Nevel

БЕЗОПАСНОСТЬ

Хранение, сроки и удаление данных

Жизненный цикл оригиналов, масок, журналов, индексов и резервных копий; базовые сроки и доказательства удаления.

Облако / В контуре

https://docs.nevel.sh/security/storage/

Удаление в Nevel рассматривается как жизненный цикл всех представлений данных. Один документ может существовать в виде оригинала, извлечённого текста, фрагментов поиска, векторов, кэша, временного файла и резервной копии. Удаление карточки из интерфейса само по себе не доказывает прекращение выдачи всех этих представлений.

Для каждой категории определяются цель хранения, владелец, расположение, доступ, срок и событие завершения. Срок таблицы масок не равен сроку истории диалога, а срок технического журнала не задаёт срок хранения исходного договора. Документы заказчика обрабатываются по установленным им целям и договорному поручению.

Категории и расположение

Категория	Назначение	Облако	On-prem
Диалоги и проекты	Продолжение работы и совместный контекст	Хранилища облачной поставки с изоляцией пространства	Хранилища заказчика
Оригиналы и артефакты	Работа с документами и результатами	Файловое хранилище облачной поставки	Внутреннее файловое хранилище
Извлечённый текст и RAG	Поиск и подготовка разрешённого контекста	Обработчики и индекс по конфигурации	Индекс установки у заказчика; место OCR и embeddings определяется маршрутом
Соответствия масок	Восстановление разрешённого ответа	Защищённое хранилище в России	Защищённое внутреннее хранилище
Аудит	Расследование и контроль политик	Российская инфраструктура, отдельно разрешённый экспорт	Аудит установки у заказчика, отдельно разрешённые получатели SIEM
Замаскированные тела	Дополнительная диагностика, если включена	Отдельно ограниченное хранение	Отдельно ограниченное внутреннее хранение
Конфигурация	Пользователи, маршруты, правила, подключения	Служебные хранилища поставки	Служебные хранилища заказчика
Резервные копии	Восстановление после сбоя	Площадки профиля резервирования	Площадки, заданные политикой резервирования заказчика

Таблица описывает хранилища Platform, а не полный состав экземпляров у модельного получателя. Если on-prem обращается к российскому провайдеру, self-hosted модели Nevel в РФ или глобальной модели, переданный контекст и его хранение у получателя учитываются отдельно. В изолированном профиле все рабочие стадии, аудит и копии остаются внутри заданной границы.

Метаданные тоже могут требовать защиты: заголовок файла, идентификатор пользователя, адрес отправителя и текст ошибки способны раскрывать сведения о человеке или процессе. Поэтому минимизация относится не только к телу документа.

Базовый профиль сроков Guardrail

Следующие параметры относятся к базовому профилю Guardrail версии 1.2. Они дают конкретную исходную конфигурацию, которую можно проверить при внедрении; договор и паспорт установленного окружения определяют применённые значения. Эти сроки не объявляются требованиями 152-ФЗ или свойством любого произвольного развёртывания.

Данные Guardrail	Значение базового профиля	Диапазон настройки	Последствие истечения
Соответствия масок	24 часа	От 1 часа до 90 дней	Старое соответствие больше не используется для восстановления
Журналы аудита	90 дней	От 30 дней до 3 лет	Записи выводятся из активного хранения по политике
Замаскированные тела запросов	Выключено	Выключено либо от 1 часа до 90 дней	Диагностическое содержание удаляется по сроку
Конфигурация организации	На период договора	По жизненному циклу поставки и обязательствам хранения	Закрытие и удаление в процедуре завершения

Таблица не задаёт срок всех пользовательских чатов и файлов Platform. Для них учитывается рабочая цель, политика организации, действие пользователя и прекращение договора. Сохранение чата в истории не требует бессрочно сохранять все соответствия масок каждого старого модельного вызова.

