**5.58 Управление доступом**

**Примечание для технического писателя**: подсистема Управление доступом допускает два взаимоисключающих варианта внедрения в конфигурацию, которые заметно различаются между собой по возможностям – это обычный и упрощенный режимы настройки прав доступа. Кроме того, в конфигурации может быть предусмотрена или отключена возможность по настройке прав доступа к отдельным объектам. Поэтому далее по тексту приведены примечания, к какому режиму настройки относится тот или иной фрагмент документации. При компоновке документации необходимо оставить только те фрагменты этого раздела, которые относятся к конкретному варианту внедрения подсистемы Управление доступом, используемому в конфигурации.

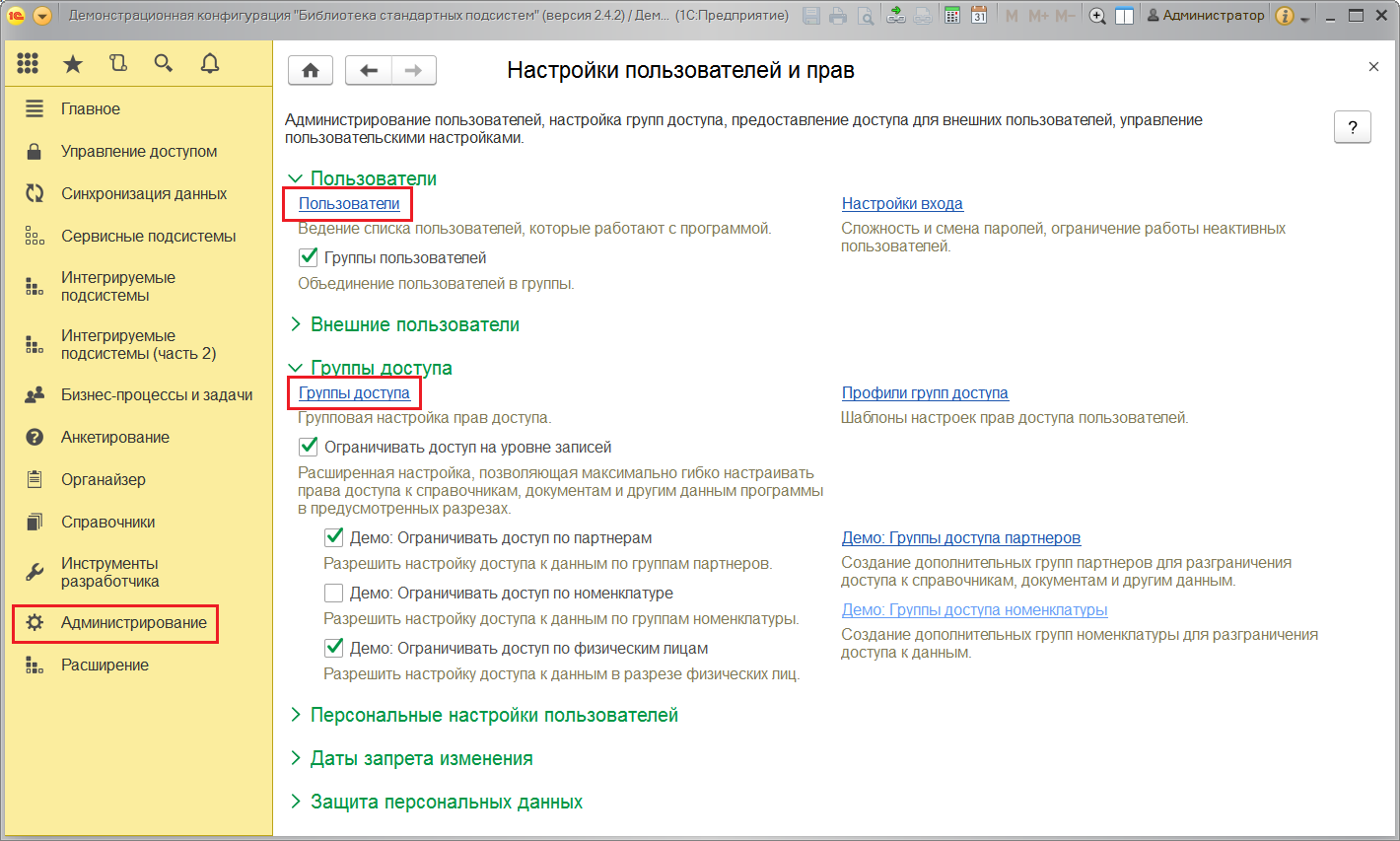
Программа позволяет настроить доступ пользователей к различным функциям, спискам и документам. Предусмотрены предопределенные наборы ролей. Кроме этого, имеется возможность самостоятельной настройки доступа. Для управления доступом необходима роль Администратор или Полные права. При этом пользователь, назначенный ответственным в группе доступа, может изменять состав своей группы доступа (для этого необходимо установить роль Изменение участников групп доступа).

**Для обычного режима настройки прав доступа**:

Для ведения списка пользователей и настройки их прав предназначены списки Пользователи и Группы доступа (раздел **Администрирование** – Настройка пользователей и прав – Пользователи).

Группа доступа определяет совокупность действий с данными программы, которые могут выполнять участники этой группы. Как правило, группы доступа соответствуют различным должностным обязанностям (или видам деятельности) пользователей программы. Пользователь может входить одновременно в одну или несколько групп доступа, которые в совокупности образуют его персональные настройки прав доступа.

Примечание: не следует для настройки прав доступа использовать режим конфигурирования 1С:Предприятия.



**Для упрощенного режима настройки прав доступа:**

Для ведения списка пользователей и настройки их прав предназначен список Пользователи (раздел **Администрирование** – Настройка пользователей и прав – Пользователи). Настройка прав доступа пользователей осуществляется с помощью профилей. Профиль определяет некоторую совокупность действий с данными программы, которые может выполнять пользователь. Как правило, профили соответствуют различным должностным обязанностям (или видам деятельности) пользователей программы. Пользователю могут быть назначены одновременно несколько профилей, которые в совокупности образуют его персональные настройки прав доступа.

Примечание: не следует для настройки прав доступа использовать режим конфигурирования 1С:Предприятия.

**Для обоих режимов настройки прав доступа**:

Кроме того, для отдельных объектов программы (например, для папок файлов) предусмотрена возможность настраивать права доступа непосредственно из окна этого объекта. Такую настройку могут выполнять не только администраторы, но и пользователи с соответствующими правами.

**Настройка программы**

Для того чтобы максимально гибко настраивать права доступа пользователей, необходимо включить флажок Ограничивать доступ на уровне записей в разделе **Администрирование** – Настройки пользователей и прав – Группы доступа. Включить этот режим рекомендуется в тех случаях, когда он действительно востребован (например, с программой работает много пользователей).

В этом случае становятся доступными следующие возможности:

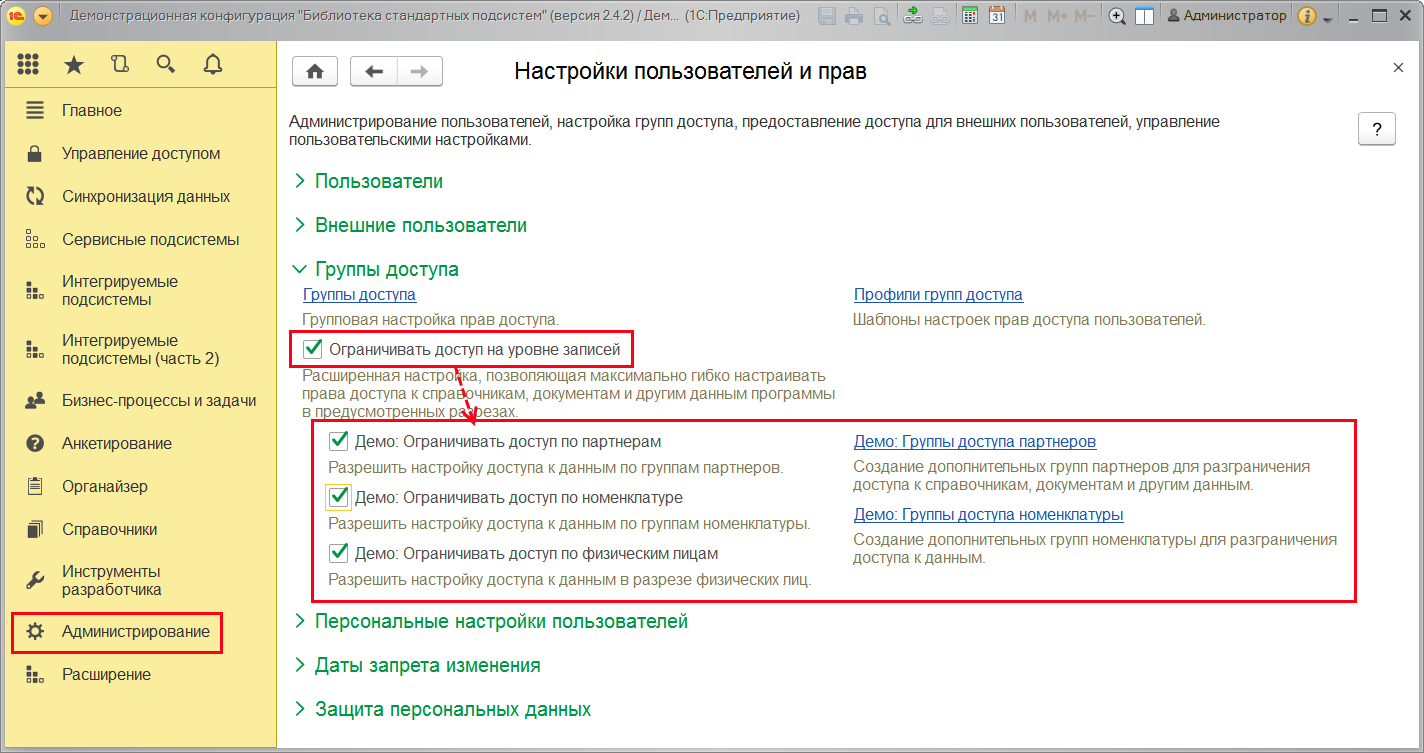
■ **Демо: Ограничивать доступ по партнерам** – разрешить настройку доступа к данным по группам партнеров, в этом случае становится доступной ссылка:

**Демо: Группы доступа партнеров** – создание групп партнеров для разграничения доступа к справочникам, документам и другим данным.

