

Управление доступом

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
Наследование прав доступа	12
Настроить права доступа на колонки	12
Настроить доступ на колонки объекта	13
Настроить приоритет прав доступа на колонки объекта	16
Настроить доступ по записям	18
Настроить доступ на экспорт данных	22
Настроить права доступа на системные операции	24
Описание системных операций	26
Управление пользователями и ролями	26
Управление пользователями портала	26
Общий доступ к данным	27
Доступ к колонкам, системным операциям	27
Доступ к особым разделам системы	28
Доступ к функциональности поиска дублей	28
Доступ к настройкам интеграций	29
Общие действия в системе	29
Делегировать права доступа	30
Делегировать права пользователя другим пользователям и ролям	30
Делегировать права пользователю от других пользователей и ролей	31
Удалить делегированные права доступа	32

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, содержащихся в двух разных объектах системы — в разделе и на детали.
- **По записям.** Подробнее: [Настроить доступ по записям](#).
- **По колонкам.** Подробне: [Настроить доступ по колонкам](#).

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 читайте в статье [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**”. ([Рис. 1](#)).

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

Права доступа на объекты				
<div> <div>ЗАКРЫТЬ</div> <div>ДЕЙСТВИЯ ▾</div> </div>		<div> <div>Разделы ▾</div> <div>Поиск</div> </div>		
Заголовок	Название	Доступ по операциям ограничен	Доступ по записям ограничен	Доступ по колонкам ограничен
Email	BulkEmail	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Активность	Activity	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Договор	Contract	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Документ	Document	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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. 2](#)).

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

курс).

Рис. 2 — Выбор объекта раздела и переход на страницу настройки прав доступа

Права доступа на объекты

ЗАКРЫТЬ

ДЕЙСТВИЯ

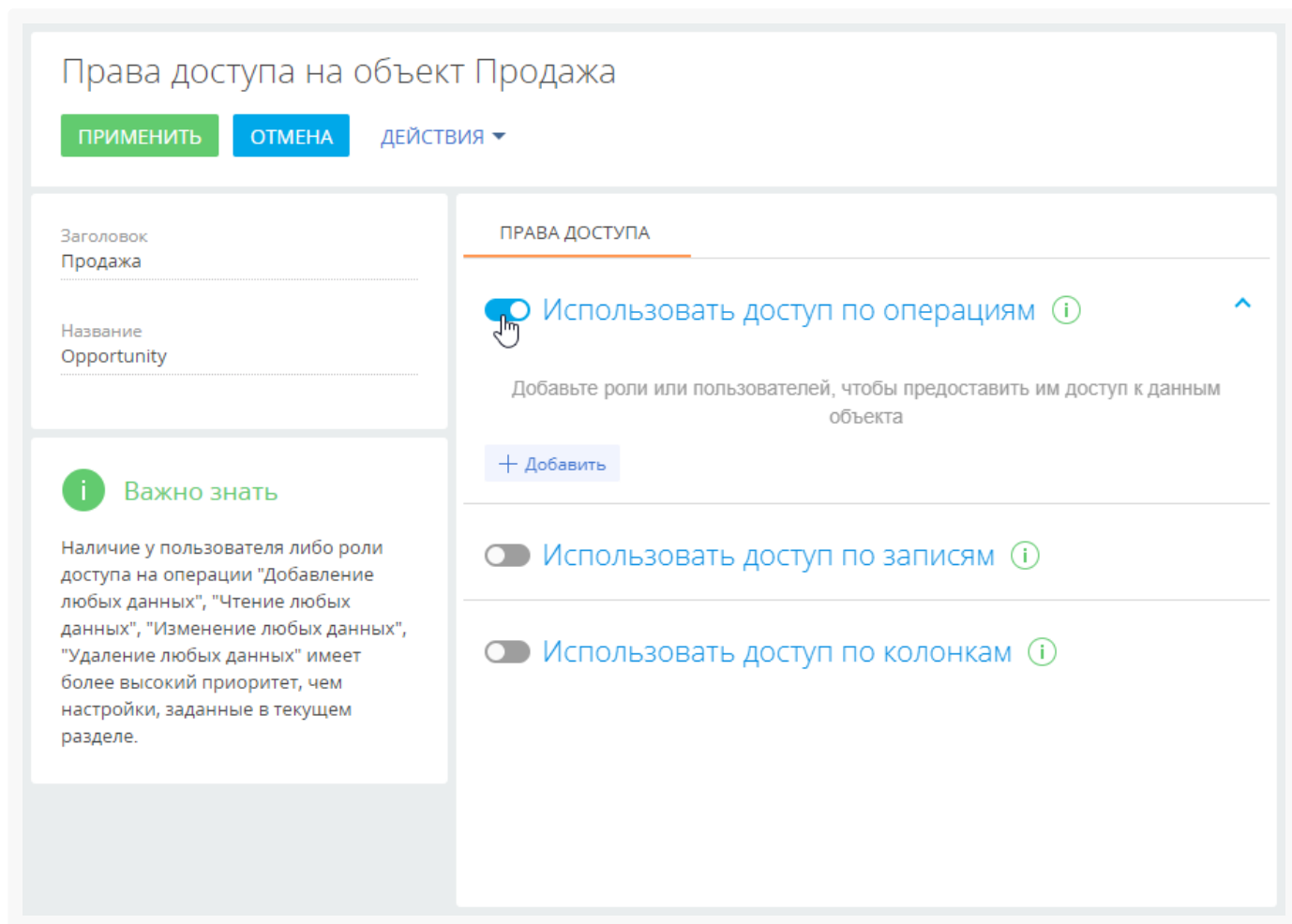
☰ Все объекты

🔍 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. 3).

Рис. 3 — 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. 4](#)), например, Ульяненко Александра.

Рис. 4 — 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

© 2022 Terrasoft. Все права защищены.

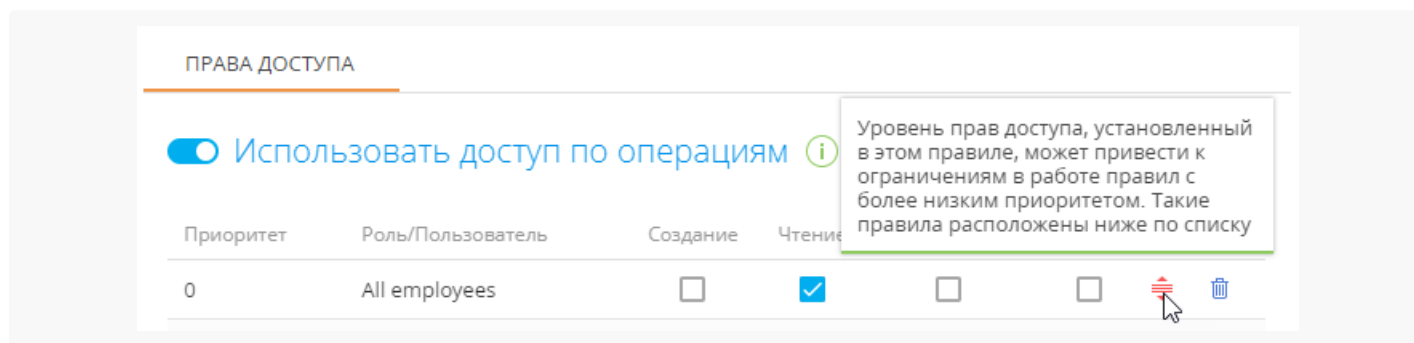
объекта

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. 5).

Рис. 5 — 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. 6):

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. 6 — 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.