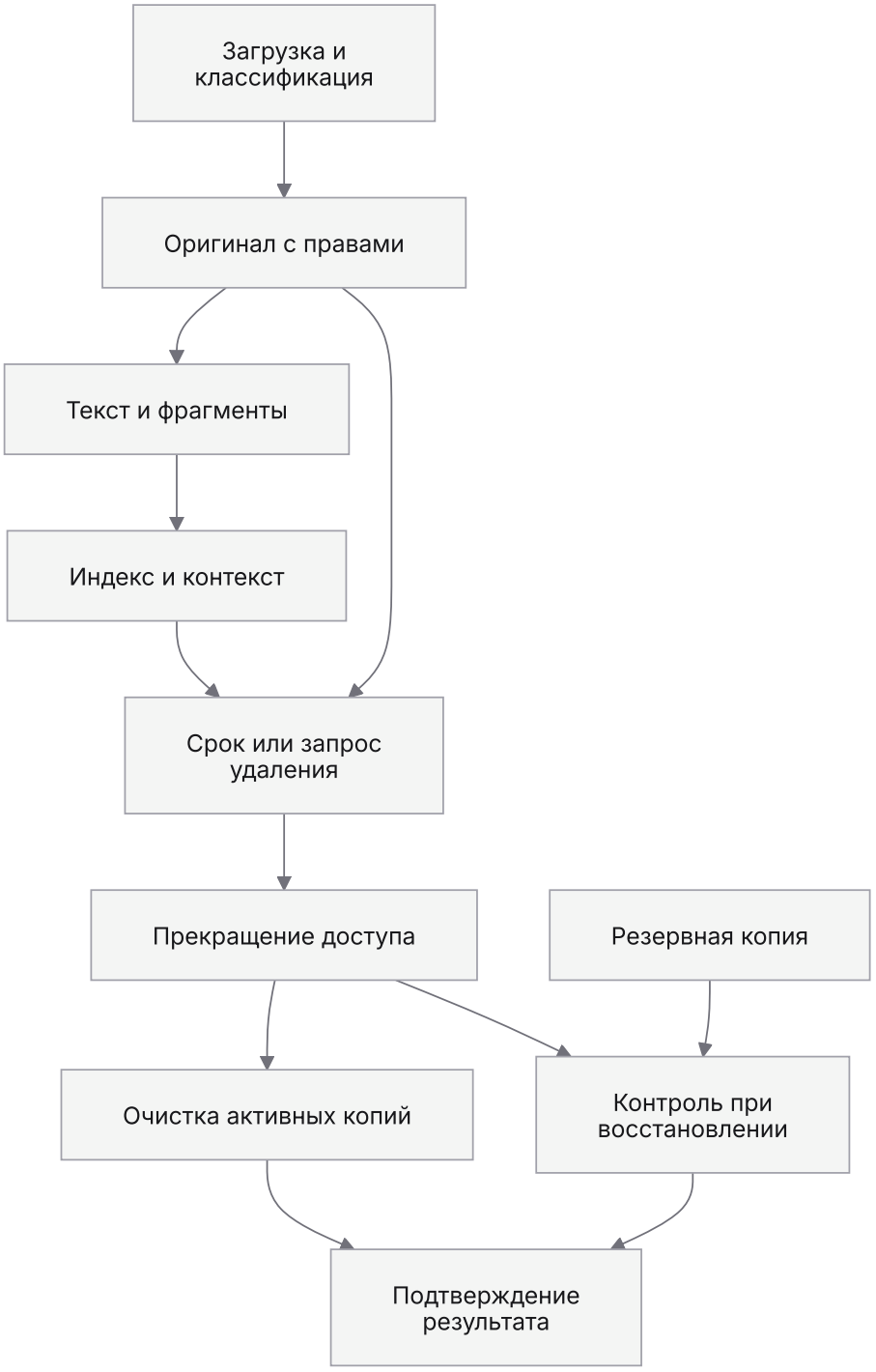
Слишком короткий срок соответствий может помешать восстановлению запоздавшего ответа. Слишком длинный увеличивает объём потенциально раскрываемых исходных значений. Поэтому срок соотносится с реальной продолжительностью задачи, включая очереди, инструменты и повторные обращения, а не выбирается по максимальному доступному диапазону.

Автоматическое завершение срока

Данные получают правило срока при создании или изменении категории. Фоновая очистка удаляет истёкшие записи и фиксирует результат без копирования удаляемого содержания в журнал. Пользовательский путь не должен продолжать раскрывать объект только потому, что физическая очистка ещё выполняется.

СХЕМА 1

Жизненный цикл документа



Изменение срока не должно незаметно продлевать жизнь данных сверх разрешённой цели. Для нового правила фиксируются инициатор, прежнее и новое значение, область применения и поведение для уже существующих объектов. Сроки активных данных и резервных копий рассматриваются раздельно.

Удаление по запросу

Удаление может относиться к конкретному запросу и соответствиям, объекту Platform, данным субъекта либо всей организации. Для каждой операции сначала проверяется полномочие инициатора и область. Запрос «удалить мои данные» не означает право пользователя удалить документы других сотрудников или обязательный след чужих операций.

