

Доступ по операциям

Настроить доступ по операциям

Версия 8.0



Эта документация предоставляется с ограничениями на использование и защищена законами об интеллектуальной собственности. За исключением случаев, прямо разрешенных в вашем лицензионном соглашении или разрешенных законом, вы не можете использовать, копировать, воспроизводить, переводить, транслировать, изменять, лицензировать, передавать, распространять, демонстрировать, выполнять, публиковать или отображать любую часть в любой форме или посредством любые значения. Обратный инжиниринг, дизассемблирование или декомпиляция этой документации, если это не требуется по закону для взаимодействия, запрещены.

Информация, содержащаяся в данном документе, может быть изменена без предварительного уведомления и не может гарантировать отсутствие ошибок. Если вы обнаружите какие-либо ошибки, сообщите нам о них в письменной форме.

Содержание

| | |
|---|----------|
| Настроить доступ по операциям | 4 |
| Настроить доступ по операциям в объекте раздела | 5 |
| Настроить приоритет прав доступа по операциям объекта | 8 |
| Настроить доступ по операциям в объекте детали | 10 |

Настроить доступ по операциям

ПРОДУКТЫ: **ВСЕ ПРОДУКТЫ**

В этой статье рассмотрена настройка прав **доступа к бизнес-данным**. Доступ к бизнес-данным подразумевает выполнение CRUD-операций с данными (создание, чтение, редактирование и удаление) и выполняется через настройку прав доступа к соответствующим объектам системы.

Если вы только начинаете знакомство с Creatio, то рекомендуем ознакомиться с концепцией прав доступа на объекты Creatio в онлайн-курсе [Управление пользователями и ролями. Права доступа](#).

Права доступа на объекты можно ограничить на следующих уровнях:

- **По операциям.** Ниже будет рассмотрена настройка прав на выполнение операций с данными, содержащимися в двух разных объектах системы — в разделе и на детали.
- **По записям.** Подробнее: [Настроить доступ по записям](#).
- **По колонкам.** Подробнее: [Настроить права доступа на колонки](#).

Доступ к действиям системы предоставляется с помощью системных операций. Операции в объекте не следует путать с системными операциями. Настройки прав доступа к действиям системы выполняются в разделе [*Доступ к операциям*] дизайнера системы. Подробнее: [Настроить права доступа на системные операции](#).

На заметку. Существует четыре системные операции, которые отменяют любые другие настройки прав на объект: “Просмотр любых данных” (код “CanSelectEverything”), “Добавление любых данных” (код “CanInsertEverything”), “Изменение любых данных” (код “CanUpdateEverything”) и “Удаление любых данных” (код “CanDeleteEverything”). Пользователь с доступом к этим операциям получит права независимо от настроек в разделе [*Доступ к объектам*].

По умолчанию в приложении настроены права:

- Для организационной роли “**All employees**” (“Все сотрудники”) предоставляется доступ на операции чтения, создания, редактирования и удаления записей всех объектов. Пользователи, входящие в роль “All employees”, будут иметь права на указанные операции, даже если доступ по операциям не используется и переключатель выключен.
- Для организационной роли “**All portal users**” (“Все пользователи портала”) запрещен доступ на выполнение любых операций с записями системы. Чтобы пользователи, входящие в роль “All portal users”, могли видеть на портале свои записи и данные своей организации, необходимо настроить в разделах, доступных на портале, права доступа по операциям.
- Для организационной роли “**System administrators**” (“Системные администраторы”) настроен доступ на системные операции “Добавление любых данных”, “Чтение любых данных”, “Изменение любых данных”, “Удаление любых данных”, имеющие более высокий приоритет, чем настройки, заданные в разделе [*Права доступа на объекты*].

Настроить доступ по операциям в объекте раздела


Пример. Выполним настройку прав доступа к разделу [*Продажи*].

У менеджеров по продажам должны быть все права на записи раздела, кроме удаления.

У их руководителей должен быть неограниченный доступ к записям.

У одного из сотрудников с ролью “Секретари” должна быть возможность просматривать записи раздела, а для остальных секретарей раздел [*Продажи*] должен быть скрыт.

Важно. Если удалить роль “All employees” из области настройки доступа по операциям, а затем выключить переключатель “Использовать доступ по операциям” и применить изменения, то пользователи не смогут видеть записи объекта.