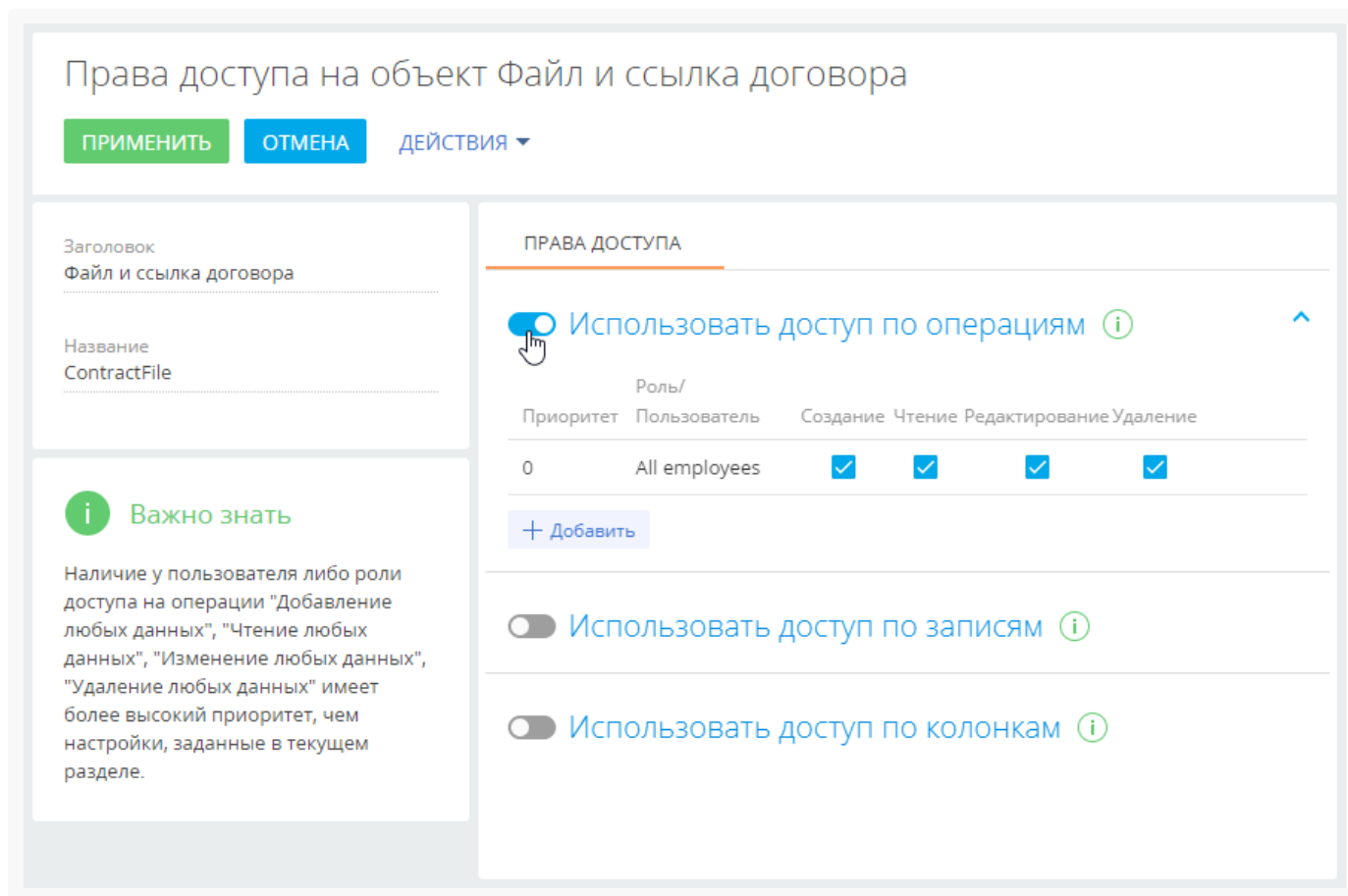

1. Перейдите в дизайнер системы, например, по кнопке , и откройте раздел настройки доступа к объектам по ссылке **“Права доступа на объекты”**.
2. Установите фильтр “Все объекты”.
3. Найдите объект “Файл и ссылка договора” с помощью строки поиска.
4. Кликните по заголовку или названию найденного объекта.
5. Включите ограничение доступа по операциям с помощью переключателя “Использовать доступ по операциям” ([Рис. 7](#)).

Рис. 7 — 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.

- а. 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*].
 - б. 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. Подробнее о настройке приоритетов читайте в блоке [Настроить приоритет прав доступа по операциям объекта](#).

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.

Наследование прав доступа

В системе реализовано наследование прав доступа от родительского объекта. Например, средства связи могут наследовать права доступа родительского контрагента. В таком случае пользователи, у которых нет прав на изменение основной записи контрагента, не смогут изменить и средства связи.

Для новых разделов эта функциональность по умолчанию выключена. Ее можно настроить отдельно в дизайнерах объектов раздела [*Конфигурация*].

Настроить права доступа на колонки

ПРОДУКТЫ: **ВСЕ ПРОДУКТЫ**

Права доступа на объекты можно ограничить на следующих уровнях:

- **По операциям.** Подробнее: [Настроить доступ по операциям](#).
- **По записям.** Подробнее: [Настроить доступ по записям](#).
- **По колонкам.** Настройка прав доступа на уровне чтения, редактирования и удаления **отдельных колонок** выбранного объекта будет рассмотрена в данной статье.

Колонки объектов отображаются в виде полей на страницах и в реестрах разделов и деталей.

Использование доступа по колонкам позволяет ограничить права на чтение и редактирование значений в отдельных полях объекта для отдельных пользователей или ролей. Например, вы можете ограничить право на просмотр данных в поле [*Годовой оборот*] для роли “Секретари”, а остальным сотрудникам компании оставить доступ к полю. При этом для пользователей, у которых нет права на чтение данных в поле [*Годовой оборот*], поле останется видимым, но его значение отображаться не будет (Рис. 1).

Рис. 1 — Пример отображения поля [Годовой оборот], когда настроен запрет на доступ к нему

При использовании доступа по колонкам для определенных ролей и пользователей более приоритетными являются настроенные для них [права доступа по операциям](#). Например, если у пользователя нет права на операцию чтения данных объекта, то для такого пользователя объект будет скрыт полностью.

Доступ к колонкам, не добавленным на деталь, и к колонкам на детали, для которых не указаны права доступа, определяется настройками прав доступа по операциям.

Если в объект, для которого уже используется администрирование по колонкам, добавляется новая колонка, то права доступа к ней нужно настраивать отдельно, независимо от того, имеет ли пользователь доступ на операции в данном объекте. Пользователи не будут иметь доступа к новой колонке, добавленной в объект после включения администрирования по колонкам, если настройки не выполнены.

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

Важно. Перед настройкой прав доступа на колонки объекта убедитесь, что у пользователя есть доступ на те операции в объекте, которые соответствуют необходимым правам доступа по колонкам. Обратите внимание, если доступ к объекту не администрируется по операциям, то всем пользователям по умолчанию предоставляется право на операции создания, чтения, редактирования и удаления данных объекта. Подробнее: [Настроить доступ по операциям](#).

Настроить доступ на колонки объекта

Рассмотрим, как предоставить или ограничить права групп пользователей на просмотр и редактирование данных, содержащихся в определенном поле записи раздела.

Пример. Выполним настройку прав доступа к полю [Годовой оборот] на странице контрагента. Все сотрудники компании, кроме секретарей, должны иметь возможность просматривать значение

поля [*Годовой оборот*], а менеджеры по продажам — просматривать и редактировать значение поля.

Для секретарей значение этого поля должно быть скрыто.


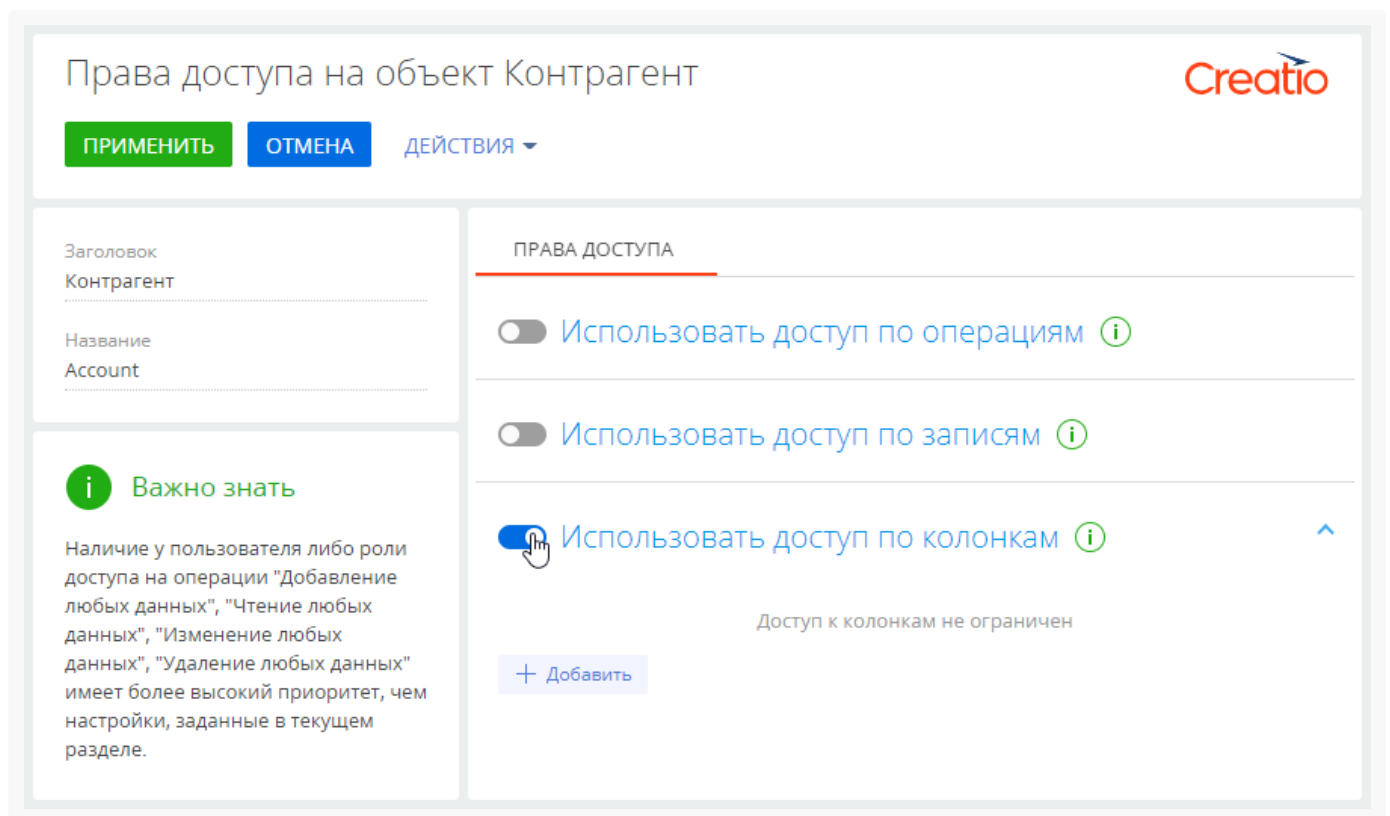
1. Перейдите в дизайнер системы, например, по кнопке , и откройте раздел настройки доступа к объектам по ссылке **“Права доступа на объекты”**.
2. Выберите необходимый объект из списка или с помощью строки поиска. Так, чтобы настроить права доступа к полю [*Годовой оборот*] контрагента, установите фильтр “Разделы” и выберите объект “Контрагент”. Кликните по его заголовку или названию — откроется страница настройки прав доступа к объекту раздела [*Контрагенты*].
3. Убедитесь, что у пользователей или ролей, для которых вы хотите настроить доступ по колонкам, уже есть доступ на операции в объекте — объект не администрируется по операциям, либо пользователи и роли имеют доступ на соответствующие операции на уровне объекта.
4. Включите ограничение доступа по колонкам с помощью переключателя “Использовать доступ по колонкам” (Рис. 2).

