемый довод. «Наверное, запрос никто не увидит» — нет. «Я убрал все детали, без которых задача решается» — конкретная мера. «В тексте нет фамилии, значит, он анонимен» — необоснованный вывод, если оставшиеся подробности указывают на человека.

Безопасность при работе с нейросетью — не единый за-

прет и не безусловное доверие. Это выбор с учётом пользы задачи, чувствительности данных, устройства конкретного сервиса и возможной цены ошибки. Следующий шаг — научиться добиваться нужного результата, не отдавая исходник целиком: передавать нейросети задачу и необходимый контекст, а не всю историю, из которой эта задача возникла.

Просить результат, не отдавая исходник

Оценка риска помогает понять, стоит ли обращаться к нейросети и чем может обернуться ошибка. Следующий шаг — решить, сколько данных передать: оставить в запросе то, что влияет на ответ, и убрать то, что лишь создаёт ощущение полноты. Это не всегда компромисс. Часто так задача становится точнее.

Перед вами длинная цепочка писем с клиентом. В ней есть номер заказа, телефон, адрес доставки, история переносов, внутренние пометки и подписи сотрудников. Нужно лишь подготовить вежливый ответ: объяснить ситуацию и не пообещать лишнего. Самый быстрый путь — скопировать переписку целиком и попросить нейросеть «учесть весь контекст». Но задача и материал для её решения — не одно и то же. Для черновика может хватить нескольких обобщённых фактов и ясных ограничений.

Промпт на диете

Вот типичный избыточный запрос:

«Подготовь ответ клиенту по этой ситуации. Учитывая всю переписку ниже, договор, данные заказа и внутренние комментарии. Нужно быть вежливыми, объяснить задержку, ответить на вопрос о сроках и возврате, не допустить проти-

воречий».

К просьбе часто добавляют всю цепочку сообщений и документы. Это понятно: никто не хочет упустить деталь, способную изменить смысл ответа. Но большой объём сам по себе не делает запрос точнее. В переписке могут оказаться ненужные для черновика сведения: личные контакты, номера заказов, подписи, внутренние оценки, повторяющиеся фрагменты и данные других участников. А важное ограничение — например, сотрудник пока не вправе подтверждать новую дату — может затеряться среди мелочей.

Начинать лучше не с вопроса «какой документ загрузить?», а с вопроса «какой результат мне нужен?». Иногда нужен готовый текст, иногда — план ответа, список вопросов для уточнения или несколько вариантов формулировки. Для каждого результата потребуется свой объём контекста.

Контекстный минимум — это сведения, без которых изменятся точность, форма или безопасность ответа. Он не обязательно состоит из минимума слов. Короткое, но двусмысленное описание иногда хуже подробного, а длинная переписка может не добавить к задаче ничего полезного.

Сначала цель, потом материал

Вернёмся к ответу клиенту. В исходной цепочке десятки деталей, но на черновик влияют лишь несколько: заказ задержан, клиент спрашивает о сроке и возврате, точная дата пока не подтверждена, сотрудник может сообщить только проверенную информацию. Для выбора тона достаточно до-

бавить, что нужно ответить уважительно, не обвинять клиента, не обещать компенсацию и не придумывать срок.

Остальное можно не передавать. Имя клиента не нужно, чтобы определить структуру ответа. Номер заказа не поможет подобрать тон, а адрес не имеет значения, если речь не о логистике. Дата в письме важна, если нужно восстановить последовательность обещаний, но может быть лишней, когда требуется лишь шаблон для похожих случаев.

Проверка проста: изменится ли результат, если убрать конкретную деталь? Если нет, её обычно не стоит включать. Если да, подумайте, нельзя ли заменить её обобщением, условным значением или пустым полем. И отдельно проверьте, разрешено ли передавать её выбранному сервису. То, что информация нужна для хорошего ответа, ещё не значит, что её безопасно отправлять.

Перед запросом полезно прояснить четыре вещи: какой результат нужен — текст, план, список вопросов или варианты формулировки; для кого он предназначен; какие факты действительно меняют ответ; какие ограничения нельзя нарушать. Вместо просьбы «прочитай всё и разберись» получится задача с ясными границами. Это помогает и сберечь данные, и сделать ответ более управляемым.

Четыре версии одной задачи

Для примера возьмём условную ситуацию, не связанную с реальным заказом. Покупатель ждёт товар, отправка задержана на три дня из-за переноса поставки. Новая дата неиз-

вестна. Клиент спрашивает, когда получит заказ и можно ли отказаться от покупки. Сотрудник вправе проверить статус, но не может подтвердить срок или компенсацию, пока не уточнит условия.

Сравним, как меняется запрос.

Первая версия — передать весь источник. Пользователь вставляет цепочку писем, данные заказа и внутренние комментарии, а затем просит подготовить ответ. Такой подход полезен, если нужно разобраться в обещаниях и противоречиях. Но нейросеть может принять устаревшую дату за актуальную, перепутать слова клиента и сотрудника или включить в ответ сведения, которые не должны попасть наружу. Кроме того, вместе с нужными фактами передаётся многое лишнее.

Вторая версия — описать задачу и добавить только важный контекст:

«Подготовь черновик ответа клиенту на русском языке. Условная ситуация: заказ задержан на три дня из-за переноса поставки. Точную дату отправки пока не подтвердили. Клиент спрашивает о сроке и возможности отказаться от заказа. Сотрудник может пообещать проверку статуса, но не новую дату и не компенсацию. Тон спокойный и уважительный. Не придумывай условия возврата. До 90 слов».

Фактической точности здесь меньше, зато границы задачи обозначены яснее. Черновик может выглядеть так:

«Здравствуйте. Приносим извинения за задержку заказа. Сейчас мы проверяем обновлённую информацию о сроках и сообщим вам подтверждённые данные до [срок, который можно обещать]. Если ожидание для вас неудобно, мы уточним доступные варианты отказа от заказа и возврата по действующим условиям. Спасибо, что сообщили о ситуации».

В тексте оставлено поле для сведений, которые нужно проверить. Нейросеть не получила имя, номер заказа или адрес, и от неё не просили самостоятельно устанавливать условия возврата. Однако отправлять такой черновик нельзя, пока сотрудник не подставит реальный срок и не сверит фразу о возврате с применимыми условиями.

Третья версия — попросить не готовый текст, а план:

«Составь план ответа клиенту на случай задержки заказа, когда новая дата ещё не подтверждена. Нужны четыре пункта: признать неудобство, сообщить проверенный статус, обозначить следующий шаг, не обещать неподтверждённую дату или компенсацию. Добавь пять вопросов, которые сотрудник должен проверить по заказу перед отправкой ответа».

Такой запрос даёт структуру и список проверок, не претендуя на знание конкретной ситуации. Пользователь сверяет пункты с перепиской у себя и сам заполняет фактические поля. Это удобно, когда важнее последовательность действий, чем автоматический пересказ источника.

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.