Nevel

БЕЗОПАСНОСТЬ

Идентификация, SSO и права

Корпоративный вход, права дирекций на источники и функции, массовые назначения, проверка полномочий и отзыв доступа.

Облако / В контуре

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

Nevel различает идентификацию пользователя, аутентификацию и разрешение конкретного действия. Успешный вход подтверждает, кто обращается к системе. Доступ к проекту, файлу, ассистенту, модели или подключению определяется отдельно. Корпоративный SSO не делает сотрудника администратором и не открывает ему все документы компании.

Внешнее приложение работает под сервисным API-ключом, а сотрудник — под личной учётной записью. Общая учётная запись отдела лишает журнал возможности установить инициатора и усложняет отзыв доступа при увольнении. Поэтому персональные пользователи, сервисные интеграции и административные операции разделяются.

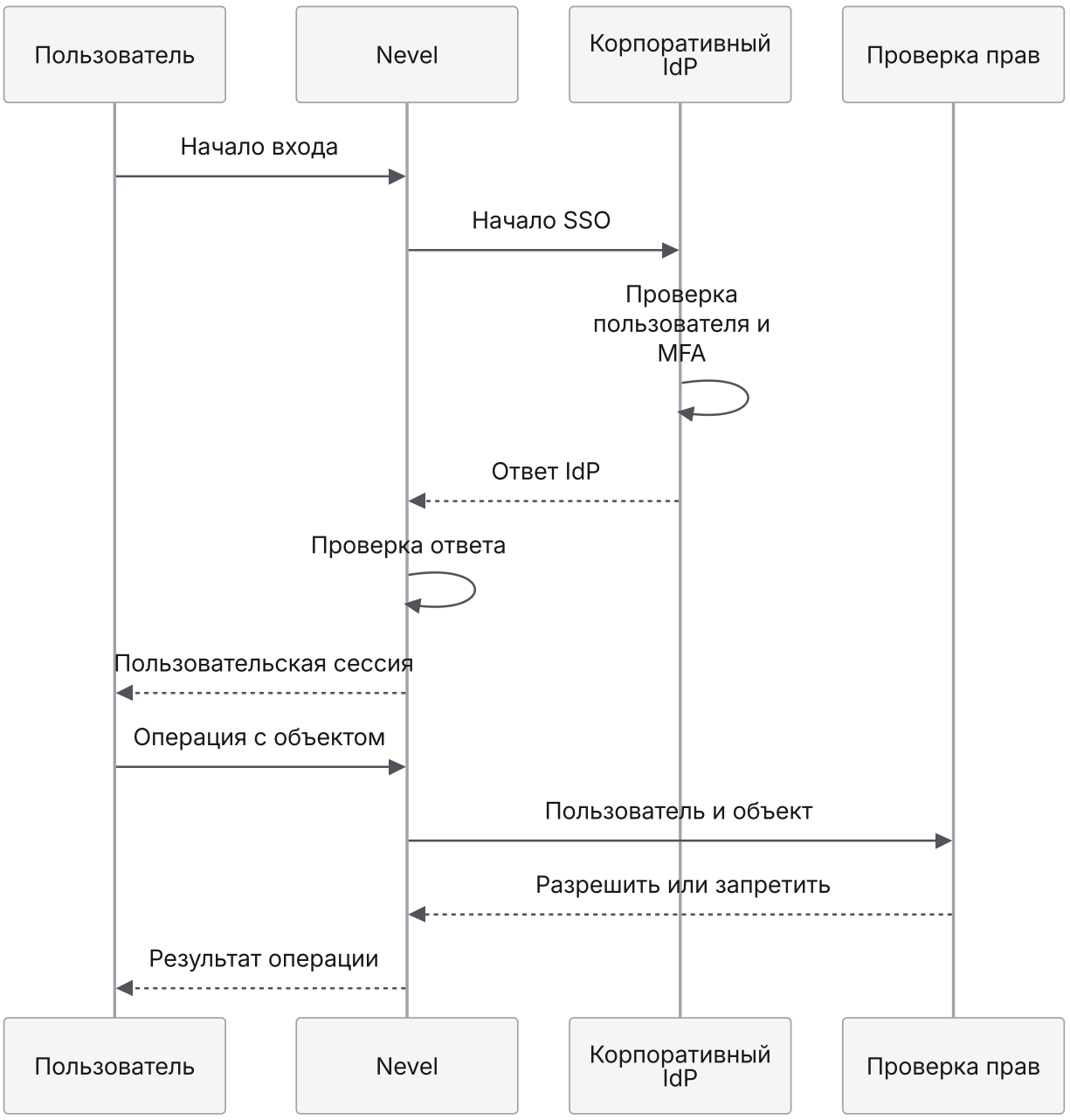
Корпоративная аутентификация

Для корпоративной интеграции используются предусмотренные поставкой механизмы OAuth 2.0 и SAML. OAuth 2.0 описывает делегирование доступа и сам по себе не является универсальным доказательством пользовательской идентичности. Конкретный сценарий входа должен определять доверенный источник идентичности, атрибут стабильного пользователя и проверку полученного ответа. SAML-сценарий использует доверие к корпоративному поставщику идентичности и проверку утверждения о пользователе.

При SSO учитываются издатель, адрес назначения, получатель, срок действия, связь с начатым входом и защита от повторного использования ответа. Для SAML проверяются подпись и доверенный сертификат поставщика идентичности. Недействительный, просроченный или предназначенный другой системе ответ не создаёт сессию. Совпадение адреса электронной почты само по себе не позволяет связать неподтверждённую внешнюю учётную запись с привилегированным пользователем.

СХЕМА 1

Вход через корпоративный источник