Область удаления	Что входит в проверку
Соответствие конкретного запроса	Маски и исходные значения, невозможность последующего восстановления
Файл	Оригинал, превью, извлечённый текст, фрагменты, векторы, временные ссылки и кэш
Диалог или проект	Сообщения, вложения и производные объекты в определённой области; общие ссылки
Данные субъекта	Поиск по установленным идентификаторам и источникам, оценка оснований сохранения отдельных данных
Организация при завершении	Пользовательские и служебные данные, соответствия, диагностические тела, ключи, конфигурация, копии и экспорт

Удаление таблицы соответствий прекращает возможность штатного обратного восстановления масок, но не удаляет автоматически исходный файл из проекта. Аналогично удаление файла из Platform не управляет самостоятельно копией, которую пользователь скачал на рабочее устройство или передал разрешённой внешней системе.

При запросе субъекта юридическая служба определяет основание и объём действий; техническая команда исполняет конкретную операцию. Существование других оснований обработки и обязательного хранения оценивается отдельно, а не заменяется общей кнопкой удаления. Процедура и сроки по закону описаны в 152-ФЗ.

Резервные копии

Базовый профиль Guardrail версии 1.2 предусматривает инкрементальную копию каждые 4 часа, полную — ежедневно, хранение 30 дней, отдельную российскую площадку, AES-256 и ежемесячную проверку восстановления. В состав включаются конфигурация, политики, аудит и действующие соответствия. Эти параметры относятся к названному профилю; резервирование Platform и внутренней инфраструктуры определяется составом конкретной поставки.

Копии защищаются отдельными правами. Компрометация пользователя приложения не должна давать доступ к архиву всей организации. Доступ к копии и доступ к ключу её расшифрования контролируются раздельно. Проверка восстановления подтверждает не только запуск сервиса, но и корректность прав, политик маршрутизации и состава данных.

Нельзя безусловно обещать мгновенное физическое уничтожение отдельной записи во всех неизменяемых резервных копиях. Процедура фиксирует, когда активная выдача прекращена, какие копии ещё существуют, как ограничен их доступ и когда они истекут. При восстановлении применяется реестр удалений или эквивалентный предусмотренный механизм, чтобы ранее удалённые данные не вернулись в рабочую выдачу.

Временные данные и внешние получатели

Извлечение файлов создаёт рабочие каталоги, изображения страниц и промежуточные результаты. Они очищаются после задачи и по аварийному сценарию. Ошибка обработчика не должна оставлять доступный следующему пользователю файл. Кэш также ограничивается организацией и полномочиями; истечение TTL не заменяет немедленное прекращение выдачи объекта при отзыве доступа.

Для любого разрешённого внешнего маршрута, из облака или on-prem, срок у получателя определяется его действующими условиями и настройками конкретного API. Политика Nevel не удаляет автоматически уже переданный экземпляр у другого участника. В реестре маршрутов учитываются модельный провайдер и промежуточные сервисы, включая OpenRouter для маршрутов API, которые его используют. При изолированном профиле внешние экземпляры в рабочем маршруте не создаются; одно только размещение Platform on-prem этого не гарантирует.

Как подтвердить результат

Доказательство удаления связывает основание, объект, инициатора, время, выполненные действия, результат и обнаруженные исключения. В подтверждение не копируется удалённое содержание целиком. Технический журнал успешного SQL-запроса или исчезновение карточки не доказывают очистку поиска, файлового хранилища и резервных восстановлений.

При автоматизированной обработке приказ Роскомнадзора № 179 от 28.10.2022 предусматривает акт об уничтожении и выгрузку из журнала; они хранятся три года с момента уничтожения. Состав реквизитов и порядок дополнения недостающих в выгрузке сведений разобраны в мерах защиты РФ. Подтверждение отражает фактические действия установленной системы. Официальная публикация приказа № 179.

Негативные проверки

Создайте синтетический документ с уникальной контрольной фразой, дождитесь индексации и проверьте выдачу. Затем удалите его и повторите поиск, запрос модели, скачивание по старой ссылке, обращение по известному идентификатору и проверку временного хранилища. После тестового восстановления копии контрольная фраза не должна возвращаться в разрешённую выдачу вопреки зарегистрированному удалению.

Для масок проверьте истечение минимального тестового срока, восстановление после истечения, обращение другого пространства и повтор старого идентификатора. Для аудита и диагностических тел проверьте отдельные сроки и отсутствие скрытого включения тел по умолчанию. Протокол фиксирует реальные параметры окружения и границы проверенных копий.

Связанные вопросы: ключи, файлы и RAG, эксплуатация и резервирование. Пересмотрено 8 сентября 2026 года; нормативная актуальность имеет границы, указанные в мерах РФ.