Nevel

БЕЗОПАСНОСТЬ

Потоки данных и маршруты обработки

Путь запроса в облаке и on-prem, разрешённые модельные маршруты, восстановление масок и отдельный изолированный профиль.

Облако / В контуре

https://docs.nevel.sh/security/data-flow/

Единицей проверки в Nevel является полный запрос к обработчику. Он может содержать сообщение пользователя, историю диалога, инструкции проекта, найденные фрагменты базы знаний, извлечённый текст файлов и результаты инструментов. Защита только последней фразы пользователя оставила бы остальной контекст за пределами контроля.

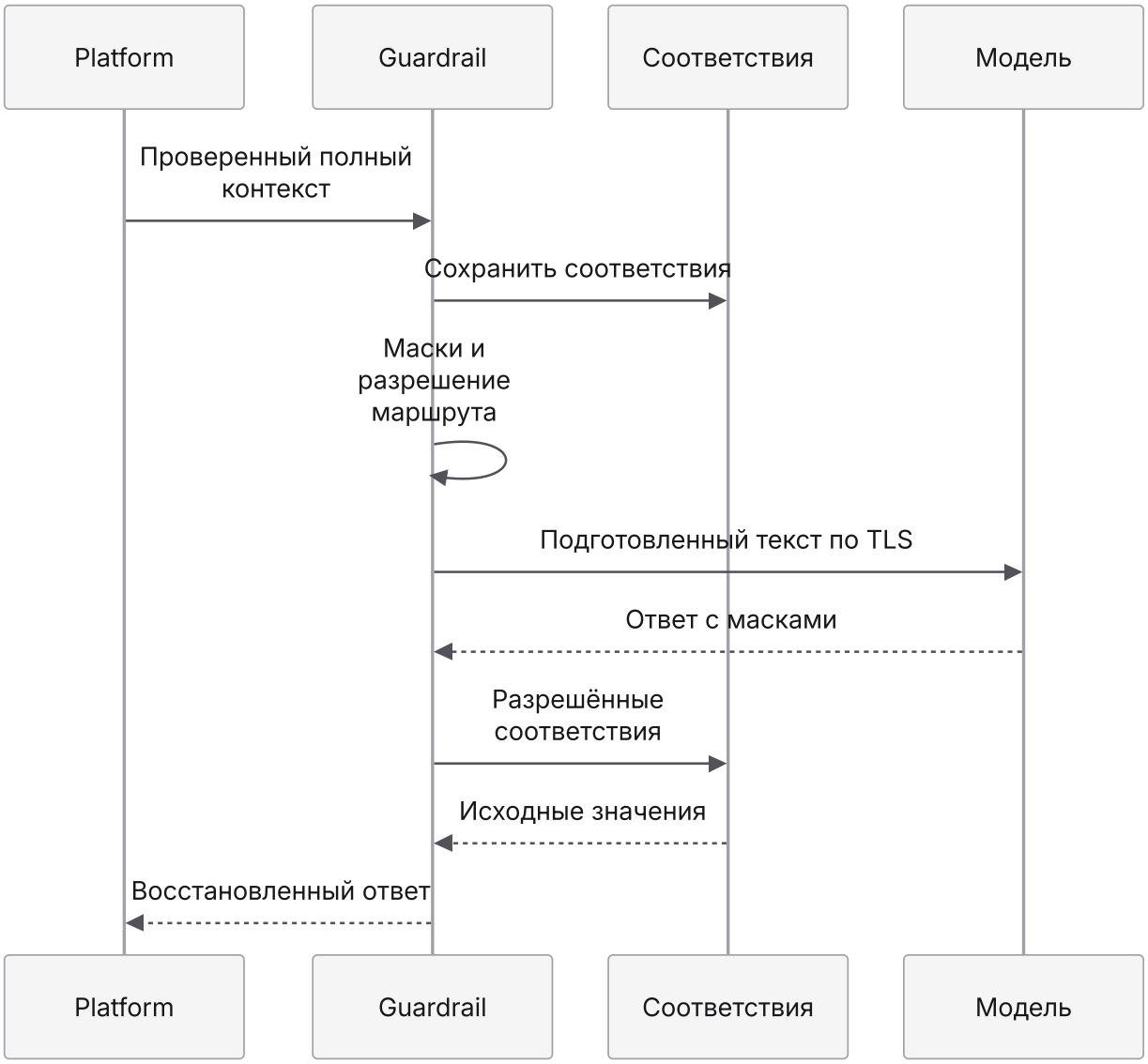
Поток описывается в двух направлениях: подготовка данных перед моделью и обработка результата после модели. Отдельно учитываются служебные ответвления — журналы, временные файлы, индексы, кэши и резервные копии. Они тоже могут содержать корпоративные сведения, хотя пользователь не видит их в чате.