Рис. 2 — Включение администрирования по колонкам

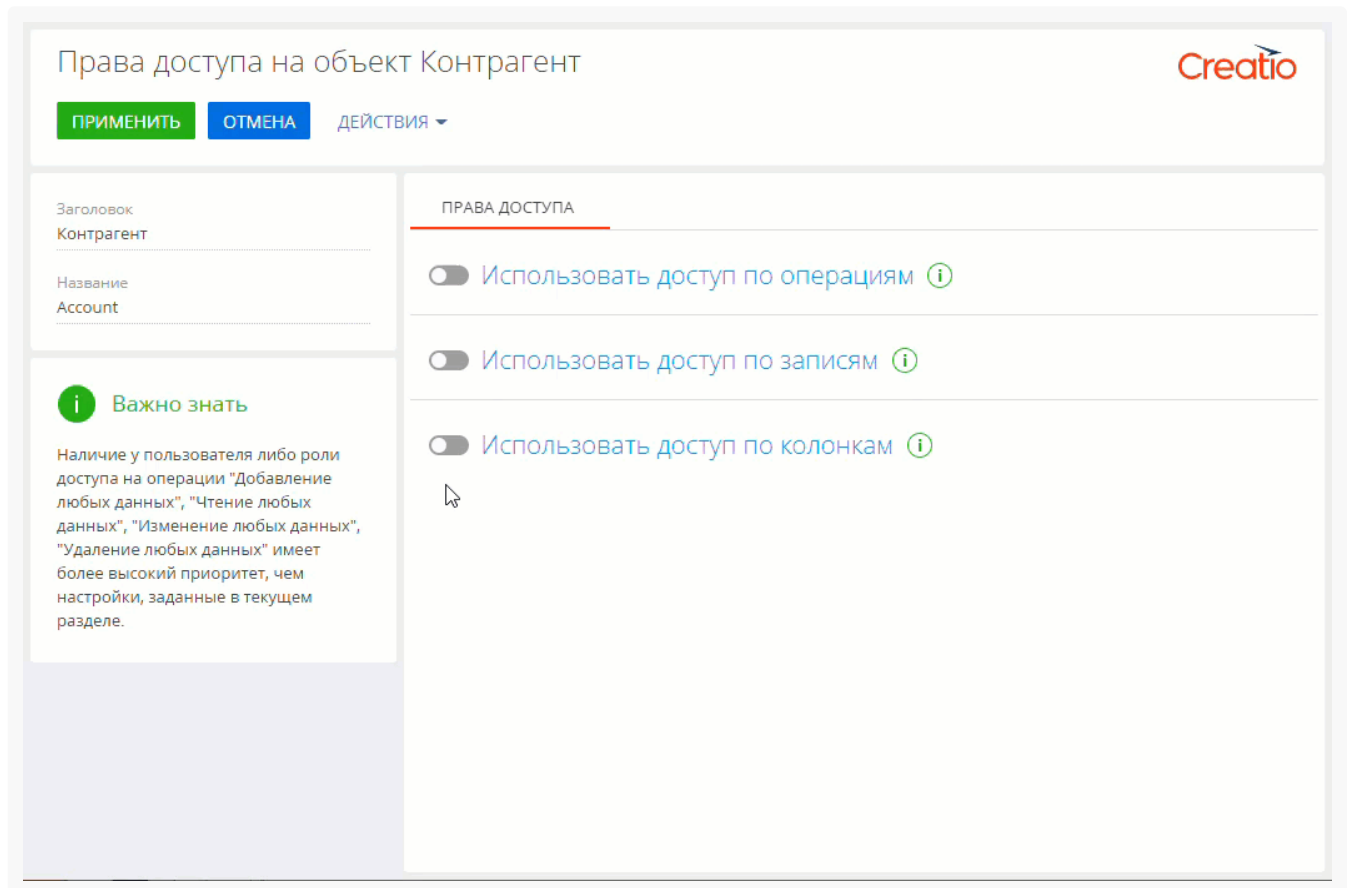


5. По кнопке [*Добавить*] выберите и добавьте колонку объекта, доступ к которой необходимо ограничить. Например, для ограничения доступа к полю [*Годовой оборот*] введите его название в строку поиска и нажмите [*Выбрать*]. Выбранная колонка отобразится в области настройки прав доступа слева. Справа можно добавить роли и пользователей и установить для них уровень прав доступа (Рис. 3). При необходимости добавьте и другие колонки, на которые нужно ограничить доступ. Переключайтесь между колонками в списке, чтобы настроить права доступа для каждой из них.

6. По кнопке [*Добавить*] в правой части области настройки добавьте все роли и пользователей, для которых нужно настроить доступ к выбранной колонке. Используйте строку поиска и вкладки [*Организационные роли*], [*Функциональные роли*] и [*Пользователи*], чтобы быстро найти нужную роль или пользователя (Рис. 3). В нашем примере это:


- роль “All employees” (Все сотрудники) — добавляется автоматически;
- организационная роль “Менеджеры по продажам”;
- организационная роль “Секретари”.

Рис. 3 — Добавление ролей и пользователей для настройки доступа к полю [*Годовой оборот*] контрагента



По умолчанию для каждой добавленной роли или пользователя устанавливается доступ на чтение и редактирование значения выбранного поля объекта. Откорректируйте уровень прав доступа в соответствии с необходимостью. Например:

- Для организационной роли “**All employees**” (Все сотрудники) измените уровень прав на “Чтение разрешено”. В итоге все сотрудники компании смогут видеть значение в поле [*Годовой оборот*] контрагента, но не смогут его отредактировать.
- Для роли “**Менеджеры по продажам**” оставьте уровень доступа “Чтение и редактирование разрешено”. Так сотрудники отдела продаж смогут видеть и редактировать значения в поле [*Годовой оборот*] контрагента.
- Для роли “**Секретари**” установите уровень прав “Чтение и редактирование запрещено”. В итоге для секретарей компании значение поля [*Годовой оборот*] будет скрыто.

После выполнения настроек рядом с некоторыми правами доступа могут отображаться значки  .