Требование MFA может исполняться корпоративным IdP в процессе входа. Приёмка проверяет, что приложение использует именно этот обязательный маршрут и что альтернативная учётная запись не даёт обойти корпоративное требование. Применение конкретного продукта IdP, автоматического создания пользователей или отдельного протокола синхронизации определяется конфигурацией интеграции; наличие SSO не означает автоматически поддержку любого каталога и метода provisioning.

Роли и административные полномочия

В модели рабочего пространства различаются OWNER, ADMIN и MEMBER: владелец, администратор и участник. Владение определяет максимальный уровень управления пространством; администратор выполняет разрешённые операции настройки; участник использует доступные ему функции. Практическое право определяется матрицей разрешений, состоянием пользователя и областью операции.

Область	Обычный участник	Административная операция
Собственные диалоги	Создание и использование в пределах политики	Не требует права читать чужие диалоги
Общие проекты и файлы	Только предоставленный уровень доступа	Выдача и отзыв совместного доступа
Пользователи	Работа под своей идентичностью	Приглашение, изменение роли, прекращение доступа
Модели и инструменты	Использование разрешённых вариантов	Настройка доступных функций и маршрутов обработки
Политики Guardrail	Исполнение установленных правил	Изменение категорий, маршрутов и режима защиты
Подключения	Личное подключение или явно разрешённое общее	Разрешение интеграции и управление областью использования
Аудит	Не равен общему доступу к журналу	Просмотр и экспорт в отдельной области полномочий

Управление пользователями не должно автоматически означать право на содержимое всех файлов. Разграничение проверяется по конкретной операции и объекту, а не только по видимости кнопки в интерфейсе. Сервер повторяет проверку даже при прямом API-запросе с известным идентификатором.

Пространства, проекты, ассистенты и группы

Рабочее пространство задаёт организационный контекст. Внутри него проекты, файлы и ассистенты могут иметь собственные правила совместного использования. Личный ассистент доступен владельцу; общий предоставляется определённым участникам; доступность внутри организации ограничена членством и политикой. Ссылка является способом найти ресурс, а право определяется правилами публикации и авторизацией.