■ **Демо: Ограничивать доступ по номенклатуре** – включите флажок, для того чтобы разрешить настройку доступа к данным по группам номенклатуры. После этого становится доступной ссылка:

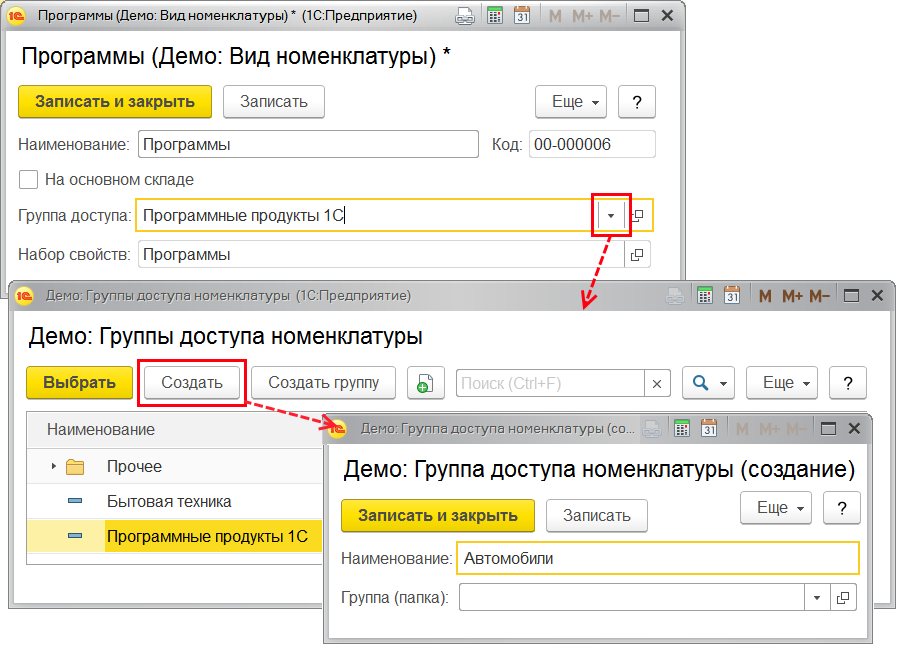
**Демо: Группы доступа номенклатуры** – создание дополнительных групп номенклатуры для разграничения доступа к данным.

■ **Демо: Ограничивать доступ по физическим лицам** – разрешить настройку доступа к данным в разрезе физических лиц.



Например, в списке **Демо: Номенклатура** после включения флажка **Демо: Ограничивать доступ по номенклатуре** становится возможным организовать группы доступа к видам номенклатуры в списке **Демо: Группы доступа номенклатуры**.

Для каждого вида номенклатуры становится доступным поле Группа доступа. Для ограничения доступа по номенклатуре укажите для вида номенклатуры группу доступа. Если в списке нет нужной группы доступа, введите ее с помощью кнопки Создать.



Включение режима ограничения прав доступа пользователей на уровне записей может занять длительное время в зависимости от объема данных, введенных в программу. Если в программу до включения этого режима был введен большой объем данных, программа выводит предупреждение.

Подготовка служебных данных, необходимых для работы в этом режиме, выполняется в фоне с помощью регламентного задания Заполнение данных для ограничения доступа. Если в программу введен большой объем данных, то рекомендуется предварительно настроить его запуск в то время, когда с программой не работают пользователи. Подробнее о работе с регламентными заданиями см. раздел документации Регламентные задания.

**Примечание для технического писателя:**

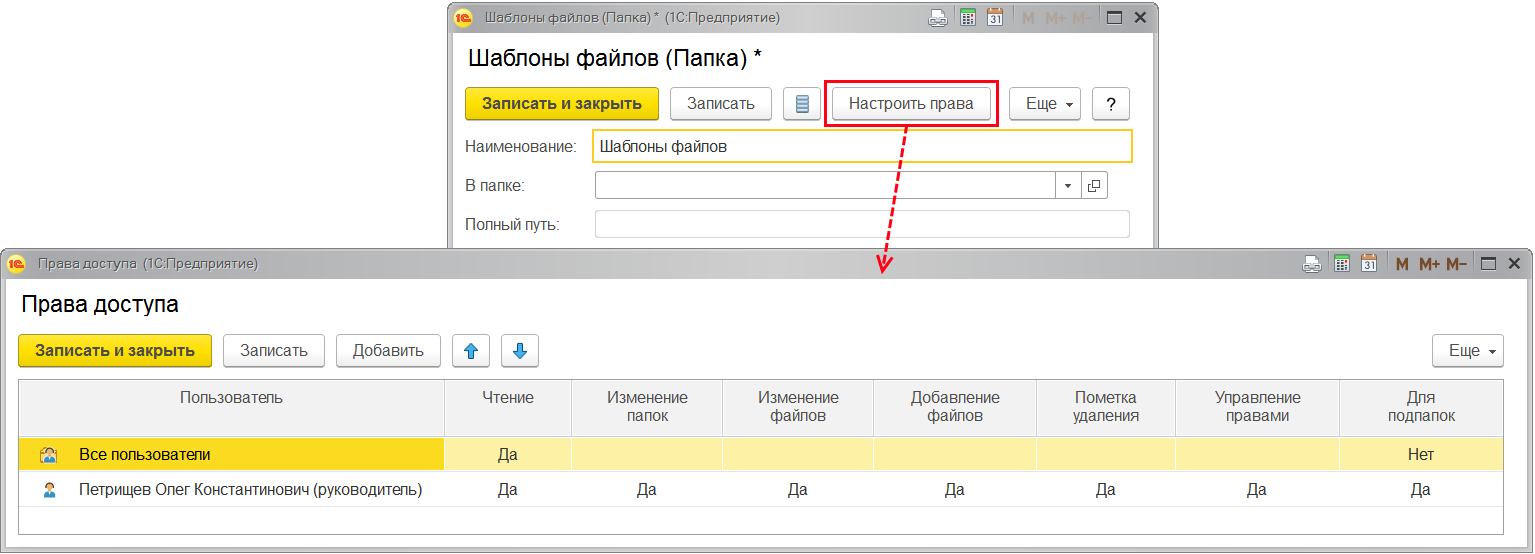
**Для версий программы, у которых режим совместимости ниже 8.3.3**, следует дополнить текст фразой: Если программа работает в файловом режиме, то регламентное задание необходимо запустить вручную.

**Настройка прав доступа к отдельным объектам**

**Для конфигураций, в которых предусмотрена возможность по настройке прав доступа к отдельным объектам:**

Для папок файлов и проектов имеется возможность индивидуальной настройки прав доступа для отдельных пользователей или групп пользователей. Способ этой настройки очень похож на тот способ, который применяется при настройке прав доступа на папки файлов в операционной системе на компьютере.

Для перехода к настройке прав из окна объекта можно воспользоваться кнопкой Настроить права. Для использования данной возможности необходимо установить роль **Демо: Работа с папками файлов**, также должен быть включен флажок Ограничивать доступ на уровне записей (см. раздел [Настройка программы](https://its.1c.ru/db/content/bsp301doc/src/5.58%20%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5%20%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BE%D0%BC.htm?_=1542292879#_настройка_программы_53)).



В открывшемся окне Права доступа можно указать, какие пользователи (или группы пользователей) должны иметь доступ к данному объекту и к его дочерним объектам. Установка прав осуществляется с помощью значений Да или Нет в соответствующих колонках. Настройку могут выполнять пользователи с установленным правом администрирования (Да в колонке Управление правами) для этого объекта.

Установив значение Нет в колонке Для подпапок, можно отказаться от наследования настроек прав доступа, заданных для родительского объекта (например, у родительской папки файлов).

В соответствующих колонках можно включить права на чтение, добавление, изменение и установку пометки удаления для папки и файлов в ней:

■ Чтение;

■ Изменение папок;

■ Изменение файлов;

■ Пометка удаления.

В колонке Управление правами необходимо установить значение Да только у тех пользователей, которые должны иметь возможность настраивать права для этого объекта.

Для того чтобы увидеть полный список папок и прав на них, настроенных для интересующего пользователя (или группы пользователей), можно воспользоваться аналитическим отчетом Отчет по правам доступа пользователя. Подробнее см. раздел [Отчет по правам доступа](https://its.1c.ru/db/content/bsp301doc/src/5.58%20%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5%20%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BE%D0%BC.htm?_=1542292879#_отчет_по_правам_4).

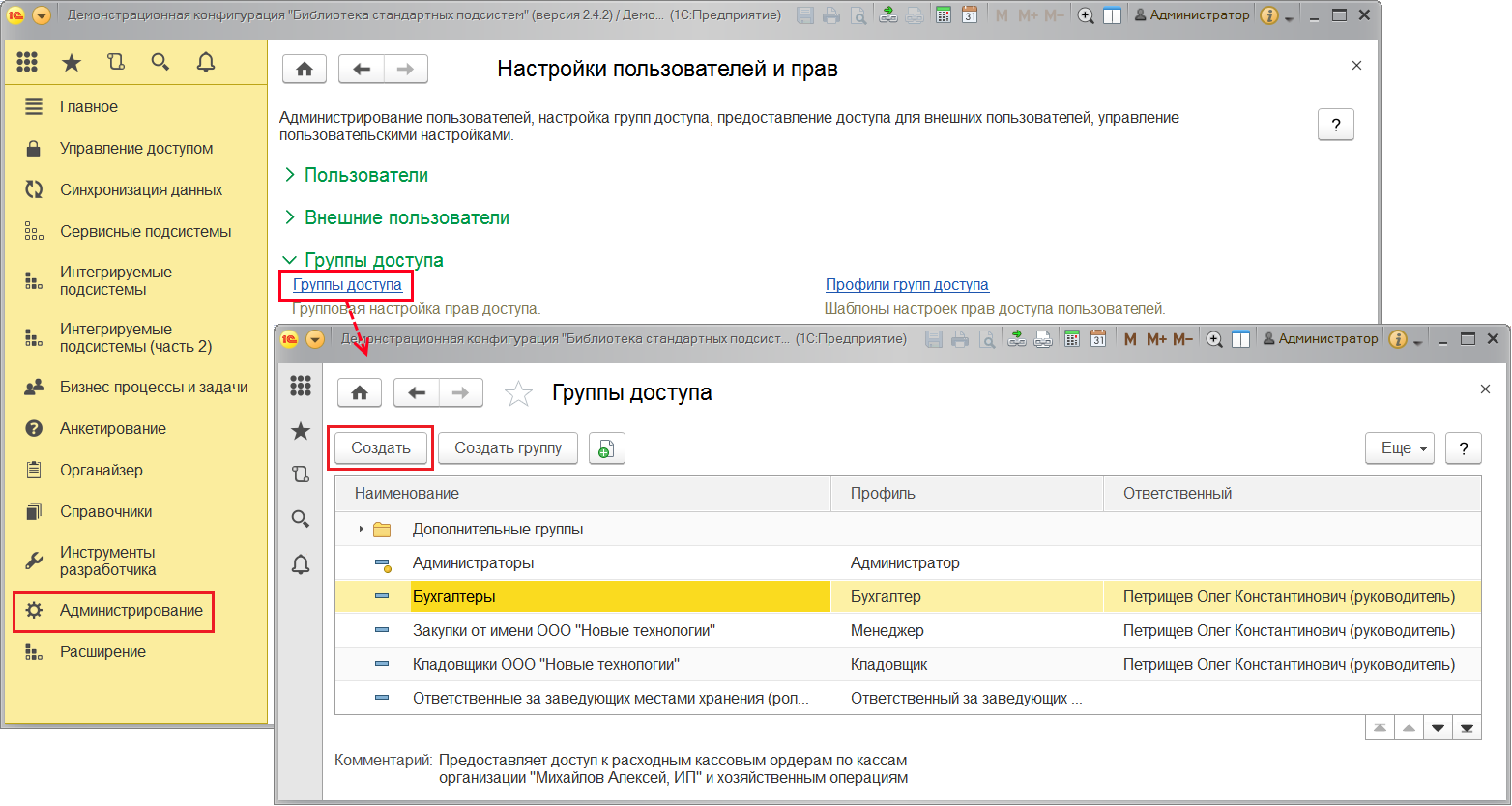
**Настройка групп доступа**

**Этот раздел содержит описание только для обычного режима настройки прав доступа**.

С помощью групп доступа можно задавать и администрировать общие настройки прав доступа для некоторой группы пользователей, выполняющих однотипные функции в программе, например: **Бухгалтеры центрального офиса** или **Менеджеры по продажам филиала в городе Н. (мелкооптовые покупатели)**. Права на редактирование списка Группы доступа имеются только у администраторов программы, перечисленных в предопределенной группе доступа Администраторы. Кроме того, пользователь, указанный в группе доступа как Ответственный, может изменять состав участников данной группы.