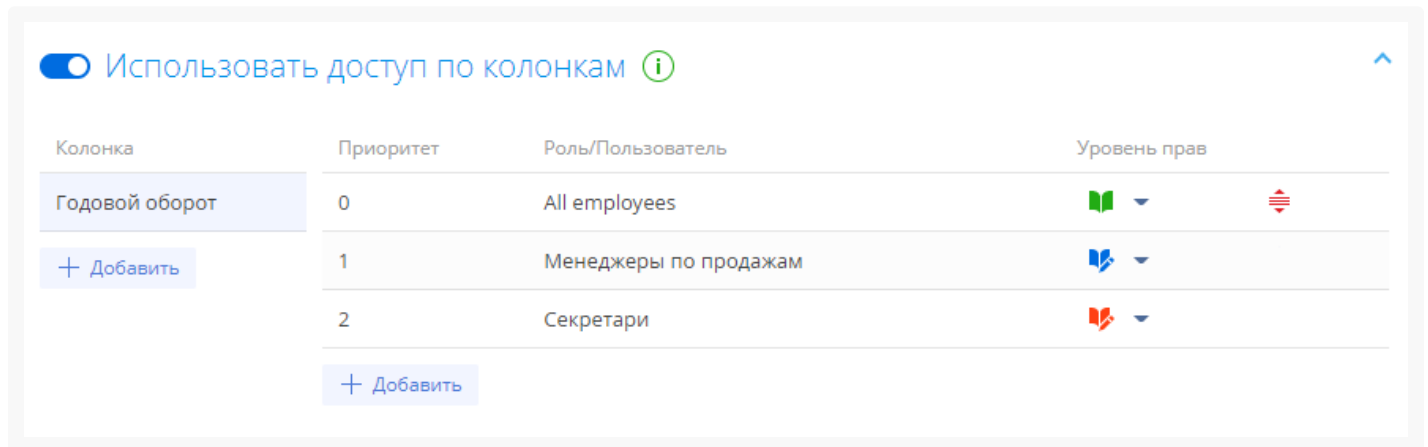
Это означает, что некоторые настройки противоречат друг другу и возможно, потребуется настроить приоритет для корректной работы прав доступа.


Настроить приоритет прав доступа на колонки объекта

Возможны случаи, когда настроенные для некоторых ролей или пользователей уровни доступа противоречат друг другу, т. к. роли пересекаются.

Например, роли “Менеджеры по продажам”, и “Секретари” входят в роль “Все сотрудники”. При этом уровень прав доступа для менеджеров по продажам выше, чем уровень прав для всех сотрудников (Рис. 4).

Рис. 4 — Пример противоречия между уровнями прав 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 и возможно, необходимо понизить или повысить приоритет одного правила, чтобы корректно работало другое.

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

- Самыми приоритетными являются ограничения по операциям, используемые для данного объекта.
- 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.

Например, мы хотим запретить всем сотрудникам редактировать поле, но менеджерам по продажам оставить возможность чтения и редактирования. Для этого расположим роль “Менеджеры по продажам” выше, а роль “All employees” (Все сотрудники) — ниже.

- Если роль, для которой необходимо полностью запретить доступ к колонке, входит в роль с более высоким уровнем доступа, то выше расположите роль, для которой ограничиваете доступ, а родительскую роль — ниже.

Так, если мы запрещаем чтение и редактирование поля для всех секретарей, то роль “Секретари” должна быть расположена выше роли “All employees” (Все сотрудники), у которых есть только право на чтение колонки. При этом рядом с уровнем прав, установленным для секретарей, отображается значок .

На заметку. В данном случае настройка приоритета не требуется, т. к. противоречие между правами доступа для роли “Секретари” и роли “All employees” (Все сотрудники), в которую входит роль “Секретари”, состоит в том, что секретари не смогут просматривать значение колонки, что и было необходимо настроить.

- Права доступа для пользователей или ролей, которые не добавлены в область настройки доступа по колонкам, соответствуют правам доступа по операциям, которые для них настроены.

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

- Организационную роль с максимальным уровнем доступа (в нашем примере это “Менеджеры по продажам”) расположите вверху списка.
- Далее расположите роль “Секретари”, для которой значение поля [*Годовой доход*] должно быть скрыто.
- Роль “All employees” (Все сотрудники) расположите внизу списка.
- Сохраните настройки по кнопке [*Применить*] в верхнем левом углу страницы.

Рис. 5 — Пример настройки приоритета прав доступа по колонкам

Права доступа на объект Контрагент

ПРИМЕНИТЬ

ОТМЕНА

ДЕЙСТВИЯ ▾

Заголовок

Контрагент

Название

Account

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	All employees	✓	✓	✓	✓

+ Добавить

Использовать доступ по записям ⓘ

Использовать доступ по колонкам ⓘ

Колонка	Приоритет	Роль/Пользователь	Уровень прав
Годовой оборот	0	Менеджеры по продажам	🔵 ▾
	1	Секретари	🔴 ▾ 🔒
	2	All employees	🟢 ▾

+ Добавить

В результате выполненных настроек:

- У пользователей с ролью “**Менеджеры по продажам**” будет возможность просматривать и редактировать значение в поле [*Годовой оборот*] контрагента.
- Для всех **секретарей** значение в поле [*Годовой оборот*] контрагента будет скрыто.
- **Все сотрудники компании** смогут видеть значение в поле [*Годовой оборот*], но не смогут его редактировать.

Подробнее: [Пользователи и права доступа](#).

Настроить доступ по записям

ПРОДУКТЫ: **ВСЕ ПРОДУКТЫ**

Права доступа на объекты можно ограничить на следующих уровнях:

- **По операциям.** Подробнее: [Настроить доступ по операциям](#).
- **По колонкам.** Подробнее: [Настроить права доступа на колонки](#).
- **По записям.** Настройка прав доступа на уровне чтения, редактирования и удаления **отдельных записей** выбранного объекта будет рассмотрена в данной статье.

Администратор системы может управлять правами на чтение, обновление или удаление **отдельных записей**, а также возможностями делегирования этих прав.

Распределение прав доступа по записям включается переключателем “Использовать доступ по записи” в разделе [*Права доступа на объекты*] дизайнера системы и зависит от авторства записи. Если автор записи входит в роль, которая указана в столбце “Автор записи”, то система раздает права роли-получателю, указанной в столбце “Получатель прав”. Если роль-получатель является подчиненной, то роль ее руководителей наследует все полученные права доступа.

По умолчанию максимальные права на управление записью имеют:

- **Системные администраторы**, которым дан доступ на системные операции “Добавление любых данных”, “Чтение любых данных”, “Изменение любых данных”, “Удаление любых данных”. Эти настройки имеют более высокий приоритет, чем настройки, заданные в разделе [*Права доступа на объекты*].
- **Автор записи и роль руководителей автора** с возможностью делегирования прав другим пользователям.
- **Ответственный за запись и роль руководителей ответственного** с возможностью делегирования прав другим пользователям.

Подробнее: [Настроить права доступа на запись](#).

На заметку. Если для объекта отключено администрирование прав доступа по записям, то записи будут доступны всем пользователям, у которых есть [доступ по операциям](#) в объекте.

Если администрирование по записям включено, но права доступа не настроены, то записи будут доступны только их автору, роли руководителей автора, ответственному по записи, роли руководителей ответственного, а также системным администраторам.

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](#).


Пример. Выполним настройку прав доступа для записей раздела [*Продажи*].

Если записи созданы менеджерами по продажам, то все сотрудники, входящие в эту роль, должны иметь возможность их просматривать (с делегированием), а также редактировать, но не иметь возможности удалять.

Если записи созданы руководителями менеджеров по продажам, то менеджеры должны иметь доступ на их чтение и редактирование, но без делегирования, а руководители должны иметь полный доступ с правом делегирования.

В нашем примере авторами записей и получателями прав будут сотрудники, входящие в роли “Менеджеры по продажам” и “Менеджеры по продажам. Группа руководителей”.

На заметку. Если для обеспечения отказоустойчивости в вашем приложении используется балансировщик нагрузки, то настройку необходимо выполнить на одном экземпляре приложения, после чего перенести на другие. Аналогичным образом выполняется установка приложений Marketplace, пакетов с пользовательской кастомизацией и другие настройки, требующие компиляции. Подробнее: [Установить приложение Marketplace на среду с балансировщиком](#).

1. Перейдите в дизайнер системы, например, по кнопке , и откройте раздел настройки доступа к объектам по ссылке “**Права доступа на объекты**”.
2. 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).

Подробнее: [Права доступа на объекты](#).

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

Права доступа на объекты Creatio

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"/>
(Устаревший)Раздел SSP	Portal_SysModule	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Bulk email throttling queue	EmailThrottlingQueue	<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"/>
BulkEmailQueue	BulkEmailQueue	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
BulkEmailQueueOp	BulkEmailQueueOp	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
BulkEmailRecipientMacro	BulkEmailRecipientMacro	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CampaignParticipantInfo	CampaignParticipantInfo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
CampaignParticipantOpInfo (операционная таблица)	CampaignParticipantOpInfo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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

Рис. 2 — Включение администрирования по записям

Права доступа на объект Продажа Creatio

ЗАКРЫТЬ **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** ⓘ

Раздача прав в зависимости от автора записи ⓘ

Отсутствуют правила раздачи прав в зависимости от автора

[+ Добавить](#)

☐ Использовать доступ по колонкам ⓘ

4. По кнопке [*Добавить*] откроется окно, в котором необходимо указать пользователя или роль, на чьи записи будут раздаваться права доступа, а также пользователя или роль, которая получит эти права. Используйте строку поиска, чтобы быстро найти нужную роль или пользователя в списке. В нашем примере нужно добавить три записи (Рис. 3).