При передаче ассистента проверяются отдельно его инструкции, исходные документы и подключения. Нельзя считать, что публикация конфигурации ассистента разрешает использование личного токена автора всеми сотрудниками. Аналогично совместный проект не обязан открывать любой диалог автора, если общий доступ предоставлен только файлам или инструкциям.

Группы и организационные признаки связывают сотрудников с дирекциями и административной матрицей. Они не образуют автоматически строгую иерархию подразделений. В таблице участников основная группа выбирается отдельно от роли команды; проектные назначения позволяют одному человеку работать с несколькими направлениями. Название должности или группы само по себе не выдаёт права владельца, доступ к источникам или разрешение инструмента.

Для совместной работы нужны одновременно подходящий состав участников, права на объекты и разрешённые действия. Например, сотрудник финансов может участвовать в общем проекте закупок, не получая доступа ко всем материалам закупочной дирекции. Общий ассистент не должен извлекать для него документы, недоступные в его текущем контексте.

Как применяется матрица дирекций

Матрица фиксирует связь **сотрудник → дирекция и проекты → ассистенты и источники → разрешённые действия**. Для каждого набора назначений определяются ответственный за состав людей, владелец материалов и администратор политики. Эти роли могут принадлежать разным сотрудникам: руководитель дирекции подтверждает рабочую потребность, а право изменить настройки принадлежит уполномоченному администратору.

При проверке действия учитываются несколько независимых условий:

1. **Идентичность и членство.** Пользователь действует под правильным аккаунтом в нужной организации; приглашение ещё не подменяет принятого членства.
2. **Право на объект.** Доступны конкретный проект, диалог, ассистент, файл или подключение, участвующие в операции.
3. **Разрешённое действие.** Пользователю разрешено читать, изменять, публиковать, запускать инструмент либо выполнять административную операцию — в зависимости от запроса.
4. **Политика обработки.** Для этих данных разрешены модель, получатель и вспомогательные обработчики. Доступ к документу не означает разрешения передать его любому провайдеру.

Разрешение одной части не компенсирует отсутствие другой. Например, сотрудник может читать финансовый документ, но не публиковать его как общий источник. Или ему доступен веб-поиск, но конкретные сведения нельзя включать во внешний поисковый запрос. Доступность кнопки подтверждает лишь видимость элемента; сервер проверяет фактическую операцию.

Когда у сотрудника несколько проектных назначений, каждое основание предоставления права должно оставаться понятным. Снятие доступа одного проекта не отменяет другое действующее назначение автоматически. Поэтому при отзыве проверяется итоговое право, включая прямую выдачу доступа и другие проекты. Обязательный запрет для категории данных или маршрута сохраняется независимо от количества разрешающих назначений.

Проверяемый сценарий	Ожидаемый результат
Сотрудник закупок обращается к своему ассистенту и регламенту	Получает результат в пределах назначенного доступа
Тот же сотрудник открывает закрытый источник финансов	Содержимое не предоставляется без отдельного назначения
Финансист участвует в общем проекте	Видит материалы общего проекта, а не все материалы второй дирекции
Участник пытается изменить роль коллеги	Операция требует отдельного административного права
Сотрудник открывает общедоступного ему ассистента с недоступным источником	Публикация ассистента не расширяет права на источник

Матрица не должна существовать только как описание отдела. Её проверяют через реальные объекты и действия: список участников, публикацию ассистента, доступ к документу и запуск разрешённого инструмента. Пример матрицы и порядок назначения находятся в администрировании команды.

Контроль массовых назначений и импорта

Массовые приглашения и импорт оргструктуры решают разные задачи. Приглашение связывает адрес, организацию и роль будущего участника. Импорт дополнительно сопоставляет существующие аккаунты, дирекции, проектные назначения и их изменения. Успешная отправка приглашений не подтверждает, что всем сотрудникам уже выдан правильный доступ к материалам.