Группа доступа всегда связана с одним из имеющихся профилей групп доступа, которые, как правило, объединяют в себе несколько ролей. При включении пользователя в группу доступа ему назначаются все роли, заданные в профиле группы доступа. Например, предопределенная группа доступа Администраторы связана с профилем Администратор, в состав которого входит роль Полные Права. Эта роль предоставляет неограниченный доступ ко всем данным и назначается всем администраторам программы, перечисленным в группе доступа Администраторы. Подробнее о профилях групп доступа см. разделы [Состав профилей групп доступа](https://its.1c.ru/db/content/bsp301doc/src/5.58%20%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5%20%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BE%D0%BC.htm?_=1542292879#_состав_профилей_групп_4) и [Особые случаи настройки прав доступа](https://its.1c.ru/db/content/bsp301doc/src/5.58%20%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5%20%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BE%D0%BC.htm?_=1542292879#_особые_случаи_настройки_4).

Для создания новой группы доступа необходимо перейти в список Группы доступа раздела **Администрирование** – Настройки пользователей и прав – Группы доступа.

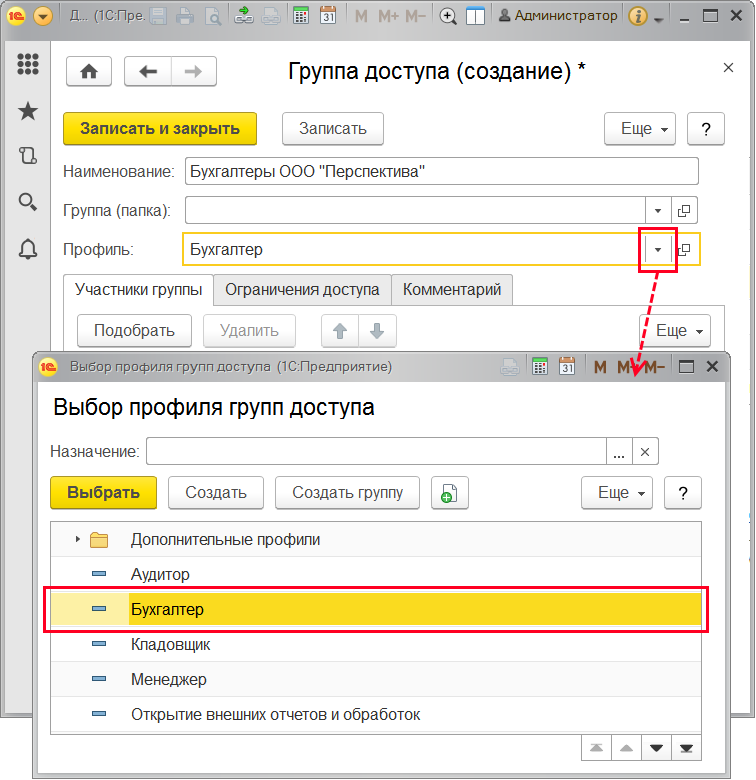


Нажмите кнопку Создать.

Заполните поле Наименование.

Рекомендуется называть группу доступа во множественном числе таким образом, чтобы ее имя содержало указание на используемый в ней профиль (в поле Профиль) и однозначно характеризовало определенный в ней состав настроек прав доступа. Например, на базе профиля **Менеджеры по продажам** могут быть введены группы доступа **Менеджеры по продажам в ООО «Далекая перспектива»** и **Менеджеры по продажам в ЗАО «Новые технологии»**.

В карточке группы доступа нужно выбрать один из имеющихся Профилей групп доступа (см. раздел [Состав профилей групп доступа](https://its.1c.ru/db/content/bsp301doc/src/5.58%20%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5%20%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BE%D0%BC.htm?_=1542292879#_состав_профилей_групп_4)) с помощью кнопки https://its.1c.ru/db/content/bsp301doc/src/_img/a8ac365292f91872c91b58b5276d597d/image403.png?_=1542292879.



Допустимые участники группы доступа определяются в профиле в соответствии с выбранным назначением.

В составе участников группы доступа могут быть также перечислены внешние пользователи и группы внешних пользователей (это может понадобиться для проведения анкетирования, например). Для этого в профиле групп доступа в поле **Назначение** должны быть выбраны партнеры или контактные лица партнеров. Подробнее см. раздел [Особые случаи настройки прав доступа](https://its.1c.ru/db/content/bsp301doc/src/5.58%20%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5%20%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BE%D0%BC.htm?_=1542292879#_особые_случаи_настройки_4).

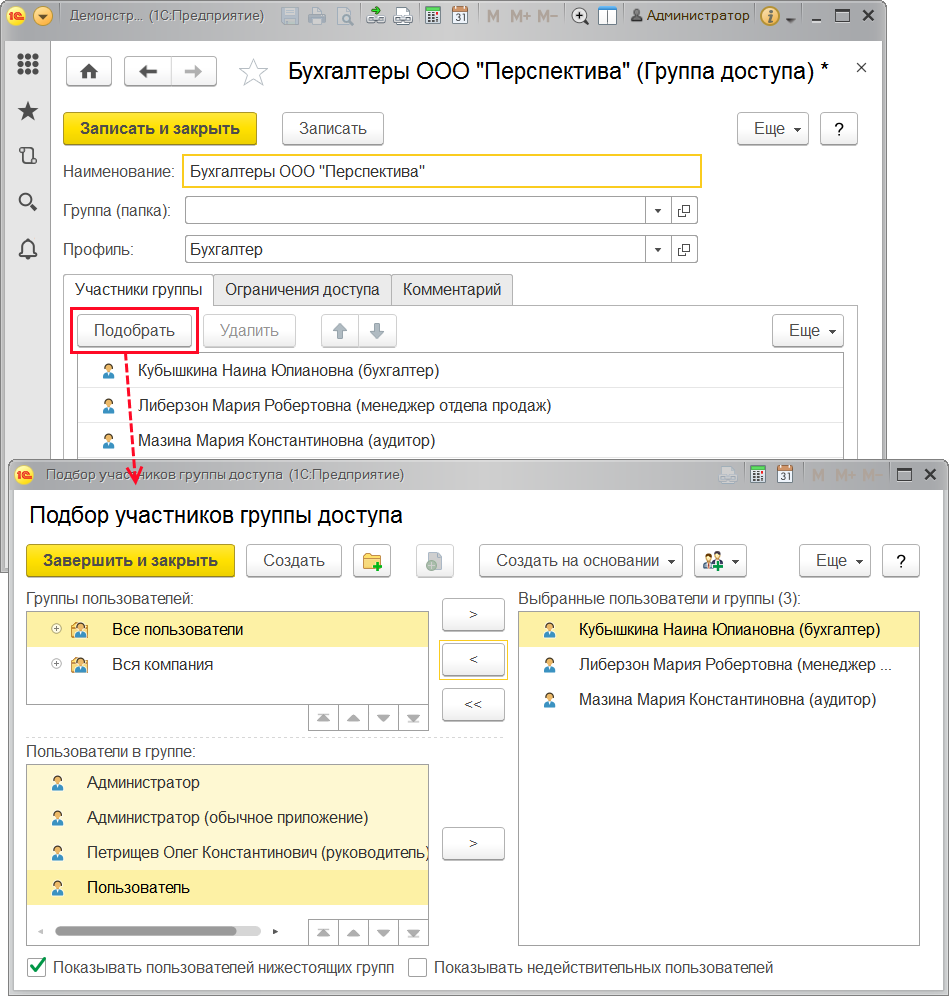
На вкладке Участники группы перечислите список пользователей (и групп пользователей), на которых должны распространяться настройки прав доступа. Списки, из которых можно выбрать участников группы, перечислены в поле Допустимые участники в нижней части вкладки.

Для быстрого перечисления пользователей можно нажать кнопку Подобрать. Подберите нужных пользователей. Открывшийся список выбора состоит из двух частей:

■ В левой части окна выберите нужную группу пользователей (можно выбрать всю группу сразу), выберите нужных пользователей из этой группы;

■ В правой части окна перечисляются выбранные пользователи.

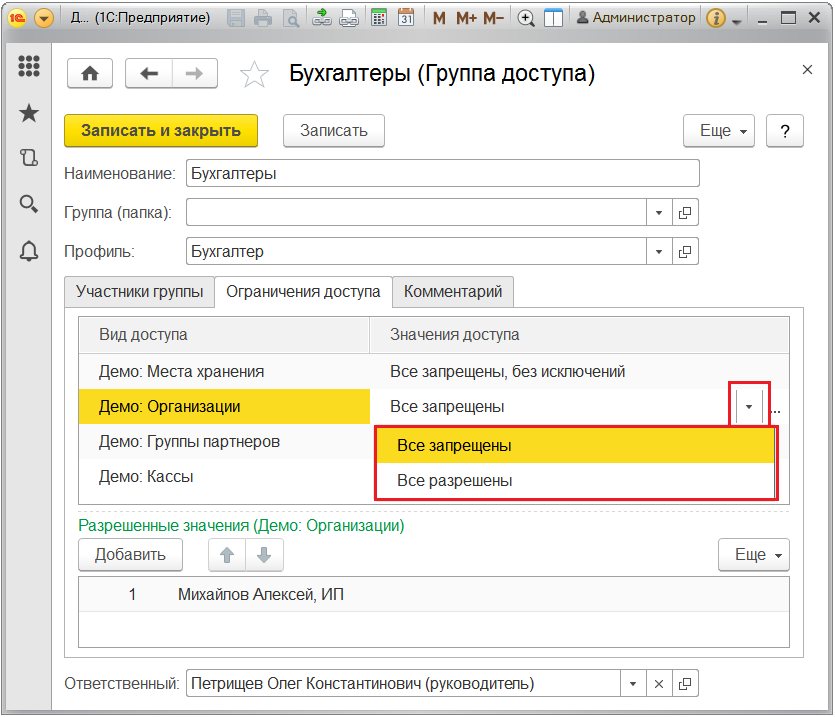
Затем нажмите кнопку Завершить и закрыть для возврата к настройке группы доступа.



В поле Ответственный выберите пользователя, который будет ответственным за состав участников группы доступа.

Затем на вкладке Ограничения доступа необходимо указать дополнительные настройки прав доступа. Примечание: вкладка может быть недоступна для тех групп доступа, в которых такая настройка не предусмотрена (зависит от настроек выбранного профиля).

На этой вкладке с помощью поля Вид доступа можно задать границы области данных, с которой разрешено работать участникам группы доступа. Под видом доступа подразумевается некоторое правило, по которому «разрешается» доступ к данным программы. Например, с помощью вида доступа **Демо: Организации** можно разрешить работать пользователям только с документами по конкретным организациям; или наоборот, скрыть от них документы некоторых организаций. Состав видов доступа, перечисленных на вкладке Ограничения доступа, зависит от профиля, выбранного в поле Профиль. Кроме того, профиль также определяет, как именно действует настройка вида доступа: она разрешает только просмотр или также включает возможность редактирования данных. Например, в случае если профиль групп доступа включает в себя роль для чтения документов **Демо:** **Поступление товаров**, то пользователи получают возможность просматривать документы по заданным организациям. Если же в профиле содержится роль для добавления и изменения, то появляется возможность редактировать такие документы.