1. Перейдите в дизайнер системы, например, по кнопке , и откройте раздел настройки доступа к объектам по ссылке “**Права доступа на объекты**”.
- Обратите внимание, признаки в колонках [*Доступ по операциям ограничен*], [*Доступ по записям ограничен*] и [*Доступ к колонкам ограничен*] в реестре объектов не редактируются. Они устанавливаются автоматически в зависимости от того, какой тип администрирования доступа (по операциям, по записям, по колонкам) используется для каждого объекта. Если ни один из типов доступа к объекту не ограничен (не установлен ни один из признаков), то все пользователи имеют полный доступ к объекту и имеют право на создание, чтение, редактирование и удаление данных объекта.
2. Выберите необходимый объект из списка или с помощью строки поиска. Например, чтобы настроить права доступа к разделу [*Продажи*], установите фильтр “Разделы” и выберите объект “Продажа”. Кликните по его заголовку или названию — откроется страница настройки прав доступа к объекту раздела [*Продажи*] (Рис. 1).

На заметку. Подробнее о выборе объекта читайте в статье [Права доступа на объекты](#) (онлайн-курс).

Рис. 1 — Выбор объекта раздела и переход на страницу настройки прав доступа

Права доступа на объекты

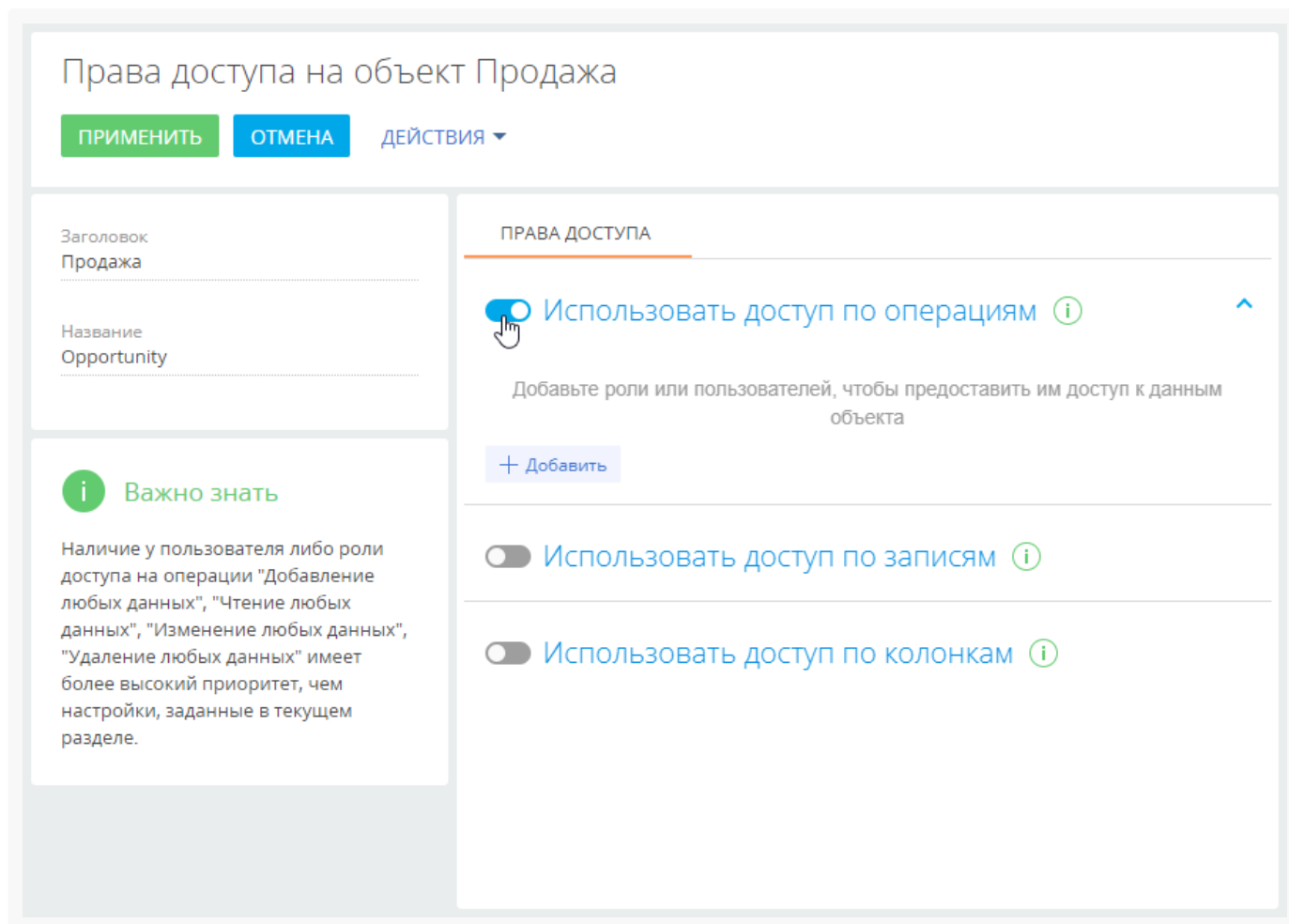
ЗАКРЫТЬ ДЕЙСТВИЯ ▼

☰ Все объекты ▼ 🔍 Поиск

| Заголовок ▲ | Название | Доступ по операциям ограничен | Доступ по записям ограничен | Доступ по колонкам ограничен |
|----------------------------------|---------------------------|----------------------------------|--------------------------------|---------------------------------|
| "Правило поиска дублей" в группе | DuplicatesRuleInFolder | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| "Правило поиска дублей" в тегах | DuplicatesRuleInTag | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| BulkEmail in campaign view | VwBulkEmailInCampaign | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| BulkEmailInProgress | BulkEmailInProgress | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| BulkEmailRecipientMacro | BulkEmailRecipientMacro | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| BulkEmailRecipientReplica | BulkEmailRecipientReplica | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| Business processes in sections | ProcessInModules | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| ContactFolder in campaign view | VwFolderInCampaign | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

3. Включите ограничение доступа по операциям с помощью переключателя “Использовать доступ по операциям” (Рис. 2).

Рис. 2 — Включение администрирования по операциям



