Содержание

Типы лицензий 4
Роли безопасности 4
«Я руководитель, но не могу делегировать задачи!» 4
Отчёты по правам безопасности 4
Принципы работы 4
Системные роли и "проектные" роли 5
Как работает сочетание прав доступа 5

О правах доступа в Advanta

Возможности пользователя в системе регулируются:

- лицензией его учётной записи;
- системной ролью;
- «проектной ролью» (роль проекта/дискуссии/согласования).

	Лицензия	**Системная роль**	**"Проектная" роль**
Что регулирует	Доступ к отдельным разделам системы (в т.ч. Администрирование) Возможность делегировать объекты	**Работают в одной плоскости**: регулируют возможности пользователя в рамках работы с объектами, отчётами, дискуссиями и согласованиями. *Например, дают или отнимают право на изменения в проекте.*	
		Доступ **ко всем объектам системы** и диапазон возможностей по работе с ними	Диапазон возможностей по работе **с теми объектами, которые делегированы** пользователю
Как назначается пользователю	Карточка пользователя → поле «Лицензия»	Карточка пользователя → «Системная роль» Или/и через настройку групп[1)] и включение пользователя в группу	Пользователю делегируется объект или его приглашают участником, или его добавляет администратор, или пользователь создаёт объект. ⇒ Получает права в рамках этого объекта согласно той роли, которую он в нем играет.
Где настраивается	Диапазон возможностей лицензий и их набор **не настраивается**. Администратор может только выбрать тип лицензии по умолчанию для новых пользователей.	**Администрирование → Управление безопасностью → Безопасность → клик по нужной роли → Изменить**	
Где создаётся новая		Администрирование → Управление безопасностью → Безопасность → портлет «**Системные роли**» → Создать новую роль. См. подробно здесь.	Администрирование → Управление безопасностью → Безопасность → портлет «**Роли проекта**» → Создать новую роль. Можно добавлять только Роли проекта. Роли дискуссий и Роли согласований добавлять нельзя.

> У пользователя может не быть никакой системной роли, и в этом нет проблемы. Пользователь может получать необходимый для работы доступ через делегированные ему проекты и задачи. Т.е. через «проектные» роли.

Лицензия регулирует другие функциональные возможности пользователя, которые с объектами не связаны (кроме возможности делегировать).

Типы лицензий

Роли безопасности

Все настройки безопасности в системе находятся тут:

Администрирование → Управление безопасностью → Безопасность.

> См. описание всего перечня прав.

Чтобы увидеть перечень того, что разрешено или запрещено:

1. клик на название роли;
2. в блоке «Права» развернуть разделы – отобразятся все текущие разрешения.

Чтобы изменить настройки роли:

1. клик на название роли;
2. Изменить;
3. поменять чек-боксы;
4. сохранить изменения.

> **«Я руководитель, но не могу делегировать задачи!»**
>
> 1. Проверить, что у пользователя лицензия «Руководитель» или «Директор» (в карточке пользователя → Изменить).
> 2. Проверить, что у него в системной/проектной роли в блоке «Операции с объектами (директориями, проектами и задачами)» разрешено:
>   - Делегирование руководителя
>   - Делегирование исполнителя

> **Отчёты по правам безопасности**
>
> Чтобы посмотреть, что получается в итоге:
>
> - отчёт по правам пользователя;
> - отчёт по правам объекта системы.

Принципы работы

- Иерархичность – все права, полученные в вышестоящем объекте, распространяются сверху вниз по дереву иерархии.

- Взаимодействие прав по принципу **И**[2)].

Системные роли и "проектные" роли

	Системная роль	Роль проекта	Роль дискуссии	Роль согласования
Распространяется на все объекты системы	да[3)]	нет[4)]		
Можно создавать свои роли	да	да	нет	
Как назначается пользователю	Через настройки пользователя (напрямую или через группы).	Через назначение пользователю роли в проекте/дискуссии/согласовании. *Делегирование объекта пользователю как руководителю или исполнителю, приглашение его участником или согласующим – это и есть назначение ему соответствующей проектной роли.*		

Пользователь может являться участником **сразу нескольких ролей безопасности**, как системных, так и проектных.
Итоговый набор разрешений формируется совокупностью разрешений в этих ролях.

Чтобы увидеть полный актуальный список прав, зайдите в Администрирование → Управление безопасностью → Безопасность → клик на любую системную роль → Изменить.

Описание этого списка.

Как работает сочетание прав доступа

На каждое право могут быть заданы следующие разрешения и ограничения:

☐	Не определено **Запрет**, если не указано ☑ в другой Системной роли или Роли проекта *Это значение выбрано по умолчанию для всех прав в создаваемых ролях безопасности.*
☑	Разрешено
☒	Запрещено **Отъём права**, даже если другой ролью это право было предоставлено ☑

Мы не рекомендуем устанавливать ☒ на Ролях проекта/дискуссий/согласований, чтобы не лишить пользователя нужной для работы функциональности.
Выбирайте ☐, чтобы соблюсти гибкость настроек.
☒ – это инструмент жёсткого, однозначного запрета.

Часто может быть ситуация, когда одна роль открывает доступ к объектам и функциональности, а другая, наоборот, ограничивает их.

В случае, если у одного и того же пользователя назначены несколько ролей по одному и тому же объекту, и они противоречат друг другу (или не определяют доступ – ☐), правила доступа работают так:

- ☐ & ☐ → ☒
- ☐ & ☑ → ☑
- ☐ & ☒ → ☒
- ☒ & ☑ → ☒

> Например, у пользователя системная роль, которая даёт доступ редактирования всех проектов системы – ☑.
> В Проекте_1 этот пользователь – руководитель, где не определены ☐ права на изменение проекта ⇒ ☐ & ☑ → ☑
> А в Проекте_2 он же – исполнитель, где запрещены ☒ изменения на Проект. ⇒ ☒ & ☑ → ☒

1)

группе присваивается системная(ые) роль(и)

2)

&, конъюнкция

3)

Если общесистемная роль разрешает пользователю создание дочерних проектов и задач, то он сможет создавать их во всех ветках дерева проектов, в которые имеет доступ.

4)

Действуют на права пользователя только тогда, когда он автоматически или вручную становится участником роли в определенных проектах, дискуссиях или согласованиях.