Для каждого вида доступа можно указать либо список разрешенных значений, либо наоборот, список тех значений, которые не должны быть доступны. Первый способ настройки подходит в тех случаях, когда стоит задача предоставить доступ только к определенной области данных. Второй способ настройки удобен тогда, когда требуется закрыть доступ к заранее известной области данных, а для всех новых значений, вводимых в программу, должны по умолчанию действовать разрешительные правила. Например, если с помощью вида доступа **Демо:** **Организации** задано правило, запрещающее работать с документами по организации **Далекая перспектива**, то на новую организацию **Новые технологии**, введенную в программу позднее, эти ограничения распространяться не будут. При этом следует учитывать, что разрешающие настройки имеют приоритет над запрещающими. Так, если в приведенном выше примере пользователю будет разрешен ввод документов по организации **Далекая перспектива** в какой-либо другой группе доступа с тем же профилем, то в итоге он получит доступ ко всем документам по этой организации.

В ряде случаев для упрощения настройки прав доступа, в списке разрешенных или запрещенных значений можно указывать не отдельные элементы, а целые группы элементов. Например, для вида доступа **Демо: Группы партнеров** можно ограничить доступ в разрезе групп доступа партнеров, а не по каждому партнеру в отдельности. Для этого необходимо определить список групп доступа партнеров, и у каждого партнера задать принадлежность к той или иной группе. Эти действия могут быть выполнены не только администратором, но и любым пользователем с соответствующими правами на редактирование списка партнеров.

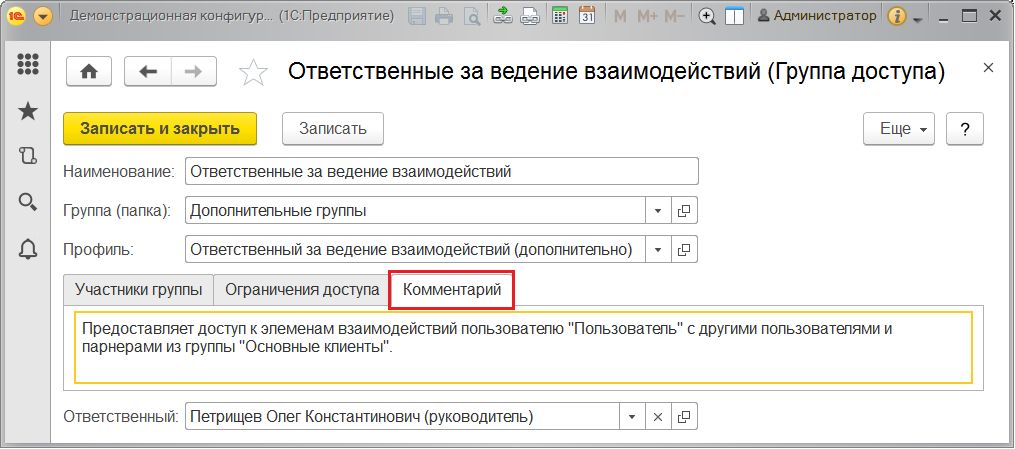
Нажмите кнопку Добавить, выберите из списка нужного партнера с помощью кнопки https://its.1c.ru/db/content/bsp301doc/src/_img/a8ac365292f91872c91b58b5276d597d/image1856.png?_=1542292879. Для использования данной возможности необходимы соответствующие настройки. См. раздел [Настройка программы](https://its.1c.ru/db/content/bsp301doc/src/5.58%20%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5%20%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BE%D0%BC.htm?_=1542292879#_настройка_программы_53).

В некоторых группах доступа предусмотрена настройка прав с помощью вида доступа Пользователи (аналогично, вид доступа **Внешние пользователи** для внешних пользователей). Настройка может учитываться только в тех документах (и других объектах программы), в полях которых могут быть указаны пользователи, получающие доступ к этим документам (Ответственный, Автор, Исполнитель и т.п.). Для того чтобы дать участникам группы права доступа ко всем ограниченным данным, с которыми работает тот или иной пользователь, необходимо включить его в список разрешенных значений для вида доступа Пользователи. Например, если доступ к документам поступления товаров и услуг зависит от того, кто указан в поле **Ответственный**, тогда записывать документы имеет возможность пользователь, который выбран в этом поле, либо он сам, либо в списке разрешенных для вида доступа **Пользователи**. Аналогичным образом действует запрещающая настройка.

Пользователь может быть включен сразу в несколько групп доступа. В этом случае его совокупные права доступа складываются (объединяются по «или») из прав доступа каждой группы. Например, в группе доступа **Менеджеры по закупкам** пользователю разрешен просмотр документов **Демо: Поступления товаров** по организации **Далекая перспектива**. В группе доступа **Менеджеры по продажам** ему разрешен ввод документов **Демо: Заказ покупателя** по организации **Новые технологии**. В результате у него появляется доступ на просмотр документов **Демо:** **Поступления товаров** по организации **Далекая перспектива** и на ввод документов **Демо:** **Заказ покупателя** по организации **Новые технологии**. При этом следует учитывать, что объединяются не списки разрешенных значений, указанные в группах, а именно права доступа. Т.е. ошибочно считать, что в приведенном примере пользователь получит доступ на просмотр документов поступления товаров и на ввод документов заказов покупателей одновременно по обеим организациям.

Просмотреть права доступа пользователя можно с помощью отчета по правам доступа. Подробнее см. раздел [Отчет по правам доступа](https://its.1c.ru/db/content/bsp301doc/src/5.58%20%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5%20%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BE%D0%BC.htm?_=1542292879#_отчет_по_правам_4).

На вкладке Комментарий введите дополнительную информацию о группе доступа.



**Настройка прав доступа отдельных пользователей**

**Этот раздел содержит описание только для обычного режима настройки прав доступа.**

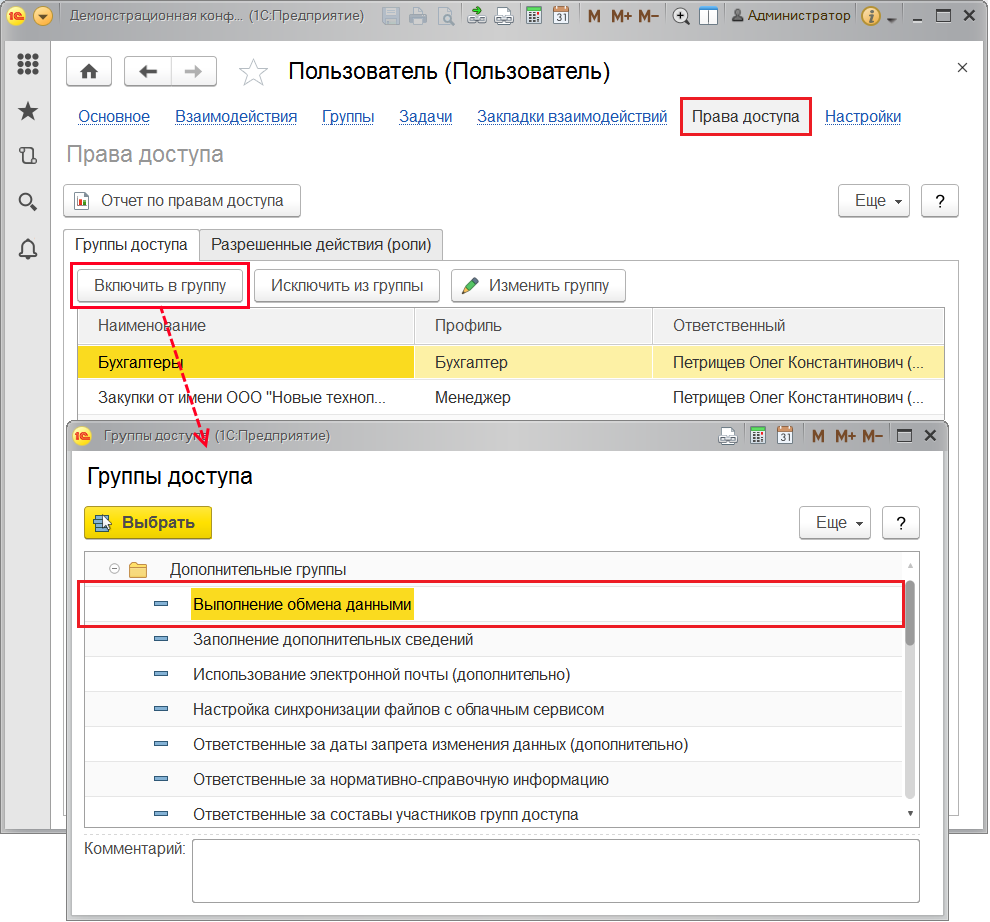
Для просмотра и настройки состава групп доступа интересующего пользователя (или группы пользователей; далее просто «пользователя») перейдите по ссылке Права доступа в панели навигации карточки пользователя.

С помощью кнопки Включить в группу на вкладке Группы доступа администратор может добавить пользователя в состав участников любой из имеющихся групп доступа.

С помощью кнопки Исключить из группы можно удалить пользователя из выделенной группы доступа.

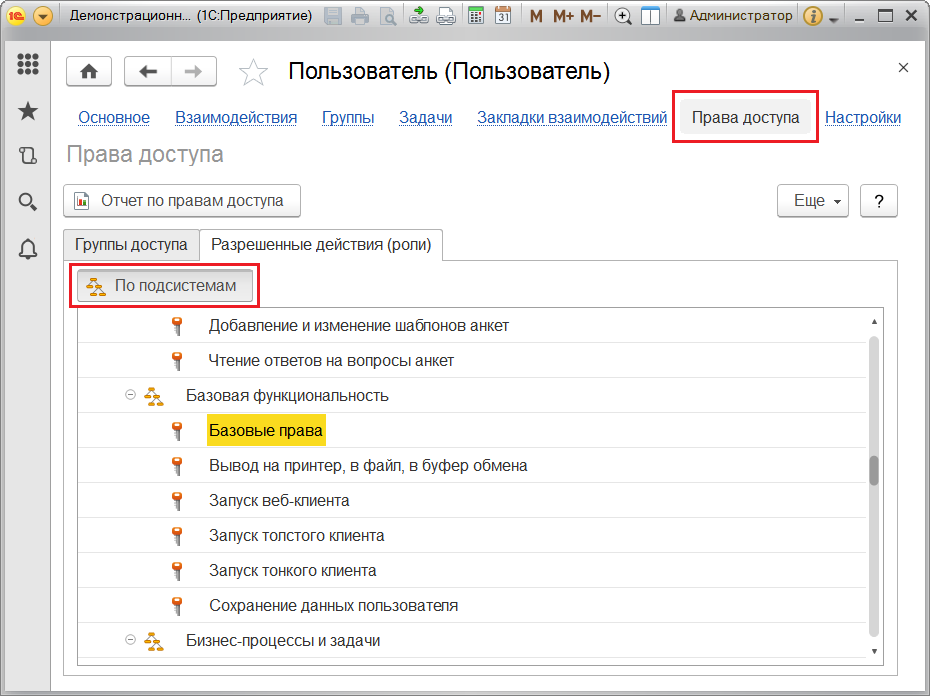
Также эту настройку могут выполнять ответственные за состав участников группы доступа для своих групп доступа.

С помощью кнопки Изменить группу можно перейти к карточке группы доступа, выбранной в списке.