4. По кнопке [*Добавить*] добавьте роли и пользователей, для которых необходимо настроить права доступа. Используйте строку поиска, а также вкладки [*Организационные роли*], [*Функциональные роли*] и [*Пользователи*], чтобы быстро найти нужную роль или пользователя в списке окна выбора. В нашем примере это:
 - a. роль “All employees” (Все сотрудники) — добавляется автоматически;
 - b. организационная роль “Менеджеры по продажам”;
 - c. организационная роль “Менеджеры по продажам. Группа руководителей”;
 - d. организационная роль “Секретари”;
 - e. определенный пользователь с ролью “Секретари” (Рис. 3), например, Ульяновенко Александра.

Рис. 3 — Добавление ролей и пользователей для предоставления им доступа к разделу

Права доступа на объект Продажа

ПРИМЕНИТЬ

ОТМЕНА

ДЕЙСТВИЯ ▾

Заголовок
Продажа

Название
Opportunity

Важно знать

Наличие у пользователя либо роли доступа на операции "Добавление любых данных", "Чтение любых данных", "Изменение любых данных", "Удаление любых данных" имеет более высокий приоритет, чем настройки, заданные в текущем разделе.

ПРАВА ДОСТУПА

Использовать доступ по операциям ⓘ

Использовать доступ по записям ⓘ


Использовать доступ по колонкам ⓘ

5. По умолчанию для каждой добавленной роли или пользователя устанавливается доступ на просмотр, создание, редактирование и удаление данных объекта. Откорректируйте уровень доступа в соответствии с необходимостью:
 - a. Для роли **“Все сотрудники”** оставьте признак только в колонке [Чтение], а признаки в колонках [Создание], [Редактирование] и [Удаление] снимите. В итоге все сотрудники компании смогут просматривать записи раздела [Продажи], но не смогут их добавлять, вносить изменения и удалять.
 - b. Для роли **“Менеджеры по продажам”** оставьте признаки в колонках [Создание], [Чтение] и [Редактирование], а признак в колонке [Удаление] снимите. В итоге сотрудники отдела продаж смогут просматривать, добавлять и редактировать записи раздела, но не будут иметь возможности их удалять.
 - c. Оставьте признаки в колонках [Создание], [Чтение], [Редактирование] и [Удаление] для роли **“Менеджеры по продажам. Группа руководителей”**. Так руководитель менеджеров по продажам получит право на просмотр, добавление, изменение и удаление записей раздела [Продажи].
 - d. Для роли **“Секретари”** снимите признаки в колонках [Создание], [Чтение], [Редактирование] и [Удаление]. В итоге для секретарей компании раздел [Продажи] будет скрыт.
 - e. Для **определенного пользователя**, который входит в роль “Секретари” (в нашем примере это Ульяновко Александра) оставьте признак в колонке [Чтение]. Так пользователь Ульяновко Александра получит право на просмотр записей раздела [Продажи].

