Права доступа в /task: персональные и групповые, поля и история, закрытие страниц

06.11.2026 · PDF-версия статьи с сайта cms.dolinais.ru

В /task права доступа — это не просто «кто может войти», а гибкий механизм, который определяет, кто и что может видеть и делать внутри проекта. В отличие от базовых ролей, здесь можно настраивать персональные права и группы, ограничивать доступ к задачам и разделам, управлять видимостью полей и истории изменений, а также закрывать целые страницы проекта от посторонних. В этой статье разберём, зачем это нужно, как настроить и какие преимущества вы получите.

Живое демо /task

Ниже — интерактивная демонстрация /task. Можно переключать виды, открывать задачи и пробовать действия.

ДЕМО /TASK — КАНБАН: ПРИМЕР ДАННЫХ

Задачи в блоке не заданы.

Зачем нужны расширенные права доступа

Стандартные роли (администратор, участник, наблюдатель) хороши для небольших команд, но когда проектов много, а в них участвуют внешние подрядчики, стажёры или несколько отделов, возникает потребность в точечном контроле. Расширенные права позволяют:

- Скрыть конфиденциальные задачи (например, по безопасности или бюджету) от большинства сотрудников.
- Ограничить редактирование критичных полей (срок, бюджет, приоритет) только ответственными.
- Запретить просмотр истории изменений для аудита, чтобы избежать утечек.
- Закрыть целые страницы проекта (дашборды, отчёты) от случайных глаз.

Без такого контроля легко получить хаос: кто-то случайно меняет дедлайн, другой видит зарплаты, третий удаляет задачу. Гибкие права решают эти проблемы.

Персональные права и группы прав

Персональные права назначаются конкретному пользователю и действуют поверх его роли. Например, вы можете дать стажёру право редактировать только свои задачи, но запретить удалять чужие. Или разрешить внешнему консультанту видеть задачи определённого раздела, но не весь проект.

Группы прав — это именованные наборы разрешений, которые можно применять к нескольким пользователям сразу. Удобно для типовых ролей: «Разработчик», «Тестировщик», «Менеджер проекта». Создав группу один раз, вы назначаете её новым сотрудникам без ручной настройки каждого права.

Комбинируя персональные права и группы, вы выстраиваете многоуровневую систему: группа задаёт базовый

уровень, а персональные настройки уточняют его для конкретного человека. Важно помнить о приоритете: обычно запрещающие правила имеют больший вес, чем разрешающие, но в /task можно гибко управлять этим порядком.

Как настроить персональные права и группы

1. Перейдите в настройки проекта (или глобальные настройки, если права сквозные).
2. Откройте раздел «Права доступа».
3. Создайте группу: нажмите «Добавить группу», введите название и отметьте нужные разрешения (например, «Просмотр задач», «Редактирование задач», «Удаление задач», «Управление спринтами»).
4. Назначьте группу пользователям: выберите сотрудников и примените группу.
5. Для точечной настройки выберите конкретного пользователя и нажмите «Персональные права». Здесь можно переопределить любые разрешения из группы.
6. Сохраните изменения.

Совет: начинайте с минимально необходимых прав и расширяйте по мере необходимости. Это принцип наименьших привилегий.

Охват задач и разделов

Права можно применять не ко всему проекту, а к отдельным задачам или разделам (например, к списку задач, канбан-доске, конкретной папке). Это называется **охватом**. Вы можете указать, что группа «Подрядчики» видит только задачи с меткой «Внешние» или только раздел «Интеграции». Остальные задачи для них останутся невидимыми.

Охват настраивается в том же разделе прав: при создании правила выберите область действия — «Весь проект», «Выбранные разделы» или «Задачи с определёнными атрибутами» (например, по метке или типу). Такой подход удобен, когда нужно разделить зоны ответственности между командами.

Пример: в проекте «Мобильное приложение» есть разделы «iOS», «Android» и «Дизайн». Разработчики iOS видят только свой раздел, а тестировщики — все три, но без права редактирования. Менеджер видит всё и может менять любые поля.

Права на поля и историю

Даже если пользователь имеет доступ к задаче, не всегда нужно, чтобы он мог менять все её поля. **Права на поля** позволяют разрешить или запретить редактирование конкретных атрибутов: например, разрешить менять статус и исполнителя, но запретить трогать срок, бюджет и приоритет. Это особенно важно для полей, влияющих на отчётность или финансы.

Настройка прав на поля осуществляется в разделе «Поля» внутри прав доступа: выберите поле и укажите, каким группам или пользователям разрешено его редактировать. Просмотр полей тоже можно ограничить — например, скрыть поле «Бюджет» от всех, кроме финансового отдела.

Права на историю управляют доступом к журналу изменений задачи. По умолчанию историю видят все, у кого есть доступ к задаче, но можно ограничить её просмотр только администраторами или менеджерами. Это

полезно, если в комментариях или изменениях могут содержаться конфиденциальные данные.

В /task история включает системные сообщения, изменения полей и комментарии. Ограничение прав на историю не скрывает саму задачу, но делает невидимыми детали её изменения.

Закрытие страниц проекта

Страницы проекта — это дашборды, отчёты, таймлайн, аналитика и другие представления. Иногда нужно закрыть их от определённых пользователей, даже если они имеют доступ к задачам. Например, страницу «Аналитика» с финансовыми показателями должны видеть только руководители.

Для этого в настройках прав выберите страницу и укажите, кому она доступна. Можно закрыть страницу полностью (никто, кроме администратора) или ограничить кругом лиц. Закрытие страниц не влияет на доступ к задачам — это независимая настройка.

Также можно закрыть страницу проекта от внешних пользователей, оставив им только список задач. Это удобно для подрядчиков, которым не нужно видеть общую статистику.

В чём плюсы

- **Безопасность данных:** конфиденциальная информация (бюджеты, персональные данные, стратегические задачи) доступна только тем, кому положено.
- **Гибкость:** можно комбинировать группы, персональные права, охват и права на поля, создавая сложные сценарии без дублирования пользователей.
- **Снижение рисков ошибок:** ограничение редактирования критичных полей предотвращает случайные изменения.
- **Аудит и соответствие:** ограничение доступа к истории помогает выполнять требования регуляторов и внутренних политик.
- **Удобство администрирования:** группы прав экономят время при онбординге и переводах сотрудников.

Права доступа в /task — это мощный инструмент, который стоит освоить, если вы работаете с внешними командами или в большой организации. Настройте их один раз, и система будет автоматически защищать ваши данные.

Источник: https://cms.dolinais.ru/prava-dostupa-v-task-personalnye-i-gruppovye-polya-i-istoriya-zakrytie-stranic