На вкладке Разрешенные действия (роли) справочно выводится совокупный список ролей, которые назначены пользователю. Список ролей складывается из всех ролей, входящих в состав групп доступа, в которые включен пользователь. Этот же список можно увидеть в Конфигураторе, в свойствах пользователя информационной базы. При этом не следует редактировать этот список в режиме конфигурирования 1С:Предприятия, настройка прав доступа пользователей должна выполняться только с помощью групп доступа.

С помощью кнопки По подсистемам можно соответственно сгруппировать разрешенные действия.

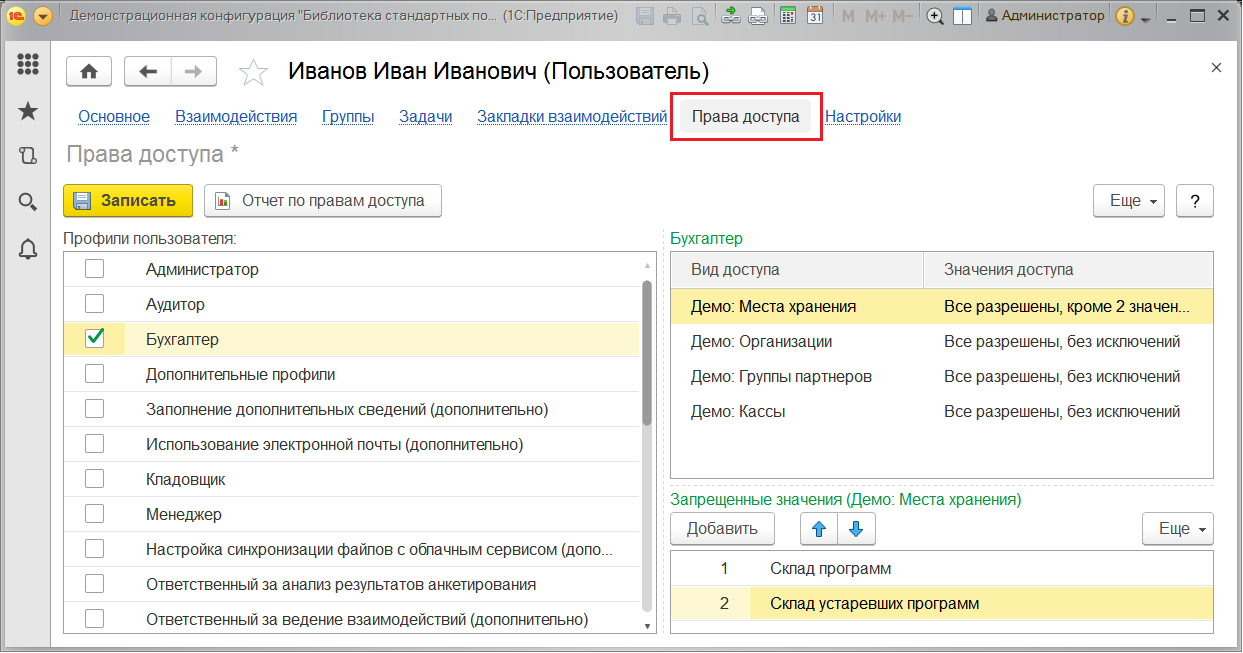


**Настройка прав доступа пользователей**

**Этот раздел содержит описание только для упрощенного режима настройки прав доступа**.

Для настройки прав доступа пользователя необходимо перейти в список Пользователи и нажать на ссылку Права доступа в панели навигации карточки пользователя. В списке Профили пользователя необходимо отметить те профили, которые требуются для работы пользователя в программе. Например, если сотрудник выполняет в программе только функции бухгалтера, то ему должны быть назначены профиль **Бухгалтер**, а также служебный профиль **Пользователь** (который разрешает выполнять вход в программу).

Профиль, как правило, объединяет в себе несколько ролей. При назначении профиля пользователю назначаются все роли, заданные в этом профиле. Например, в профиль Администратор входит роль Полные права, которая предоставляет неограниченный доступ ко всем данным. Описание имеющихся профилей см. далее в разделе [Состав профилей групп доступа](https://its.1c.ru/db/content/bsp301doc/src/5.58%20%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5%20%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%BE%D0%BC.htm?_=1542292879#_состав_профилей_групп_4). Права доступа могут настраивать только администраторы программы (пользователи, у которых отмечен профиль Администратор).



В списке справа с помощью поля Вид доступа можно задать границы области данных, с которой пользователю разрешено работать. Под видом доступа подразумевается некоторое правило, по которому «разрешается» доступ к данным программы. Например, с помощью вида доступа **Демо:** **Организации** можно разрешить пользователю работать только с документами по конкретным организациям; или наоборот, скрыть от него документы некоторых организаций. Состав видов доступа, перечисленных в списке справа, зависит от профиля, выбранного в списке слева. Кроме того, профиль также определяет, как именно действует настройка вида доступа: она разрешает просмотр или также включает возможность редактирования документов. Например, в случае если профиль включает в себя роль для чтения документов **Демо: Поступление товаров**, то пользователь получает возможность просматривать документы по заданным организациям. Если же в профиле содержится роль для добавления и изменения, то появляется возможность редактировать такие документы.

Для каждого вида доступа можно указать либо список разрешенных значений, либо наоборот, список тех значений, которые не должны быть доступны. Первый способ настройки подходит в тех случаях, когда стоит задача предоставить доступ только к определенной области данных. Второй способ настройки удобен тогда, когда требуется закрыть доступ к заранее известной области данных, а для всех новых значений, вводимых в программу, должны по умолчанию действовать разрешительные правила. Например, если с помощью вида доступа **Демо:** **Организации** задано правило, запрещающее работать с документами по организации **Далекая перспектива**, то на новую организацию **Новые технологии**, введенную в программе позднее, эти ограничения распространяться не будут. При этом следует учитывать, что разрешающие настройки имеют приоритет над запрещающими. Так, если в приведенном выше примере пользователю будет разрешен ввод документов по организации **Далекая перспектива** в какой-либо другой группе с этим же профилем, то в итоге он получит доступ ко всем документам по этой организации.

В ряде случаев для упрощения настройки прав доступа, в списке разрешенных или запрещенных значений можно указывать не отдельные элементы, а целые группы элементов. Например, для вида доступа **Демо: Группы партнеров** можно ограничить доступ в разрезе групп доступа партнеров, а не по каждому партнеру в отдельности. Для этого необходимо определить список групп доступа партнеров, и у каждого партнера задать принадлежность к той или иной группе. Эти действия могут быть выполнены не только администратором, но и любым пользователем с соответствующими правами на редактирование списка партнеров.

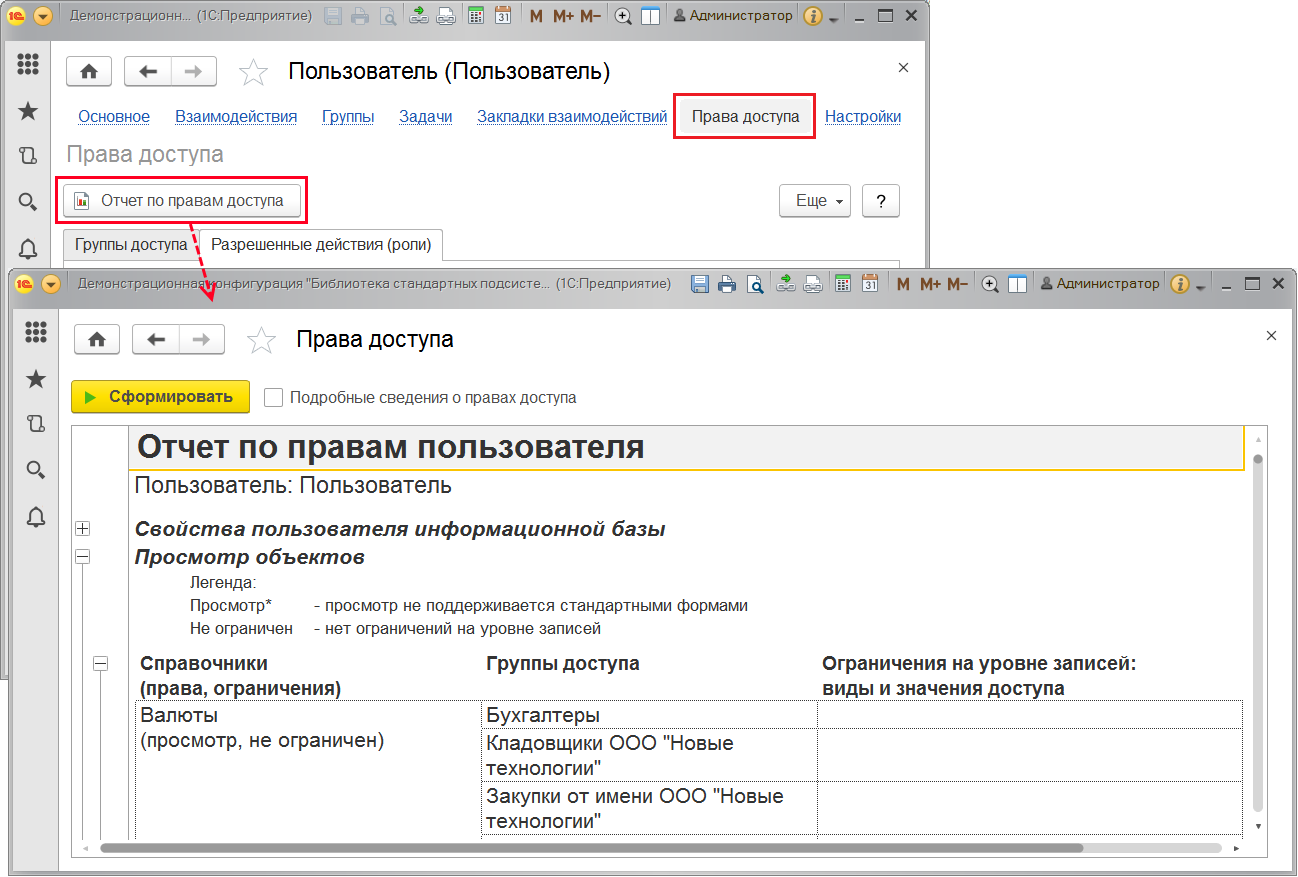
Для некоторых профилей предусмотрена настройка прав с помощью вида доступа Пользователи (аналогично, вид доступа **Внешние пользователи** для внешних пользователей). Настройка может учитываться только в тех документах (и других объектах программы), в полях которых могут быть указаны пользователи, получающие доступ к этим документам (Ответственный, Автор, Исполнитель и т.п.). Для того чтобы дать доступ ко всем ограниченным данным, с которыми работает тот или иной пользователь, необходимо включить его в список разрешенных значений для вида доступа Пользователи. Например, если доступ к документам поступления товаров и услуг зависит от того, кто указан в поле **Ответственный**, тогда записывать документы имеет возможность пользователь, который либо выбран в этом поле, либо указан в списке разрешенных для вида доступа **Пользователи**. Аналогичным образом действует запрещающая настройка.

В случае если в разделе **Администрирование** – Настройки пользователей и прав – Группы доступа выключен флажок Ограничивать доступ на уровне записей, список видов доступа скрыт.

**Отчет по правам доступа**

Для того чтобы увидеть полный список прав доступа пользователя, можно воспользоваться аналитическим отчетом Отчет по правам доступа пользователя.

Отчет можно открыть из карточки пользователя (группы пользователя) со страницы Права доступа с помощью соответствующей кнопки.