Контроль начинается с идентичности. Источник состава должен содержать устойчивую связь с человеком; имя используется для отображения, но не для объединения аккаунтов. Смена адреса, одинаковые имена и несколько строк одного сотрудника требуют однозначного сопоставления. Конфликтующие строки не должны создавать привилегированный аккаунт по предположению. Неподтверждённая связь между аккаунтом и сотрудником остаётся основанием не применять конкретное назначение до исправления данных.

До применения администратор видит разницу между существующим и требуемым состоянием. В проверку входят новые участники, смена дирекции, новые доступы, административные роли и отзываемые назначения. Для каждого существенного изменения должно быть понятно, какой сотрудник затронут, какой объект или функция меняются и откуда взято требуемое состояние.

Добавление и обновление, merge, сохраняет пользователей и назначения вне обрабатываемого набора. Отсутствие строки в выгрузке не является указанием на отзыв. **Замена состава выбранной области** предполагает, что её источник полный; перечень снимаемых назначений просматривается отдельно. Исключение из проекта, снятие группы и прекращение членства в команде учитываются как разные изменения.

В журнале массовой операции сохраняются инициатор, время, область, источник или версия набора, просмотренные изменения и результат применения. Для разбора важны выполненные, не изменившиеся и ошибочные строки. Сам исходный кадровый файл содержит сведения о сотрудниках и должен храниться в предназначенной для этого административной области, а не становиться общей базой знаний ассистента.

При частичном выполнении итоговые права проверяются по фактическому состоянию. Повтор исправленных строк не должен создавать дубликаты аккаунтов или приглашений. Если результат неизвестен из-за обрыва связи, сначала сопоставляются участники и назначения, затем выполняются оставшиеся изменения. Отсутствие ответа клиенту не доказывает отмену серверной операции.

Для исправления ошибочного импорта используется перечень обратных изменений: снять лишние права, восстановить необходимое назначение и проверить новый запрос. Возврат состава не означает удаления созданных сотрудниками материалов или всего аккаунта. Подробные этапы подготовки, предпросмотра и восстановления приведены в инструкции импорта дирекций.

Сервисные ключи и собственный ключ модели

Ключ Nevel API связан с владельцем, рабочим пространством, статусом, сроком действия и ограничениями использования. Приложению выдаётся отдельный ключ по назначению; производственная интеграция и тестирование не используют один общий секрет. Ограничения расходов и модели уменьшают масштаб возможной компрометации, но не заменяют запрет доступа к данным.

Собственный ключ провайдера модели хранится и используется отдельно от ключа доступа к Nevel. Первый определяет право обратиться к провайдеру, второй — право приложения воспользоваться маршрутом Nevel. Использование ключа заказчика не отменяет Guardrail, допустимый перечень моделей или правила обработки информации. География провайдера остаётся свойством маршрута, а не владельца ключа.

Ротация и отзыв описаны в управлении ключами. Секрет не публикуется в ассистенте, системной инструкции, общем файле или примере кода. Модель получает возможность вызвать разрешённый инструмент через сервер, а не значение секрета для самостоятельного использования.

Отзыв и жизненный цикл доступа

При уходе сотрудника прекращаются членство, активные разрешения и использование его личных подключений. Отдельно рассматриваются API-ключи, фоновые задания, общие ассистенты и документы, владельцем которых он был. Передача владения не означает перенос личных секретов другому человеку. Объекты, нужные компании, передаются управляемо с сохранением происхождения и прав.

Для перевода между дирекциями сначала составьте перечень сохраняемых и снимаемых назначений. Основная группа, роль команды, доступ проекта, доступ к ассистенту и полномочия внешнего подключения — разные записи. Если изменить только группу для аналитики, прямое право на старый источник может остаться. Для увольнения аналогично недостаточно удалить человека из одного проекта, оставив его членом команды с другими назначениями.