Путь защищённого запроса

1. **Приём.** Gateway проверяет ключ или пользовательскую сессию, состояние доступа, рабочее пространство и ограничения запроса. Создаётся идентификатор для связывания дальнейших событий.
2. **Проверка объектов.** Platform проверяет права на историю, проект, файлы и подключения. Данные недоступного объекта не извлекаются для модели.
3. **Сборка контекста.** Из разрешённых источников формируется фактическое содержание запроса. Результат инструмента считается новым входом, а не доверенной инструкцией.
4. **Обнаружение и маскирование.** DLP/NER выделяет поддерживаемые чувствительные сущности; исходные значения заменяются типизированными идентификаторами. Соответствия сохраняются в защищённой области текущего запроса.
5. **Классификация и маршрут.** Содержание, метки, политика организации и ограничения модели определяют допустимый периметр. Запрет имеет приоритет перед предпочтением пользователя и автоматическим выбором модели.
6. **Обработка моделью.** Разрешённый получатель получает подготовленный контекст по защищённому каналу. При ошибке резервный маршрут обязан удовлетворять тем же ограничениям.
7. **Обратная обработка.** В ответе восстанавливаются только действительные соответствия разрешённого запроса. Незнакомая или просроченная маска не вызывает поиск по чужим данным.
8. **Возврат и аудит.** Результат получает уполномоченный клиент. Журнал связывает идентичность, политику, маршрут, маскирование, результат и ошибку без обязательной записи полного содержания.

СХЕМА 1

Маскирование и восстановление



Пример преобразования

Ниже используются вымышленные данные. Формат масок иллюстрирует принцип и не является обязательной схемой ответа API.

```
Исходный запрос:
Подготовь письмо Анне Примеровой по адресу anna@example.invalid
о переносе встречи. Телефон для связи: +7 000 000-00-00.

Содержание после обнаружения сущностей:
Подготовь письмо [PERSON_1] по адресу [EMAIL_ADDRESS_1]
о переносе встречи. Телефон для связи: [PHONE_NUMBER_1].

Ответ модели:
[PERSON_1], сообщаем о переносе встречи ...

После разрешённого восстановления:
Анна Примерова, сообщаем о переносе встречи ...
```

Модель получает смысл задачи и заменители, а таблица исходных значений остаётся внутри защищённой области. Но маскирование не скрывает факт переноса встречи, коммерческие условия или другие немаскированные детали. Для документа, содержание которого целиком запрещено передавать наружу, правильное решение — локальный маршрут либо отказ, даже если все известные идентификаторы обнаружены.

Что меняется в облаке

В облаке Platform и Guardrail размещены в российской инфраструктуре Nevel. Модель может быть self-hosted у Nevel в РФ, например DeepSeek, либо находиться у российского или глобального провайдера. При обращении к отдельному провайдеру подготовленный запрос пересекает границу инфраструктуры Nevel. Это описание сетевой границы; фактическая страна обработки определяется отдельно для всей цепочки, включая доставку запросов, поиск, преобразование файлов и инструменты.

Для запроса составляется цепочка: инициатор → Platform → Guardrail → каждый промежуточный обработчик → модель → обратная обработка. Применение одним участником режима без обучения не доказывает такой же режим у остальных. Отсутствие сохранения истории в интерфейсе также не подтверждает отсутствие технического хранения у получателя.