Для того чтобы получить подробный отчет, включите флажок Подробные сведения о правах доступа, нажмите кнопку Сформировать.

В отчете отражены все сведения о правах доступа пользователя:

■ Свойства пользователя информационной базы:

доступ к информационной базе, имя для входа, имя пользователя операционной системы и другие сведения;

■ Группы доступа пользователя:

Наименование группы, ответственный, профиль;

■ Роли пользователя по профилям;

■ Просмотр объектов:

Включает таблицу из 3 колонок: Объект/Права/Ограничения, Группа доступа/Профиль/Роли, Ограничения на уровне записей/Виды и значения доступа;

■ Редактирование объектов:

Включает таблицу из 3 колонок: Объект/Права/Ограничения, Группа доступа/Профиль/Роли, Ограничения на уровне записей/Виды и значения доступа;

■ Права на объекты:

Папки.

Отчет с помощью стандартных кнопок можно распечатать или сохранить на компьютере в нужном формате.

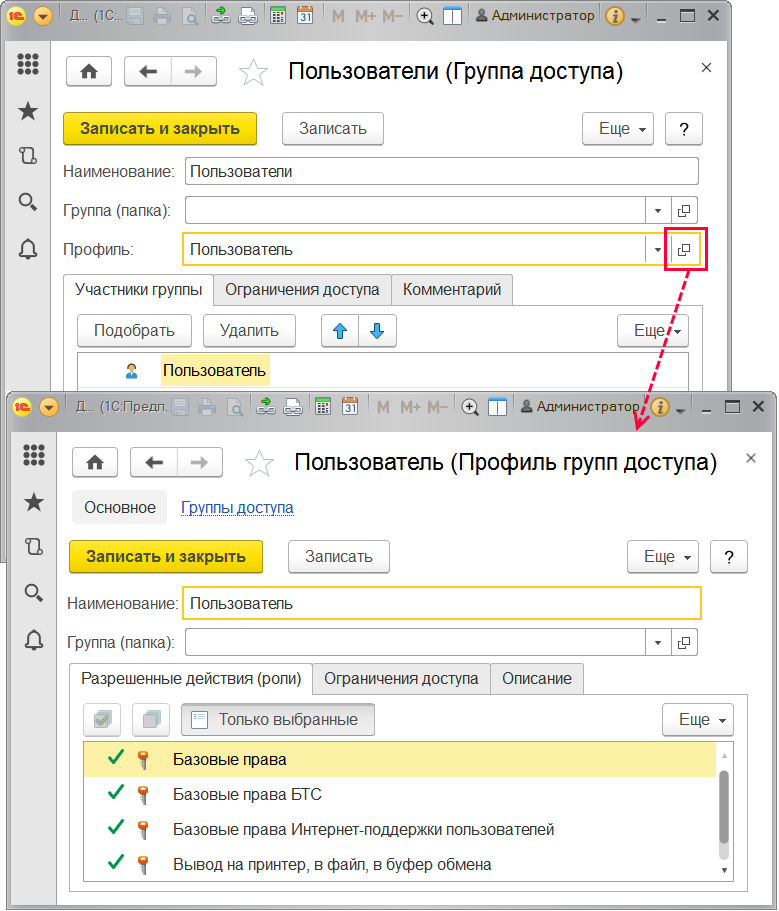
**Особые случаи настройки прав доступа**

**Для упрощенного режима настройки прав доступа термин «профиль групп доступа» далее по тексту рекомендуется называть «профиль пользователей».**

В ряде случаев предустановленных профилей групп доступа оказывается недостаточно для осуществления требуемой настройки прав доступа пользователей. В таких случаях администратор имеет возможность добавить новые или изменить предустановленные профили групп доступа.

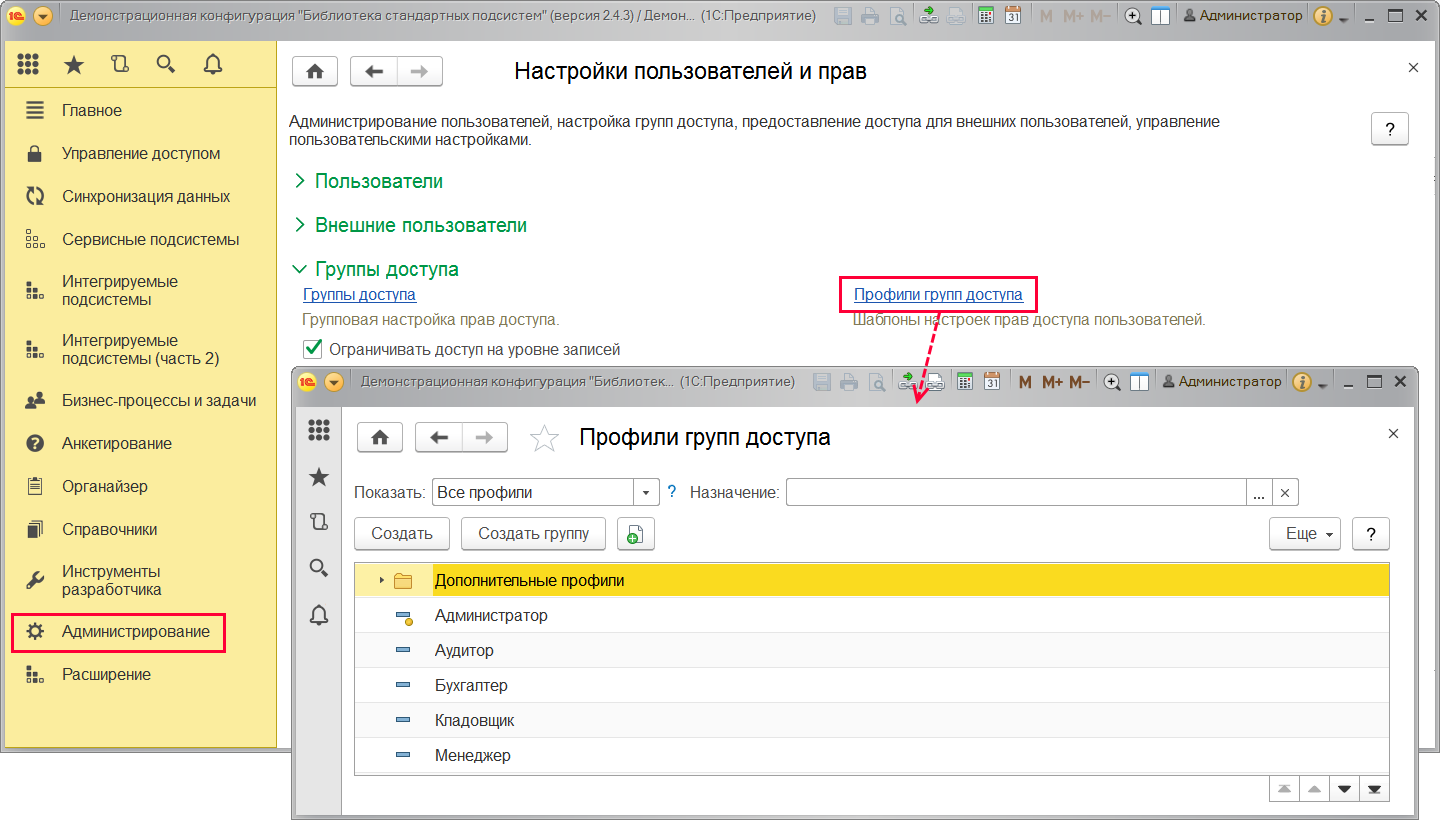
**Для обычного режима настройки прав доступа:**

Профиль групп доступа объединяет в себе, как правило, несколько ролей, а также содержит описание видов доступа, в разрезе которых администратор может настраивать права с помощью групп доступа. Таким образом, профиль представляет собой определенный шаблон, в соответствии с которым администратор ведет группы доступа. Для просмотра профиля доступа в карточке пользователей нажмите кнопку https://its.1c.ru/db/content/bsp301doc/src/_img/a8ac365292f91872c91b58b5276d597d/image2680.png?_=1542292879.



С одним профилем может быть связана одна или несколько групп доступа. Например, на базе профиля **Бухгалтер** могут быть настроены группы доступа **Бухгалтеры центрального офиса** и **Бухгалтеры филиала в Н-ске**, которые отличаются друг от друга разрешенными организациями: **Центральный офис** и **Филиал в Н-ске**.

Список Профили групп доступа можно открыть с помощью соответствующей ссылки в разделе **Администрирование** – Настройка пользователей и прав – Группы доступа.



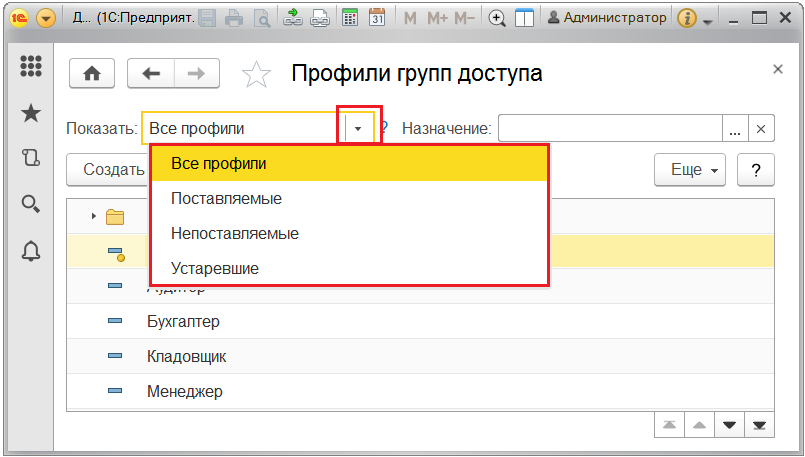
С помощью поля Показать в списке можно отобрать профили групп доступа:

■ Все профили;

■ Поставляемые;

■ Непоставляемые;

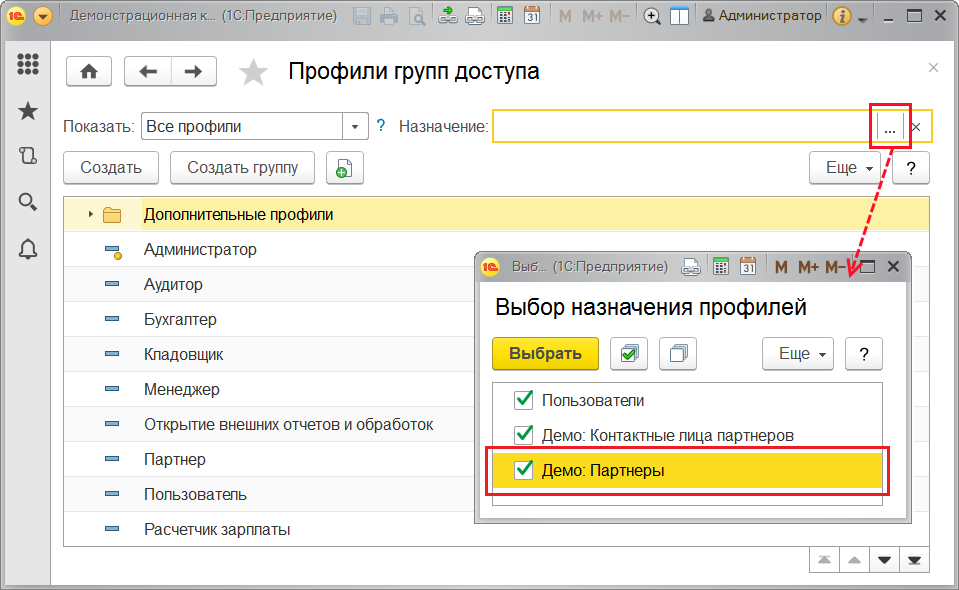
■ Устаревшие.