После выполнения настроек рядом с некоторыми правами доступа могут отображаться значки ⓘ . Это означает, что некоторые настройки противоречат друг другу и для корректной работы прав доступа необходимо настроить их приоритет.

Настроить приоритет прав доступа по операциям

объекта

Возможны случаи, когда настроенные для некоторых ролей уровни доступа противоречат друг другу, т. к. роли пересекаются. Например, роли “Менеджеры по продажам”, “Менеджеры по продажам. Группа руководителей” и “Секретари” входят в роль “Все сотрудники”. А для одного из секретарей настроены права доступа, которые отличаются от прав, настроенных для всех секретарей. О необходимости настроить приоритеты свидетельствует значок  рядом с противоречащим правом доступа.


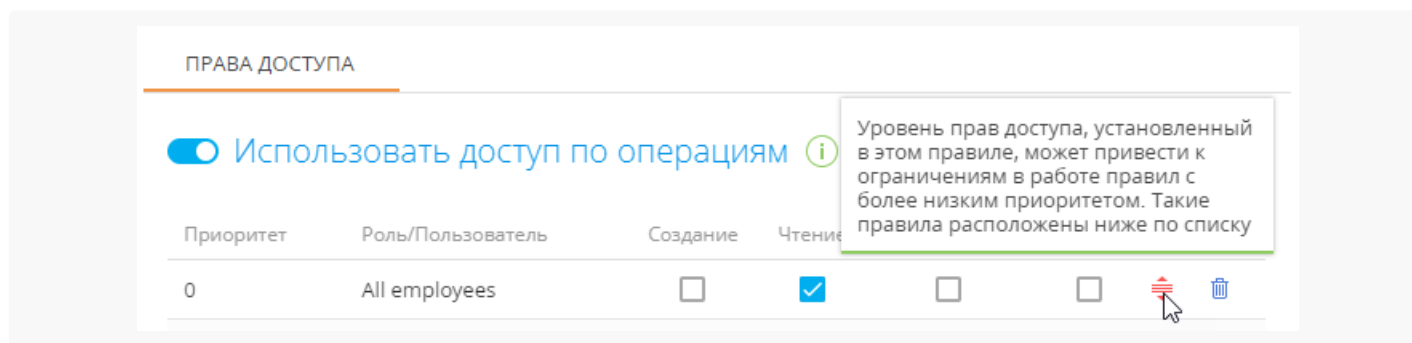
Чем выше в списке правило, тем выше его приоритет. Наиболее приоритетному правилу соответствует значение “0” в колонке [*Приоритет*]. Чем ниже в списке расположено правило и чем больше число в колонке [*Приоритет*], тем ниже приоритет этого правила. Значок , который может отображаться рядом с некоторыми из правил, обозначает, что некоторые из настроенных правил пересекаются. Необходимо понизить или повысить приоритет одного правила, чтобы корректно работало другое (Рис. 4).

Рис. 4 — Предупреждение о необходимости откорректировать приоритет прав доступа



При настройке приоритетов прав доступа **руководствуйтесь следующими правилами:**

- Например, мы хотим запретить всем пользователям доступ к записям раздела [*Продажи*], но менеджерам по продажам (они также входят в роль “Все пользователи”) необходимо дать все права, кроме удаления записей. Для этого расположим роль “Менеджеры по продажам” выше, а роль “Все пользователи” — ниже.
- Если пользователь входит в несколько ролей, для которых настраиваются права доступа, то для него будет применен уровень доступа той роли, которая расположена **выше** в списке. Если определенной роли, за исключением одного или нескольких пользователей, необходимо запретить доступ к какой-либо операции, то расположите такую роль **ниже**, а пользователей, которым надо предоставить доступ — выше. Так, если мы запрещаем доступ к разделу [*Продажи*] для всех секретарей, но предоставляем право просмотра данных одному из них, то роль “Секретари” должна быть расположена ниже того сотрудника, который должен иметь доступ к разделу.
- Пользователи или роли, которые **не добавлены** в область настройки доступа по операциям, не получают доступа к операциям и не участвуют при определении приоритетов прав.