Рис. 3 — Пример добавления ролей для настройки 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 ⓘ

Использовать доступ по записям ⓘ

Раздача прав в зависимости от автора записи ⓘ

Автор записи	Получатель прав	Чтение	Редактирование	Удаление
Менеджеры по продажам	Менеджеры по продажам	☑ ▾	☑ ▾	☐ ▾
Менеджеры по продажам. Группа руководителей	Менеджеры по продажам	☑ ▾	☑ ▾	☐ ▾

+ Добавить

Использовать доступ по колонкам ⓘ

5. По умолчанию права доступа для получателей не установлены. Чтобы определить уровни доступа, для каждого из получателей в колонке, соответствующей праву (чтение, редактирование или удаление) нажмите кнопку ☐ ▾ и выберите “Разрешено” ☒ или “Разрешено с делегированием” ☒. В нашем примере устанавливаются следующие права (Рис. 4):

Рис. 4 — Пример настройки прав доступа по записям

Использовать доступ по записям ⓘ


Раздача прав в зависимости от автора записи ⓘ

Автор записи	Получатель прав	Чтение	Редактирование	Удаление
Менеджеры по продажам	Менеджеры по продажам	☑ ▾	☑ ▾	☐ ▾
Менеджеры по продажам. Группа руководителей	Менеджеры по продажам	☑ ▾	☑ ▾	☐ ▾
Менеджеры по продажам. Группа руководителей	Менеджеры по продажам. Группа руководителей	☑ ▾	☑ ▾	☑ ▾

+ Добавить

- Чтобы сотрудники отдела продаж могли просматривать записи, созданные их коллегами, делегировать это право другим пользователям, вносить в записи изменения, но не могли их удалять, для роли “**Менеджеры по продажам**” установите признак “Разрешено с делегированием” ☒ в колонке [Чтение] и признак “Разрешено” ☒ в колонке [Редактирование].
- Чтобы сотрудники отдела продаж могли просматривать записи, созданные их руководителями, вносить в записи изменения, но не могли их удалять, для роли “**Менеджеры по продажам**”

установите признак “Разрешено”  в колонках [Чтение] и [Редактирование].

- с. Чтобы руководители менеджеров по продажам имели право на просмотр, изменение и удаление записей раздела [Продажи], созданных их коллегами, а также возможность делегировать эти права другим пользователям, установите признак “Разрешено с делегированием”  для роли **“Менеджеры по продажам. Группа руководителей”** в колонках [Чтение], [Редактирование] и [Удаление] для записей, авторы которых входят в роль “Менеджеры по продажам. Группа руководителей”.

На заметку. В отличие от прав доступа по операциям, для прав доступа по записям порядок добавления не влияет на приоритет.

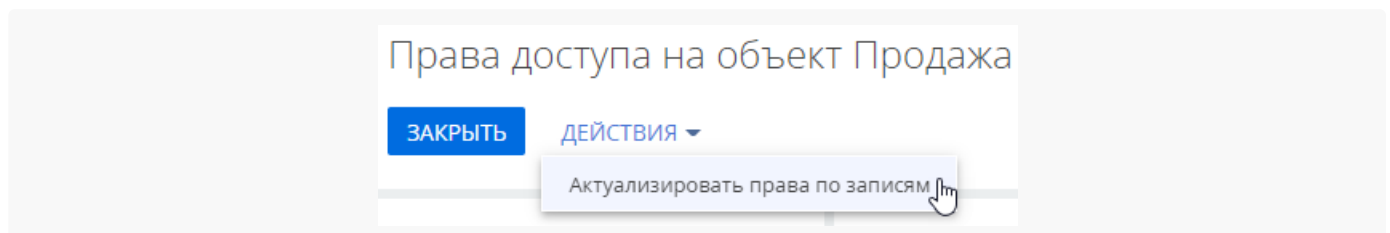
6. Чтобы сохранить настроенные права доступа, нажмите кнопку [Применить].

Важно. Если права доступа настроены в разделе, в котором уже есть записи, то необходимо выполнить актуализацию прав доступа. Иначе настроенные права доступа будут применяться только к новым записям раздела.

Актуализация прав доступа — это ресурсоемкая процедура. В зависимости от количества записей в разделе, а также ролей и пользователей, для которых она выполняется, актуализация может занять от 3 минут и более и повлиять на производительность системы. Чтобы этого избежать, рекомендуем выполнять актуализацию прав доступа во время наименьшей нагрузки на систему.

Чтобы применить новые права доступа к существующим записям раздела, откройте страницу настройки прав доступа к объекту и в меню [Действия] выберите пункт “Актуализировать права по записям” (Рис. 5).

Рис. 5 — Запуск актуализации прав по записям раздела



В результате актуализации прав записи будут удалены все права, установленные настройками по умолчанию, и созданы новые. Права, которые были [добавлены пользователем вручную](#) на странице настройки прав определенной записи или [настроены в рамках бизнес-процесса](#), при актуализации прав не удаляются.

На заметку. Для одной роли может существовать несколько записей прав. Например, это могут быть права, созданные в результате выполнения действия [Актуализировать права по записям] и полученные в ходе выполнения бизнес-процесса, или добавленные пользователем вручную и полученные в ходе выполнения бизнес-процесса.

Настроить доступ на экспорт данных

настроить доступ на экспорт данных

ПРОДУКТЫ: **ВСЕ ПРОДУКТЫ**

Вы можете предоставить доступ ролям и отдельным пользователям на экспорт реестра как для отдельных объектов, так и для всех разделов системы.

Права на экспорт реестра являются разновидностью прав [доступа на объекты](#) приложения. Вы можете предоставить некоторым ролям и пользователям, например, руководству компании, неограниченный доступ на экспорт данных. Для этого необходимо предоставить им права на выполнение системной операции [системной операции](#) “Экспорт реестра” (код “CanExportGrid”). Для конфиденциальной и чувствительной информации рекомендуем настраивать права на экспорт для отдельных объектов. Например, предоставить руководителям финансового департамента право экспортировать счета.

Пример. Необходимо настроить для роли “Руководители финансового отдела” доступ к экспорту только реестра счетов.



1. Перейдите в дизайнер системы, например, по кнопке .
2. В блоке “Пользователи и администрирование” перейдите по ссылке “Права доступа на объекты”.
3. В списке объектов системы найдите необходимый вам объект раздела, справочника или детали. Установите фильтр “Разделы” и выберите объект “Счет”.
4. Кликните по заголовку или названию — откроется страница настройки прав доступа к объекту раздела [*Счета*].
5. На открывшейся странице перейдите на вкладку [*Расширенные действия*].
6. Нажмите кнопку [*Добавить*] и в открывшемся окне укажите роль или пользователя, которым необходимо предоставить доступ к экспорту реестра.
 - a. В поле [*Роль/Пользователь*] нажмите , выберите нужную организационную, функциональную роль или пользователя, а затем подтвердите действие по кнопке [*Выбрать*].
 - b. В поле [*Выбрать операцию*] укажите “Export”.
 - c. Подтвердите действие по кнопке [*Добавить*].
7. При необходимости повторите шаг 6 для добавления прав на экспорт другим пользователям и ролям.
8. Для сохранения настроек нажмите кнопку [*Применить*] (Рис. 1).

Рис. 1 — Пример настройки прав на экспорт реестра

В результате сотрудники, входящие в роль “Руководители финансового отдела”, смогут выполнять экспорт только реестра раздела [Счета]. Экспорт остальных реестров системы для них будет недоступен.

Настроить права доступа на системные операции

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

В этой статье рассмотрена настройка прав **доступа к действиям системы**. Примеры таких действий: импорт и экспорт данных, создание бизнес-процессов, настройка рабочих мест, изменение содержимого справочников, конфигурирование системы и т. д.

Действия системы не относятся к конкретному объекту и права на них не могут настраиваться на уровне операций чтения, редактирования и удаления данных в объекте. Для настройки прав доступа к действиям системы используются **системные операции**. Они имеют два уровня доступа: у пользователя либо роли есть право на выполнение системной операции, или его нет. Например, если вы разрешите роли “Все сотрудники компании” выполнять операцию “Экспорт реестра” (код “Export list records”), то все без исключения пользователи смогут экспортировать данные реестра раздела в Excel.

Управление доступом к системным операциям доступно в дизайнера системы, по ссылке **“Права доступа на операции”**. Работа с группами в реестре системных операций не предусмотрена, но вы можете воспользоваться [стандартным](#) или [расширенным](#) фильтром.

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. Подробнее читайте в статье [Настроить доступ по операциям](#).

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

Обратите внимание, что право на выполнение системной операции не отменяет других прав доступа. Например, пользователи смогут экспортировать только те данные, к которым у них есть доступ.

По умолчанию доступ к основным системным операциям есть только у администраторов системы. Вы можете настроить права доступа к системным операциям для определенных пользователей или групп

пользователей.