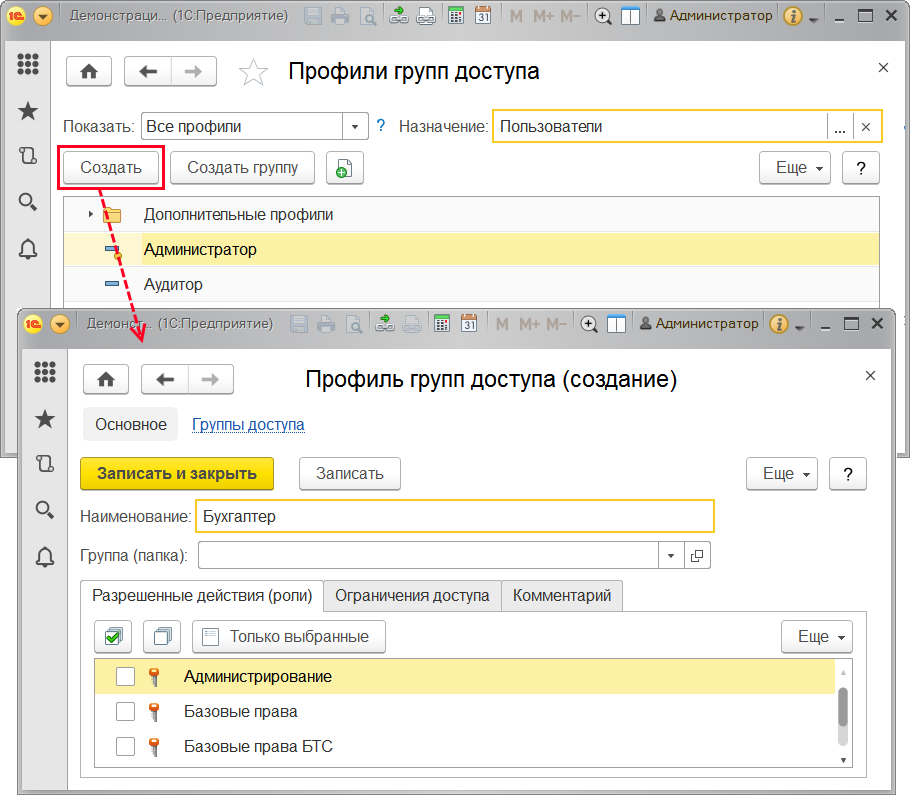
Можно отобрать профили групп доступа также по полю Назначение.

С помощью кнопки https://its.1c.ru/db/content/bsp301doc/src/_img/a8ac365292f91872c91b58b5276d597d/image1856.png?_=1542292879 выберите назначение профилей.

Укажите с помощью флажков, для кого предназначены профили групп доступа, например, Пользователи или **Демо: Партнеры**.



Для ввода нового профиля групп доступа воспользуйтесь кнопкой Создать.



При добавлении нового профиля сначала необходимо определить состав его ролей, исходя из потребностей целевой группы пользователей.

Роль определяет некоторую совокупность действий над объектами программы, которые может выполнять пользователь. Роли могут соответствовать как различным должностным обязанностям (или видам деятельности) пользователей программы, так и могут соотноситься с более мелкими функциями. Например, роль **Бухгалтер** предоставляет доступ к функциональному блоку, необходимому для выполнения должностных обязанностей бухгалтера, а для включения отдельной возможности просмотра файлов может быть дополнительно назначена роль **Чтение файлов**. Зачастую, роли либо разрешают просмотр, либо дают возможность редактирования тех или иных данных в программе.

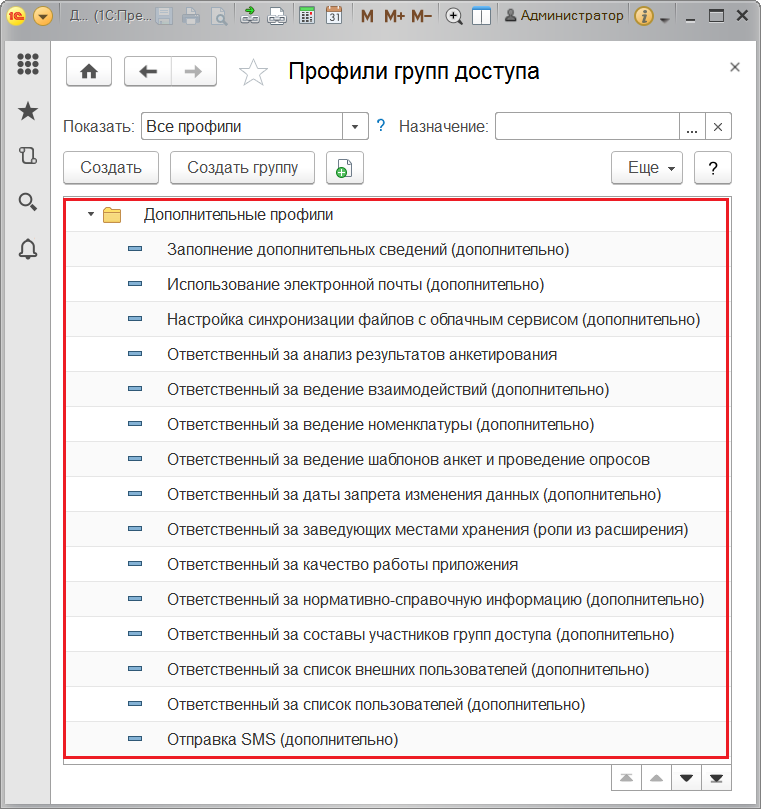
Каждому пользователю, посредством профилей и групп доступа, может быть назначена одна или несколько ролей, которые в совокупности образуют его персональные настройки прав доступа.

Как правило, различают основные и дополнительные профили.

Основной профиль описывает некоторую совокупность прав доступа, достаточную для выполнения в программе определенного участка работ, например, профиль **Бухгалтер** включает в себя все необходимые для работы бухгалтера роли.

С помощью дополнительных профилей пользователям могут быть выданы какие-либо вспомогательные права дополнительно к основному профилю.

Например, дополнительно к основным профилям **Бухгалтер** и **Кладовщик** предусмотрены профили **Использование электронной почты** и **Печать непроведенных документов**.



В основных профилях важно предусмотреть такой набор ролей, который с одной стороны, не будет давать избыточного (нежелательного) доступа к функциям и данным программы, а с другой – будет достаточным для работы пользователей в рамках их круга задач и обязанностей. В частности, в основном профиле следует предусмотреть ряд вспомогательных ролей, которые напрямую не связаны с основной деятельностью пользователей, но, тем не менее, необходимы для нее.

Например, для оператора по вводу документов помимо роли на добавление и изменение этих документов нужно также не забыть включить в профиль следующие роли:

■ роль для входа в программу с помощью тонкого, толстого или веб-клиента;

■ предопределенные роли Базовые права и **Базовые права УТ**;

■ роли для просмотра справочников, элементы которых требуется выбирать в полях документов;

■ роли для просмотра отчетов по движениям документов и т.п.

Например, в профиль **Аудитор** были включены основная роль **Чтение физических лиц**, разрешающая просмотр сведений о физических лицах, а также ряд вспомогательных ролей, обеспечивающих базовые возможности для работы в программе.

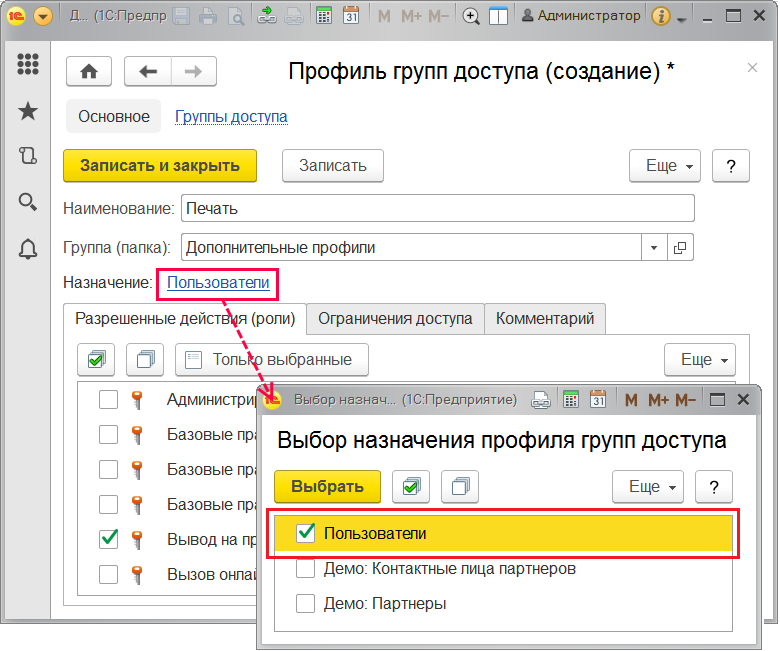
При вводе нового профиля групп доступа введите его Наименование.

Если профилей групп доступа много, то их можно группировать по разным признакам, например, можно выделить в отдельные группы основные и дополнительные профили групп доступа, также можно сгруппировать профили групп доступа и по другим признакам.

Профиль групп доступа можно включить в Группу (папку) с помощью кнопки https://its.1c.ru/db/content/bsp301doc/src/_img/a8ac365292f91872c91b58b5276d597d/image403.png?_=1542292879, выделите в списке нужную группу, нажмите кнопку Выбрать.

Если нужной группы нет в списке, с помощью кнопки Создать группу можно добавить в список новую группу (папку) профилей групп доступа.

 В поле Назначение перейдите по ссылке, с помощью флажков выберите, для кого предназначен профиль групп доступа, например, Пользователи, нажмите кнопку Выбрать. После этого ссылка принимает выбранное значение.



На вкладке Разрешенные действия (роли) с помощью флажков выберите одну или несколько ролей. Роли обычно выводятся в алфавитном порядке.

С помощью команды По подсистемам меню Еще можно увидеть роли, сгруппированные по подсистемам.

С помощью соответствующей кнопки можно вывести в список Только выбранные роли.

Затем на вкладке Ограничения доступа необходимо принять решение по поводу состава видов доступа, которые должны быть определены в профиле. Под видом доступа подразумевается некоторое правило, по которому «разрешается» доступ к данным программы. С их помощью можно более точно настраивать границы области данных, с которой разрешено работать участникам тех или иных групп доступа. В простейшем случае, если в профиль не включено ни одного вида доступа, то права доступа к данным определяются только ролями. Например, в случае если профиль включает в себя роль для чтения документов **Демо:** **Поступление товаров**, то участники групп доступа получают возможность просмотра всех документов. Но если в дополнение к этой роли в профиль добавить вид доступа **Демо:** **Организации**, то появляется возможность разрешать пользователям работу с документами только по конкретным организациям; или наоборот, скрывать от них документы некоторых организаций. Таким образом, если список ролей в профиле отвечает на вопрос, «что должно быть доступно, а что – нет» (какие функции и данные программы), то виды доступа уточняют, как именно они должны быть доступны (в разрезе каких разрешенных и запрещенных значений). Состав видов доступа в профиле рекомендуется определять, исходя из соображений гибкости настройки прав доступа.