Настроим приоритет прав доступа для приведенного выше примера. Для изменения порядка отображения правил захватите правило курсором мыши и перетащите на нужное место (Рис. 5):

1. Организационную роль с максимальным уровнем доступа (в нашем примере это “Менеджеры по продажам. Группа руководителей”) расположите сверху списка.
2. Далее расположите роль “Менеджеры по продажам”.
3. Роль “All employees” и пользователь Ульяненко Александра, который входит в роль “Секретари”,

имеют одинаковый уровень доступа. Поэтому расположите их под ролью “Менеджеры по продажам” в любом порядке.

4. У роли “Секретари” не должно быть доступа к разделу [*Продажи*], поэтому расположите ее внизу списка.
5. Сохраните настройки по кнопке [*Применить*] в верхнем левом углу страницы.

Рис. 5 — Настройка приоритета прав доступа

Права доступа на объект Продажа

ПРИМЕНИТЬ ОТМЕНА ДЕЙСТВИЯ ▾

Заголовок
Продажа

Название
Opportunity

Важно знать

Наличие у пользователя либо роли доступа на операции "Добавление любых данных", "Чтение любых данных", "Изменение любых данных", "Удаление любых данных" имеет более высокий приоритет, чем настройки, заданные в текущем разделе.

ПРАВА ДОСТУПА

☒ Использовать доступ по операциям ⓘ

| Приоритет | Роль/Пользователь | Создание | Чтение | Редактирование | Удаление |
|-----------|--|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| 0 | Менеджеры по продажам. Группа руководителей | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 1 | Менеджеры по продажам | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 2 | All employees | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3 | Ульяненко Александра | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 4 | Секретари | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

+ Добавить

В результате выполненных настроек:

- У пользователей с ролью “**Менеджеры по продажам**” будет доступ к разделу [*Продажи*] с возможностью создавать и редактировать записи раздела. Удалять записи менеджеры по продажам не смогут.
- У **руководителей менеджеров по продажам** будет полный доступ к разделу с возможностью удаления записей.
- **Все сотрудники компании** смогут просматривать записи раздела, но не смогут их создавать, редактировать и удалять.
- Для всех **секретарей** компании, кроме Ульяненко Александры, раздел [*Продажи*] будет скрыт.
- Секретарь **Ульяненко Александра** сможет перейти в раздел и просмотреть записи.

Настроить доступ по операциям в объекте детали

Пример. Выполним настройку доступа к детали [*Файлы и ссылки*] раздела [*Договоры*]. Пользователи с ролью “Менеджеры по продажам” должны иметь полный доступ к записям на детали.

Остальным пользователям необходимо разрешить только просмотр содержащихся на детали файлов и ссылок и запретить их редактирование и удаление.