Пример. Дать доступ на экспорт реестра для руководителей менеджеров по продажам.



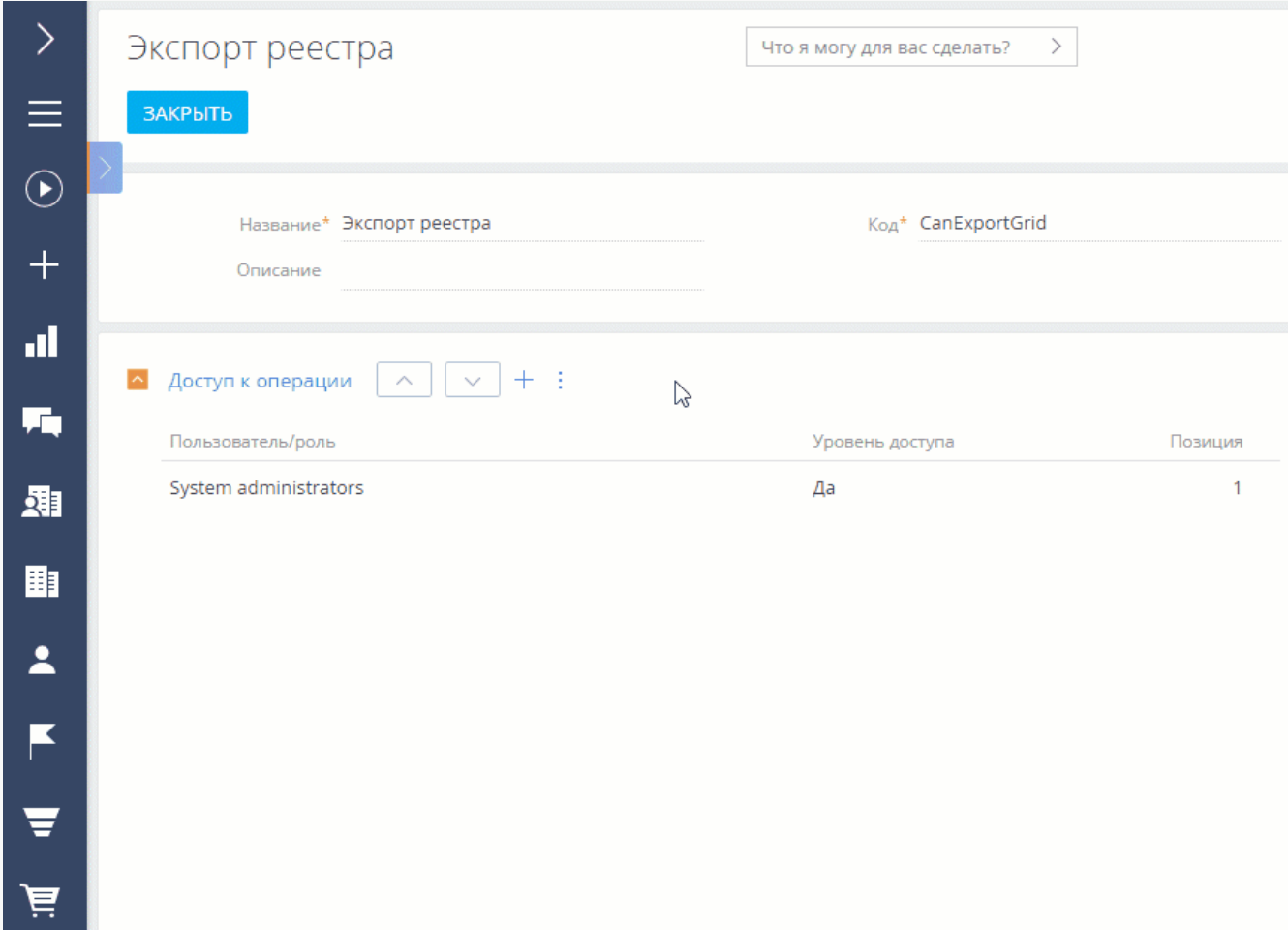
1. Нажмите  —> Дизайнер системы —> **“Права доступа на операции”**.
2. Установите фильтр “Название = Экспорт реестра” (или “Код = CanExportGrid”). **Кликните по заголовку** системной операции или выделите ее в реестре и нажмите кнопку [Открыть].
3. На детали [Доступ к операции] нажмите кнопку  —> **укажите получателя прав**. В нашем примере это роль “Менеджеры по продажам. Группа руководителей”. Запись появится на детали со значением “Да” в колонке “Уровень доступа”. В результате пользователи, входящие в роль “Менеджеры по продажам. Группа руководителей” получают доступ к системной операции [Экспорт реестра] ([Рис. 1](#)).

Рис. 1 — Добавление прав доступа на системную операцию



Экспорт реестра

Что я могу для вас сделать? >

ЗАКРЫТЬ



Название* Экспорт реестра Код* CanExportGrid

Описание

Доступ к операции

Пользователь/роль	Уровень доступа	Позиция
System administrators	Да	1

На заметку. Чтобы запретить доступ, установите в колонке [Уровень доступа] значение “Нет”. Для этого выберите пользователя или роль в списке. Значение в колонке “Уровень доступа” отобразится в виде признака. Снимите признак, чтобы запретить доступ для выбранного пользователя или роли. Сохраните запись.

Когда вы настраиваете ограничения на доступ к системной операции для определенных пользователей или ролей, возможны случаи, что уровни доступа противоречат друг другу, т. к. роли пересекаются. Настройте приоритетность прав доступа на операцию, чтобы для всех ролей они обрабатывали корректно. Для этого воспользуйтесь кнопками  и  на детали [*Доступ к операции*]. Если пользователь будет входить в несколько ролей, добавленных на деталь, то для него будут применен уровень доступа той роли, которая расположена выше в списке. Например, если вы хотели бы запретить всем пользователям, кроме руководителей менеджеров по продажам, экспорт реестра, расположите роль “Все сотрудники компании” ниже, а роль “Менеджеры по продажам. Группа руководителей” — выше.

На заметку. Пользователи или роли, которые не добавлены на деталь, не получают права доступа к операции. При этом они не участвуют в определении приоритетов прав.

Описание системных операций

ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Ниже представлено описание системных операций, доступом к которым вы можете управлять.

Управление пользователями и ролями

Системная операция	Описание
Управление списком пользователей Код “CanManageUsers”	Право добавлять, изменять и удалять учетные записи пользователей в разделах управления ролями и пользователями дизайнера системы.
Управление лицензиями пользователей Код “CanManageLicUsers”	Право доступа к разделу [Менеджер лицензий]. Пользователи, обладающие этим правом, могут войти в систему и перераспределить лицензии даже в случае блокировки системы в связи с превышением количества лицензий.
Изменение делегируемых прав Код “CanChangeAdminUnitGrantedRight”	Возможность делегировать права доступа одних пользователей другим при помощи детали [Делегирование прав доступа] на странице пользователя.

Управление пользователями портала

Системная операция	Описание
Возможность управлять пользователями портала Код "CanAdministratePortalUsers"	Право добавлять, изменять и удалять учетные записи пользователей портала в разделах управления ролями и пользователями дизайнера системы.
Доступ к модулю настройки главной страницы портала Код "CanManagePortalMainPage"	Право настраивать главную страницу портала .

Общий доступ к данным

Операции общего доступа к данным относятся ко всем записям во всех объектах. Как правило, общий доступ к данным предоставляется **администратору системы**.

Важно. Действие прав доступа, предоставленных данными операциями, не может быть ограничено никакими специфическими правами доступа к записям, операциям либо колонкам объектов: если такие ограничения существуют, то они не будут приниматься во внимание. Например, если пользователь имеет доступ к операции [*Просмотр любых данных*], то он сможет просматривать данные всех объектов, даже если доступ к операциям чтения в таких объектах ограничен.

Системная операция	Описание
Просмотр любых данных Код "CanSelectEverything"	Право просматривать все записи во всех объектах.
Добавление любых данных Код "CanInsertEverything"	Право добавлять записи в любые объекты системы.
Изменение любых данных Код "CanUpdateEverything"	Право редактировать любые записи во всех объектах системы.
Удаление любых данных Код "CanDeleteEverything"	Возможность удалять любые записи из любых объектов системы.

Доступ к колонкам, системным операциям

Системная операция	Описание
Изменение прав на системные операции Код "CanChangeAdminOperationGrantee"	Право предоставления доступа к системным операциям . Данная операция также включает в себя право регистрации дополнительных системных операций.