Данные соответствий не включаются в запрос к модели. Их содержимое не должно попадать в заголовки, диагностический ответ, трассировку, события SIEM или текст сообщения об ошибке. Результат восстановления возвращается только по исходному авторизованному маршруту.

Что меняется в on-prem

При on-prem Platform и её рабочие хранилища находятся у заказчика. После сборки контекста и проверки Guardrail запрос направляется внутренней модели или разрешённому получателю за пределами инфраструктуры заказчика: российскому провайдеру, self-hosted модели Nevel в РФ либо глобальному провайдеру. Место Platform не снимает требований к данным и получателям.

В реестре отдельно фиксируются место выполнения модели, владелец endpoint и география. Например, DeepSeek, размещённый Nevel в РФ, и внешний API с той же моделью имеют разные цепочки обработки. Ответ из внешнего маршрута возвращается в установленную у заказчика платформу для обратной обработки и выдачи уполномоченному клиенту.

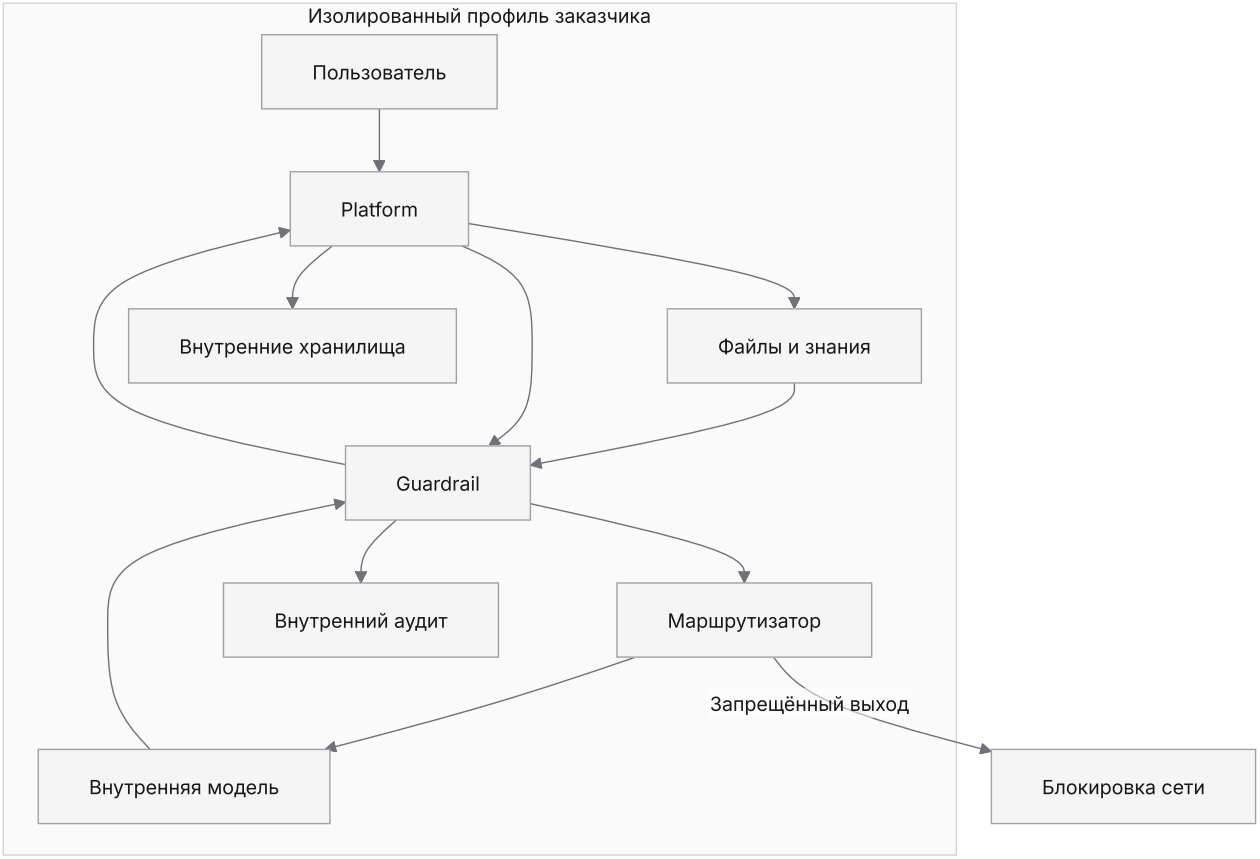
Резервный маршрут выбирается только из вариантов, заранее разрешённых для категории данных. Его использование отражается в аудите. При отсутствии допустимой альтернативы запрос завершается отказом; SDK и фоновые задачи не должны самостоятельно включать скрытый внешний fallback. Матрица вариантов связывает место платформы и модельные маршруты.