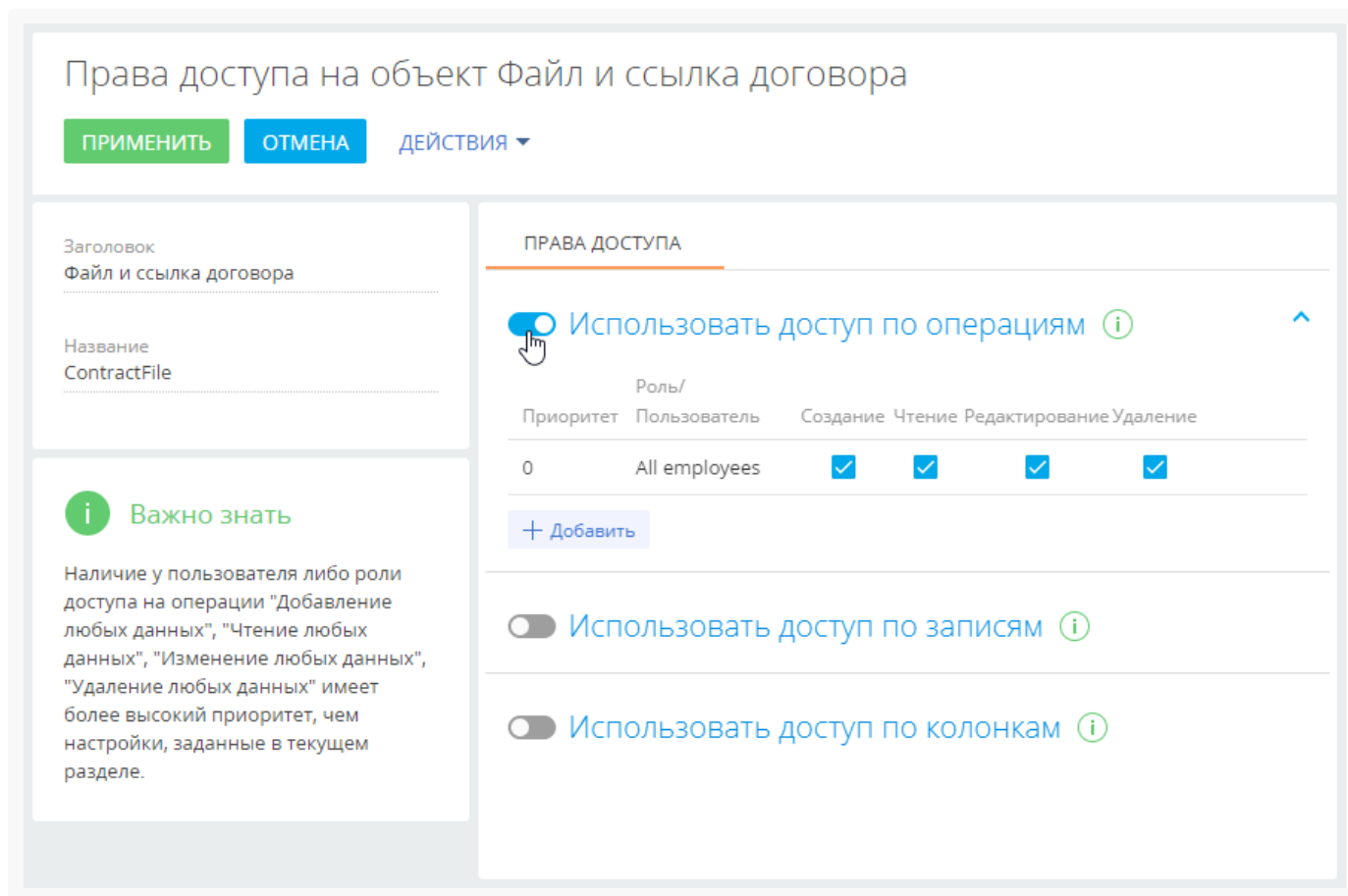

1. Перейдите в дизайнер системы, например, по кнопке , и откройте раздел настройки доступа к объектам по ссылке **“Права доступа на объекты”**.
2. Установите фильтр “Все объекты”.
3. Найдите объект “Файл и ссылка договора” с помощью строки поиска.
4. Кликните по заголовку или названию найденного объекта.
5. Включите ограничение доступа по операциям с помощью переключателя “Использовать доступ по операциям” (Рис. 6).

Рис. 6 — Включение администрирования по операциям



6. По кнопке [*Добавить*] добавьте роли и пользователей, для которых необходимо настроить права доступа. Используйте строку поиска, чтобы быстро найти нужную роль или пользователя в списке. В нашем примере это:
 - a. роль “All employees” (Все сотрудники) — добавляется автоматически;
 - b. роль “Менеджеры по продажам”.
7. По умолчанию для каждой добавленной роли или пользователя устанавливаются права на просмотр, создание, редактирование и удаление данных объекта. Откорректируйте уровень прав доступа в соответствии с необходимостью.

- a. Для роли **“Менеджеры по продажам”** оставьте признаки в колонках [*Создание*], [*Чтение*], [*Редактирование*] и [*Удаление*]. Так сотрудники отдела продаж смогут просматривать, добавлять, изменять и удалять данные на детали [*Файлы и ссылки*].
 - b. Для роли **“Все сотрудники”** оставьте признак только в колонке [*Чтение*], а признаки в колонках [*Создание*], [*Редактирование*] и [*Удаление*] снимите. Так все сотрудники смогут только просматривать содержимое детали [*Файлы и ссылки*] договора, но не смогут его добавлять, редактировать и удалять.
8. При необходимости настройте приоритеты прав доступа для указанных ролей. Настройка может потребоваться, если уровни доступа противоречат друг другу, т. к. роли пересекаются. Например, роль “Менеджеры по продажам” входит в роль “Все сотрудники”. О необходимости настроить приоритеты свидетельствует значок  рядом с противоречащим правом доступа.

В результате выполненных настроек:

- У пользователей с ролью **“Менеджеры по продажам”** будет полный доступ к детали [*Файлы и ссылки*] договора с возможностью просматривать, создавать, редактировать и удалять содержимое детали.
- **Все сотрудники компании** смогут просматривать содержимое детали [*Файлы и ссылки*] договора, но не смогут их создавать, редактировать и удалять.