Доступ к особым разделам системы

Системная операция	Описание
Доступ к рабочему месту "Администрирование" Код "CanManageAdministration"	Право доступа к разделам [Права доступа на объекты] и [Права доступа на операции]. Требуется для управления записями sysAdminUnit. Доступ к конкретным операциям администрирования должен быть предоставлен отдельно.
Доступ к разделу "Дизайн процессов" Код "CanManageProcessDesign"	Право доступа к дизайнеру процессов , а также возможность добавлять и редактировать бизнес-процессы.
Доступ к разделу "Журнал изменений" Код "CanManageChangeLog"	Право доступа к разделу [Журнал изменений].
Доступ к разделу "Системные настройки" Код "CanManageSysSettings"	Право доступа к разделу [Системные настройки].
Доступ к разделу "Справочники" Код "CanManageLookups"	Право доступа к разделу [Справочники].
Доступ к разделу "Конфигурация" Код "CanManageSolution"	Право доступа к разделу [Управление конфигурацией] дизайнера системы.
Просмотр раздела "Журнал аудита" Код "CanViewSysOperationAudit"	Право на просмотр содержимого раздела [Журнал аудита].
Управление разделом "Журнал аудита" Код "CanManageSysOperationAudit"	Право на просмотр содержимого раздела [Журнал аудита], а также на выполнение действия архивирования журнала.

Доступ к функциональности поиска дублей

Системная операция	Описание
Поиск дублей Код "CanSearchDuplicates"	Право выполнять поиск дублирующихся записей в разделах, для которых настроены правила поиска дублей .
Обработка дублей Код "CanMergeDuplicates"	Право на выполнение слияния дублей на странице результатов массового поиска дублей, а также во всех разделах и справочниках.
Доступ к правилам поиска дублей Код "CanManageDuplicatesRules"	Право создавать и редактировать правила поиска дублей.

Доступ к настройкам интеграций

Системная операция	Описание
Доступ к OData Код "CanUseODataService"	Право доступа к интеграции с внешними ресурсами по протоколу OData.

Общие действия в системе

Системная операция	Описание
Настройка списка почтовых провайдеров Код "CanManageMailServers"	Право формировать список email-серверов, используемых для отправки и получения писем.
Настройка синхронизации с общими почтовыми ящиками Код "CanManageSharedMailboxes"	Право управлять доступом к почтовым ящикам, для которых был установлен признак [Общий].
Изменение прав на запись Код "CanChangeEntitySchemaRecordRight"	Право устанавливать доступ по записям в объектах. Для того чтобы доступ по записям объекта работал, переключатель [<i>Использовать доступ по операциям</i>] в том же объекте должен быть включен.
Не учитывать проверку доступа по IP-адресу Код "SuppressIPRestriction"	Для пользователя, который имеет доступ к данной операции, при попытке входа в систему будут игнорироваться ограничения по IP-адресу.
Экспорт реестра	Право сохранения данных реестра в файл

Код "CanExportGrid" Системная операция	Описание формата *.xlsx. Если у пользователя нет права на данную операцию, то действие [Экспорт в Excel] в разделах и в меню блоков итогов "Список" неактивно.
Возможность запускать бизнес-процессы Код "CanRunBusinessProcesses"	Право запускать выполнение любых бизнес-процессов в системе. По умолчанию права на эту системную операцию предоставлены всем пользователям.
Отмена выполнения процесса Код "CanCancelProcess"	Право отменять выполнение запущенного бизнес-процесса в журнале процессов.
Доступ к настройке рабочих мест Код "CanManageWorkplaceSettings"	Право на создание и настройку рабочих мест : управление перечнем разделов, которые доступны в боковой панели.
Доступ к комментариям Код "CanEditOrDeleteComment"	Право редактировать и удалять комментарии к сообщениям в ленте.
Права на удаление сообщений и комментариев Код "CanDeleteAllMessageComment"	Право удалять сообщения и комментарии, оставленные другими пользователями в разделе [<i>Лента</i>], вкладке [<i>Лента</i>] панели уведомлений, а также на вкладке [<i>Лента</i>] страниц просмотра и редактирования разделов системы. Пользователи могут редактировать и удалять собственные сообщения и комментарии, не обладая доступом к данной системной операции.

Делегировать права доступа


ПРОДУКТЫ: [ВСЕ ПРОДУКТЫ](#)

Делегирование прав доступа позволяет передать все права доступа одного сотрудника другому на ограниченный период времени. Это полезно, например, когда сотрудник находится вне офиса или иным образом недоступен, и кто-то должен взять на себя его обязанности. Можно делегировать права отдельных пользователей или ролей любому количеству других пользователей или ролей.

Для делегирования прав у пользователя должен быть доступ к системным операциям **"Управление списком пользователей"** (код CanManageUsers) и **"Изменение делегируемых прав"** (код CanChangeAdminUnitGrantedRight).

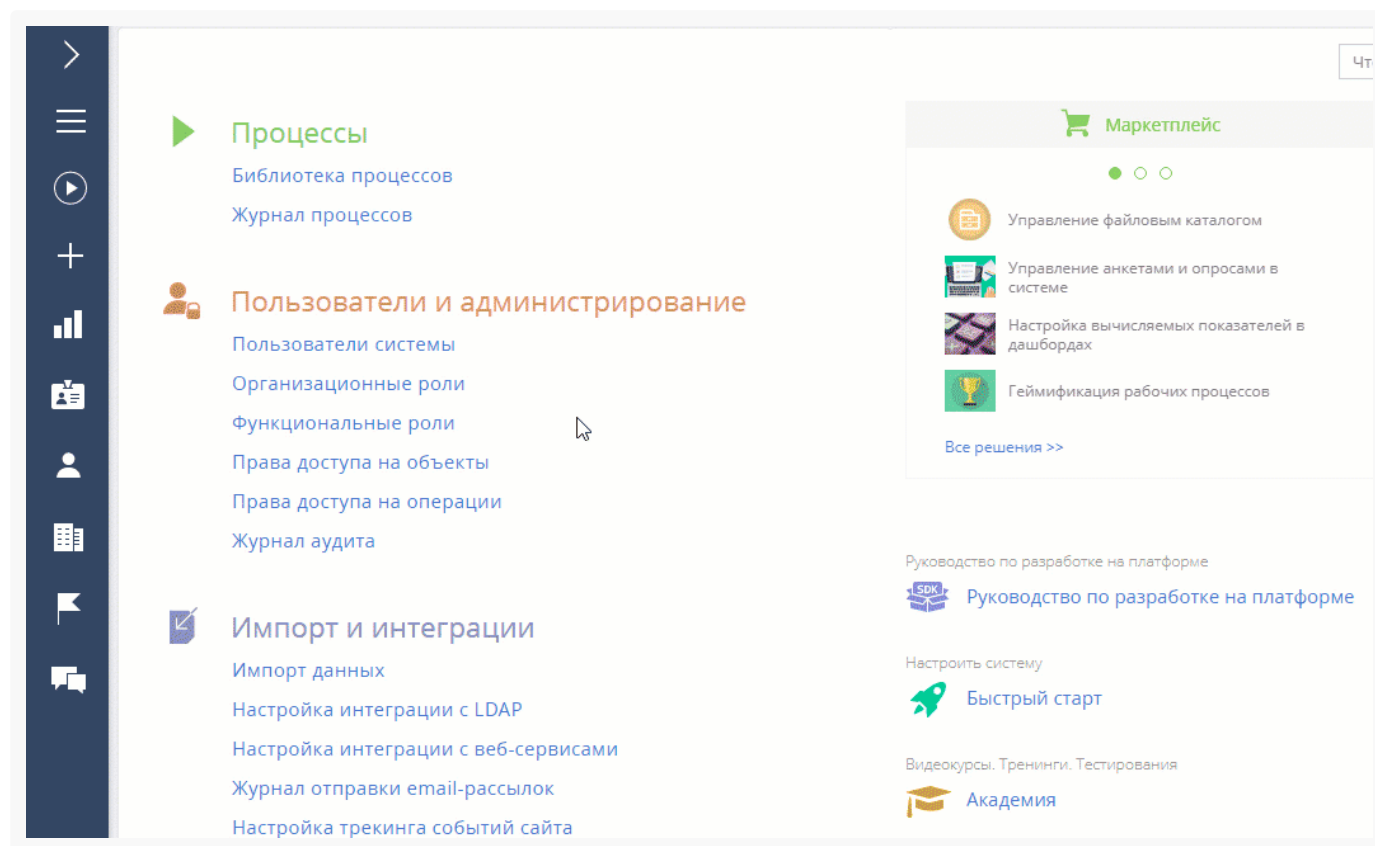
Делегировать права пользователя другим пользователям и ролям

Для того, чтобы делегировать права другому пользователю или группе пользователей:

1. Нажмите  —> **“Пользователи системы”**.
2. Откройте страницу пользователя, **чьи права вы хотите делегировать**.
3. Откройте вкладку [**Делегирование прав**] —> кнопка [**Делегировать права**].
4. В открывшемся окне выберите пользователя или группу пользователей, **которые получают права**, например организационная роль “Отдел продаж”.
5. Нажмите кнопку [**Выбрать**] в окне выбора пользователя или роли. Нажмите кнопку [**Заккрыть**] на странице пользователя.
6. Чтобы изменения вступили в силу, нажмите [**Действия**] —> [**Актуализировать роли**].