Практический порядок отзыва:

1. **Определите область.** Перевод, завершение временного проекта и уход из организации требуют разного набора изменений. Зафиксируйте сохраняемые проектные права.
2. **Передайте общие объекты.** Укажите нового ответственного за рабочие ассистенты, документы, подключения и задания. Секреты заново выдаются по нужному назначению, а не копируются из личной учётной записи.
3. **Снимите прежние назначения.** Измените состав группы и проектов, права на источники, административные полномочия и доступ к подключениям в соответствующей области.
4. **Разберите действующие способы доступа.** Проверьте аккаунт, корпоративный вход, пользовательские сессии, сервисные ключи и фоновые задания. Отзыв одного способа не означает отзыва остальных.
5. **Проверьте новое действие.** Выполните обращение к прежде доступному закрытому источнику под затронутой идентичностью и проверьте результат. При переводе отдельно выполните рабочую задачу новой дирекции.
6. **Сверьте журнал и матрицу.** Ожидаемые назначения должны совпасть с фактическими; лишний доступ расследуется до завершения административной операции.

Отзыв в IdP и прекращение доверия к уже созданной сессии — разные события. Проверка внедрения устанавливает, когда изменение доходит до приложения, какие действующие сессии прекращаются и может ли сохранённый токен выполнить новый запрос. Не следует считать выход из браузера удалением данных или отзывом всех сервисных ключей.

Фоновая задача проверяет права в момент выполнения. Если доступ к источнику отозван после настройки расписания, следующий запуск не продолжает извлечение по устаревшему разрешению. Ошибка фиксируется без автоматического перехода на привилегированное общее подключение.

Отзыв доступа ограничивает дальнейшие обращения, но сам по себе не стирает сведения, уже показанные человеку или сохранённые им вне платформы. Уже открытый экран также может отображать ранее загруженный результат. Поэтому контроль проводится новым запросом, повторным скачиванием, открытием старой ссылки и следующим запуском задания; закрыть вкладку и увидеть пустой экран недостаточно.

Различия двух установок

В облаке корпоративный IdP связывается с облачным приложением по разрешённым защищённым маршрутам. Политика организации определяет допустимые домены, пользователей и способы входа. В on-prem корпоративный вход настраивается для установленной у заказчика платформы; разрешённый IdP и модели являются отдельными подключениями. В изолированном профиле все необходимые компоненты идентификации и проверки находятся внутри заданного контура, поэтому рабочий запрос не требует внешнего сервиса аутентификации.

Аварийный административный доступ отделяется от повседневного входа, ограничивается процедурой и журналируется. Он нужен для восстановления управления при отказе IdP, но не должен превращаться в незаметный постоянный обход MFA и корпоративного увольнения.

Негативные проверки

Проверьте вход с просроченным ответом IdP, повтор ответа, неправильного издателя и чужого получателя. После успешного входа проверьте доступ к файлу другого пространства и изменение роли через прямой запрос участника. Отзовите пользователя во время сессии, затем попробуйте новый чат, скачивание файла, старую ссылку и фоновую задачу.

Для ключей проверьте истечение, отзыв, превышение ограничения и запрос запрещённой модели. Для совместных объектов — доступ нового участника, бывшего участника и человека с одной ссылкой без членства. Результат фиксируется вместе с событием аудита и версией матрицы прав.

Для дирекций подготовьте отдельные тестовые аккаунты с разными назначениями. Проверьте разрешённые действия каждой дирекции, межфункциональный проект, перевод и снятие прямого права на источник. После изменения повторите как обычное действие в интерфейсе, так и проверяемое серверное обращение к тому же объекту. Известный идентификатор объекта не должен давать обход прав.

Для массового импорта проверьте повтор того же набора, конфликт двух записей сотрудника, неизвестную группу, частичную ошибку и замену состава ограниченной области. Итог проверяется по назначениям и рабочим действиям, а не только по сообщению о завершении. Сохраните ожидаемое состояние, фактический результат и необходимые обратные изменения, чтобы проверить исправление без повторного массового вмешательства.