Изолированный профиль

Внутри контура находится вся рабочая цепочка. Используются внутренние модели, внутренний обработчик файлов, внутреннее векторное хранилище и внутренние инструменты. Даже если запрос выглядит безобидным, политика закрытого контура не разрешает автоматический внешний fallback.

СХЕМА 2

Изолированный рабочий маршрут



Проверка отсутствия внешней обработки проводится по всем сценариям: OCR изображения, разбор сложного PDF, построение embeddings, вызов инструмента, создание файла, повторная попытка и диагностика сбоя. On-prem с разрешённым облачным векторизатором остаётся локальной установкой платформы, но не соответствует изолированному профилю.

Файлы, история и повторные запросы

Файл может породить несколько объектов: оригинал, извлечённый текст, изображения страниц, фрагменты, векторы, предварительный просмотр и итоговый артефакт. Каждый наследует контекст организации и исходные ограничения доступа. При изменении метки исходного документа производные представления учитывают новое ограничение до дальнейшей выдачи.

История диалога повторно передаёт модели ранее написанные сообщения. Поэтому правило защиты применяется к собранной истории, а не только к новым данным. Старое решение «разрешено» не должно бессрочно действовать после смены политики или модели. Если срок хранения соответствия маски истёк, это не повод возвращаться к исходным значениям из чужого запроса или отправлять их во внешнюю модель без повторного контроля.

Вызов инструмента продолжает тот же процесс. Модель предлагает параметры, сервер проверяет разрешённость действия, инструмент возвращает результат, после чего этот результат проходит контроль перед следующим модельным вызовом. Полномочия инструмента не определяются текстом модели. Для фоновых и запланированных запусков учитываются текущий доступ владельца и актуальность секрета подключения.

Потоковый ответ и частичный результат

Потоковая передача требует аккуратной обработки границ фрагментов: маска может разделиться между несколькими порциями текста. Восстановление выполняется по целой распознанной маске в пределах запроса. Неполный фрагмент не используется для приблизительного подбора значения. Если соединение прерывается, журнал отличает частичный ответ от успешного завершения.

Повторный запрос может привести к новому вызову модели и новой стоимости. Поэтому клиент связывает повторы с исходной операцией, а расследование учитывает количество фактических отправок. Отмена на стороне браузера не означает, что уже отправленный внешний запрос был отменён у получателя или что все временные объекты уничтожены мгновенно.

Контрольная матрица

Проверка	Ожидаемый результат	Доказательство
Чувствительное значение только в старом сообщении	Оно также проходит контроль	Синтетический захват перед моделью и событие маскирования
Запрещённый документ в результате инструмента	Следующий вызов не уходит по запрещённому маршруту	Решение политики и отсутствие исходящего вызова
Поддельная маска из другого запроса	Чужое значение не восстанавливается	Ответ, событие отказа, изоляция соответствий
Локальная категория и отказ внутренней модели	Внешний fallback не происходит	Сетевой журнал и событие маршрутизатора
Отказ DLP или хранилища соответствий	Защищённый маршрут не отправляет исходный текст	Ошибка, идентификатор, отсутствие вызова модели
Запрос с удалённым файлом	Файл и его фрагменты больше не попадают в контекст	Проверка доступа и поиск по индексу

Подробности: Guardrail, хранение, файлы и RAG. Юридическая оценка внешней передачи изложена в 152-ФЗ; техническая замена идентификаторов не подменяет её.