В результате на детали [**Делегирование прав доступа**] пользователи и роли, которые получили права, отображаются в колонке [**Получает права**], а пользователь, чьи права были делегированы, отображается в колонке [**Раздает права**] ([Рис. 1](#)).

Рис. 1 — Делегирование прав сотрудника другому сотруднику или группе



Делегировать права пользователю от других пользователей и ролей

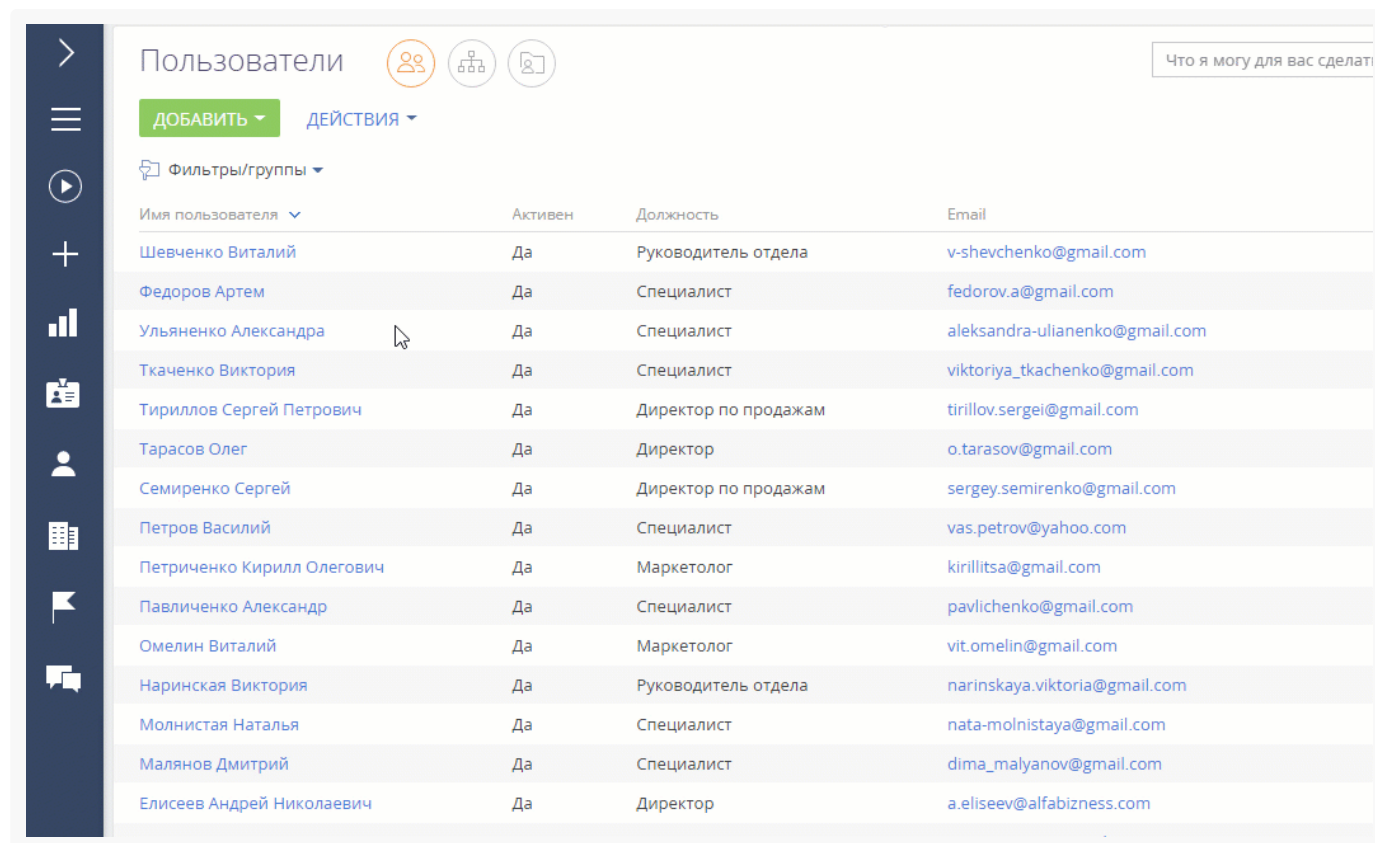
Чтобы передать пользователю права от других пользователей и ролей:

1. Нажмите  —> **“Пользователи системы”**.
2. Откройте страницу пользователя, **который получит права**.
3. Откройте вкладку [**Делегирование прав**] —> кнопка [**Получить права**].

4. В открывшемся окне выберите пользователя или группу пользователей, **чьи права необходимо делегировать**, например организационная роль “Отдел продаж”.
5. Нажмите кнопку [**Выбрать**] в окне выбора пользователя или роли. Нажмите кнопку [**Заккрыть**] на странице пользователя.
6. Чтобы изменения вступили в силу, нажмите [**Действия**] —> [**Актуализировать роли**].

В результате имя пользователя, который получил права, появится на детали [**Делегирование прав доступа**] в колонке [**Получает права**], а организационная роль, чьи права были делегированы, появится в колонке [**Раздает права**] ([Рис. 2](#)).

Рис. 2 — Делегирование прав пользователю от других пользователей и ролей



Имя пользователя	Активен	Должность	Email
Шевченко Виталий	Да	Руководитель отдела	v-shevchenko@gmail.com
Федоров Артем	Да	Специалист	fedorov.a@gmail.com
Ульяненко Александра	Да	Специалист	aleksandra-ulianenko@gmail.com
Ткаченко Виктория	Да	Специалист	viktoriya_tkachenko@gmail.com
Тириллов Сергей Петрович	Да	Директор по продажам	tirillov.sergei@gmail.com
Тарасов Олег	Да	Директор	o.tarasov@gmail.com
Семиренко Сергей	Да	Директор по продажам	sergey.semirenko@gmail.com
Петров Василий	Да	Специалист	vas.petrov@yahoo.com
Петриченко Кирилл Олегович	Да	Маркетолог	kirillitsa@gmail.com
Павличенко Александр	Да	Специалист	pavlichenko@gmail.com
Омелин Виталий	Да	Маркетолог	vit.omelin@gmail.com
Наринская Виктория	Да	Руководитель отдела	narinskaya.viktoria@gmail.com
Молнистая Наталья	Да	Специалист	nata-molnistaya@gmail.com
Малянов Дмитрий	Да	Специалист	dima_malyanov@gmail.com
Елисеев Андрей Николаевич	Да	Директор	a.eliseev@alfabizness.com

Удалить делегированные права доступа



1. Нажмите  —> “Пользователи системы”.
2. Откройте страницу пользователя, **делегированные права которого вы хотите удалить**.
3. Откройте вкладку [**Делегирование прав**], **отметьте запись**, которую вам необходимо удалить.
4. Нажмите  —> “Удалить” ([Рис. 3](#)). **Закройте страницу пользователя**.
5. Чтобы изменения вступили в силу, нажмите [**Действия**] —> [**Актуализировать роли**].

Рис. 3 — Удаление делегированных прав

Пользователи				Что я могу для вас сделать
<div>ДОБАВИТЬ</div> <div>ДЕЙСТВИЯ</div>				
Фильтры/группы				
Имя пользователя	Активен	Должность	Email	
Шевченко Виталий	Да	Руководитель отдела	v-shevchenko@gmail.com	
Федоров Артем	Да	Специалист	fedorov.a@gmail.com	
Ульяненко Александра	Да	Специалист	aleksandra-ulianenko@gmail.com	
Ткаченко Виктория	Да	Специалист	viktoriya_tkachenko@gmail.com	
Тириллов Сергей Петрович	Да	Директор по продажам	tirillov.sergei@gmail.com	
Тарасов Олег	Да	Директор	o.tarasov@gmail.com	
Семиренко Сергей	Да	Директор по продажам	sergey.semirenko@gmail.com	
Петров Василий	Да	Специалист	vas.petrov@yahoo.com	
Петриченко Кирилл Олегович	Да	Маркетолог	kirillitsa@gmail.com	
Павличенко Александр	Да	Специалист	pavlichenko@gmail.com	
Омелин Виталий	Да	Маркетолог	vit.omelin@gmail.com	
Наринская Виктория	Да	Руководитель отдела	narinskaya.viktoria@gmail.com	
Молнистая Наталья	Да	Специалист	nata-molnistaya@gmail.com	
Малянов Дмитрий	Да	Специалист	dima_malyanov@gmail.com	
Елисеев Андрей Николаевич	Да	Директор	a.eliseev@alfabizness.com	

В результате делегированные права доступа удаляются, у пользователя останутся только те права, которые были у него изначально.