Для каждого вида доступа, заданного в профиле, можно указать один из четырех вариантов настройки:

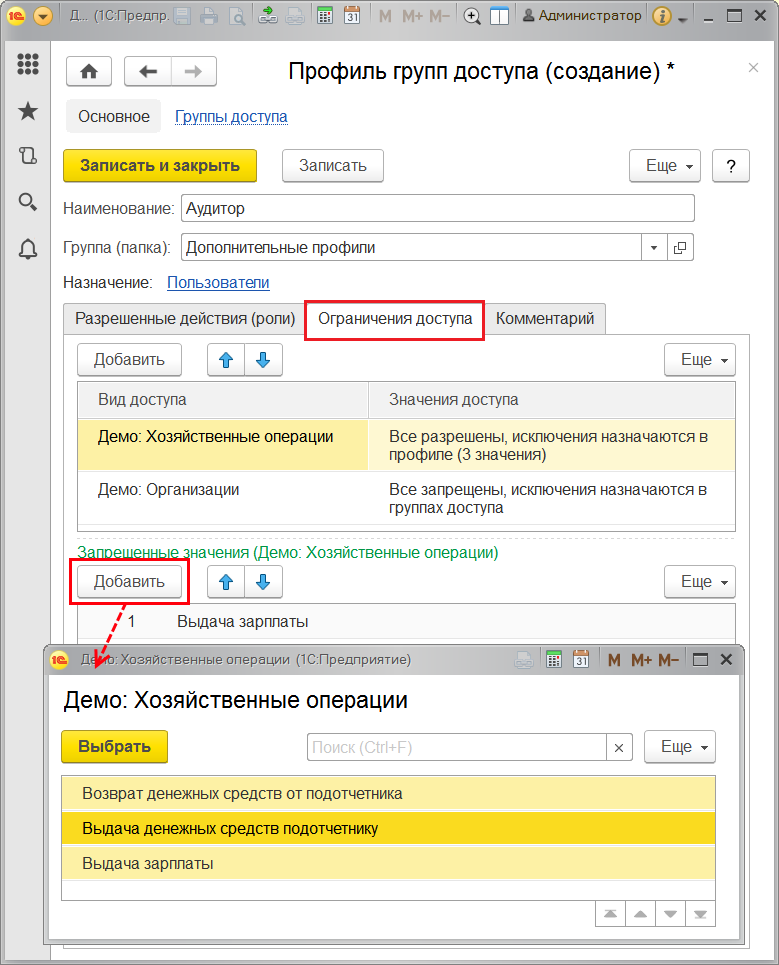
■ Все запрещены, исключения назначаются в группах доступа – применяется в тех случаях, когда по умолчанию доступ ко всем данным должен быть закрыт, но для отдельных объектов в группах доступа могут быть настроены разрешения;

■ Все разрешены, исключения назначаются в группах доступа – аналогично предыдущему варианту, но по умолчанию все данные разрешены, а для отдельных объектов в группах доступа могут быть установлены исключения – запрет;

■ Все запрещены, исключения назначаются в профиле – используется тогда, когда в группах доступа не предполагается предоставлять возможность настройки для вида доступа; т.е. вся настройка должна быть выполнена непосредственно в самом профиле и не может быть изменена в группах доступа. Такие виды доступа скрыты в группах доступа;

■ Все разрешены, исключения назначаются в профиле – аналогично предыдущему варианту.

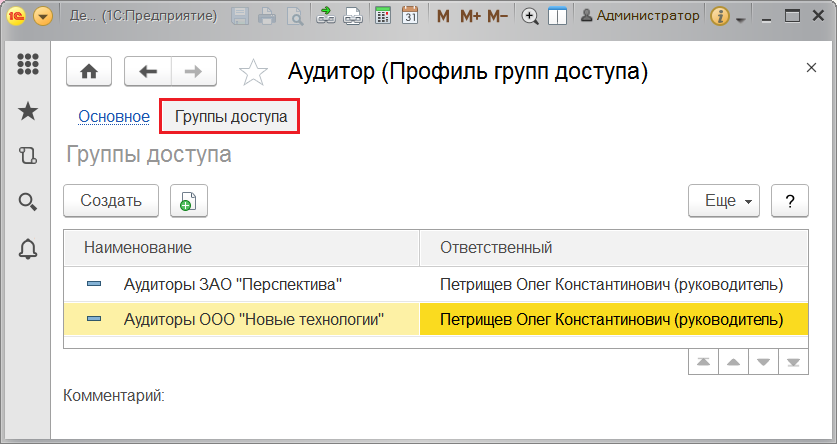
В примере на рисунке в профиль **Аудитор** были включены виды доступа **Демо:** **Организации** и **Демо: Хозяйственные операции**. При этом аудиторам запрещено работать с данными, которые относятся к хозяйственной операции **Выдача зарплаты**, а состав организаций, в разрезе которых аудиторы получают доступ к остальным данным, предполагается настраивать в группах доступа.



Если данная возможность в программе отключена, то вид доступа будет неактивен и в нижней части окна программа выводит об этом сообщение.

Для быстрого перехода к списку групп доступа, созданных на базе данного профиля, можно перейти по ссылке Группы доступа на панели навигации.

В данном списке с помощью кнопки Создать можно добавить новые группы доступа.



**Для упрощенного режима настройки прав доступа:**

Необходимо переработать раздел выше, исключив все упоминания о «группах доступа», имея в виду, что в этом режиме работы профили назначаются пользователям непосредственно, без использования групп доступа.

Профиль пользователей объединяет в себе, как правило, несколько ролей. Состав ролей следует подбирать, исходя из потребностей целевой группы пользователей. Как правило, различают основные и дополнительные профили. Основной профиль описывает некоторую совокупность прав доступа, достаточную для выполнения в программе определенного участка работ. С помощью дополнительных профилей пользователям могут быть выданы какие-либо вспомогательные права, дополнительно к основным. Например, дополнительно к основным профилям **Бухгалтер** и **Кладовщик** предусмотрены профили **Ведение переписки с контрагентами** и **Печать непроведенных документов**. В основных профилях важно предусмотреть такой набор ролей, который с одной стороны, не будет давать избыточного (нежелательного) доступа к функциям и данным программы, а с другой – будет достаточным для работы пользователей в рамках их круга задач и обязанностей. В частности, в основном профиле следует предусмотреть ряд вспомогательных ролей, которые напрямую не связаны с основной деятельностью пользователей, но, тем не менее, необходимы для нее.

Например, для оператора по вводу документов, помимо роли на добавление и изменение этих документов нужно также не забыть включить в профиль следующие роли:

■ роль для входа в систему с помощью тонкого, толстого или веб-клиента;

■ предопределенную роль **Базовые права**;

■ роли для просмотра справочников, элементы которых требуется выбирать в полях документов;

■ роли для просмотра отчетов по движениям документов и т.п.

**Состав профилей групп доступа**

**Для упрощенного режима настройки прав доступа этот раздел рекомендуется назвать «Состав профилей пользователей».**

Для настройки прав доступа пользователей в распоряжении администратора имеются следующие профили:

| Профиль | Краткое описание |
| --- | --- |
| **Основные профили** | |
| Администратор | Настройка прав доступа пользователей и администрирование программы. Включает в себя роль **Полные права**, которая предоставляет неограниченный доступ ко всем данным. |
| Аудитор | Включает в себя набор функций, необходимых для работы аудитора (чтение данных по бухгалтерии). |
| Бухгалтер | Включает в себя набор функций, необходимых для работы бухгалтера (кассовые документы, добавление персональных данных физических лиц). |
| Кладовщик | Включает набор функций, необходимых для работы кладовщика (кроме этого, доступно ведение дополнительных сведений, редактирования проектов и их присоединенных файлов). Работа со складскими документами, просмотр документов покупателей. |
| Менеджер | Контрольные функции (добавление и изменение проектов, добавление и изменение опросов, добавление и изменение шаблонов анкет). |
| Партнер | Назначается внешним пользователям для проведения анкетирования, а также работы со счетами. |
| Пользователь | Назначается всем пользователям программы, содержит базовые функции для работы в программе. |
| Расчетчик зарплаты | Содержит все функции, необходимые для добавления и изменения зарплаты. |
| Руководитель | Выполнение контрольных функций, контроль выполнения бизнес-процессов. |
| **Дополнительные профили** | |
| Заполнение дополнительных сведений (дополнительно) | Предназначен для ведения дополнительных сведений. |
| Использование электронной почты (дополнительно) | Использование электронной почты, доступ к учетным записям электронной почты запрещен и исключения назначаются в группах доступа. |
| Настройка синхронизации файлов с облачным сервисом (дополнительно) | Дополнительно назначается тем пользователям, которым должна быть доступна настройка синхронизации файлов с облачными сервисами. |
| Ответственный за анализ результатов анкетирования | Предназначен для работы с анкетированием и анализа его результатов. Работа с респондентами. |
| Ответственный за ведение взаимодействий (дополнительно) | Набор функций, необходимых для ведения взаимодействий (добавление и изменение взаимодействий, использование учетных записей электронной почты). |
| Ответственный за ведение номенклатуры (дополнительно) | Добавление и изменение номенклатуры. |
| Ответственный за ведение шаблонов анкет и проведение опросов | Предназначен для ведения шаблонов анкет, проведения опросов, работы с респондентами. |
| Ответственный за даты запрета изменения данных (дополнительно) | Дополнительно назначается тем пользователям, которым должна быть доступна возможность работы с датами запрета изменения данных (см. раздел документации Даты запрета изменения). |
| Ответственный за качество работы приложения | Предназначен для настройки и оценки производительности программы. |
| Ответственный за нормативно-справочную информацию (дополнительно) | Набор функций, необходимых для ведения всей нормативно-справочной информации в программе, ведение и обновление классификаторов. |
| Ответственный за составы участников групп доступа (дополнительно) | Изменение участников групп доступа. |
| Ответственный за список внешних пользователей (дополнительно) | Добавление и изменение внешних пользователей, настройка свойств пользователей информационной базы (без разрешения входа). |
| Ответственный за список пользователей (дополнительно) | Добавление и изменение пользователей, настройка свойств пользователей информационной базы (без разрешения входа). |
| Отправка SMS (дополнительно) | Предназначен для отправки SMS. |
| Печать непроведенных документов (дополнительно) | Содержит роль **Демо: Печать непроведенных документов**, позволяет выводить на печать непроведенные документы. Обычно это сделать невозможно. |
| Просмотр версий объектов | Предназначен для работы с хранением версий объектов. |
| Просмотр согласий на обработку персональных данных (дополнительно) | Просмотр согласий на обработку персональных данных. |
| Работа с папками файлов (дополнительно) | Работа с папками файлов. |
| Редактирование макетов печатных форм | Предназначен для работы с макетами печатных форм. |
| Редактирование согласий на обработку персональных данных (дополнительно) | Добавление и изменение согласий на обработку персональных данных. |
| Синхронизация данных с другими программами | Выполнение синхронизации данных, чтение информации о версиях объектов. |

**Роли для настройки прав доступа**

**Этот раздел содержит описание ролей, которые могут быть включены в профили групп доступа.**

Для настройки прав доступа могут быть назначены следующие роли:

|  |  |
| --- | --- |
| Роль | Краткое описание |
| Изменение участников групп доступа | Изменение состава участников групп доступа, в которых пользователь назначен ответственным. |
| Полные права | Неограниченный доступ ко всем данным, настройка прав доступа пользователей, администрирование информационной базы. |