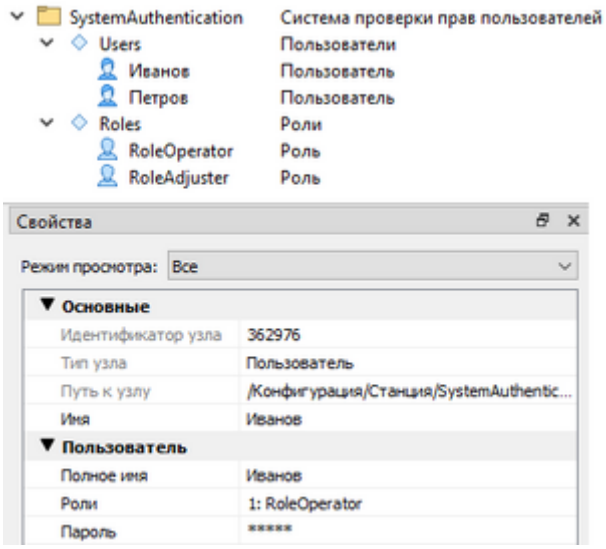
Система проверки прав пользователей AgavaSCADA/AgavaPLC

Редакция от 19.10.2026 · docs.kb-agava.ru

Содержание

1 Назначение 2
2 Состав системы 2
3 Порядок настройки 3
4 Свойства системы 3
4.1 Пользователь по умолчанию 4
5 Пользователи и роли 4
5.1 Свойства пользователя 4
5.2 Свойства роли 5
6 Виды привилегий 5
7 Окно «Привилегии» 6
7.1 Просмотр 6
7.2 Добавление правила 6
7.3 Удаление и замена правила 6
8 Наследование и порядок ролей 7
8.1 Наследование по дереву 7
8.2 Несколько ролей 7
9 Вход, выход и смена пароля 8
9.1 Действие входа 8
9.2 Работа с диалогом 8
9.3 Выход 8
9.4 Смена пароля 9
10 Отказ в доступе и поведение интерфейса 9
11 Пример разграничения доступа 10
12 Проверка и диагностика 11
12.1 Проверка конфигурации 11
12.2 Проверка при выполнении 11
12.3 Диагностические ситуации 11



Система проверки прав пользователей

1 Назначение

Система проверки прав пользователей предназначена для разграничения доступа к значениям и окнам прикладного проекта. Она позволяет определить, какие операции доступны наблюдателю, оператору, наладчику и другим категориям пользователей.

В дереве проекта используется узел **«Система проверки прав пользователей»**, размещаемый внутри станции. В системе создаются пользователи и роли. Ролям назначаются привилегии на узлы проекта, а пользователям — одна или несколько ролей.

При входе выбирается текущий пользователь. Его роли определяют результат последующих проверок доступа. Настройки относятся к выполняемому прикладному проекту; они не создают учётные записи операционной системы и не задают права редактирования проекта в среде разработки.

API системы описано на странице `Класс SystemAuthentication`.

2 Состав системы

Элемент	Назначение
Система проверки прав пользователей	Настройка пользователя по умолчанию и представление текущего пользователя.
Роли	Группа для размещения узлов «Роль».
Роль	Набор разрешений и запретов на операции с узлами проекта.
Пользователи	Группа для размещения узлов «Пользователь».
Пользователь	Учётная запись проекта с паролем и списком ролей.
Привилегия	Разрешение или запрет определённой операции для узла и его потомков.

Типовая структура имеет следующий вид:

```
Станция проекта
└── Система проверки прав пользователей
```

```
    ├── Роли
    │   ├── Наблюдение
    │   ├── Оперативное управление
    │   └── Наладка
    └── Пользователи
        ├── Наблюдатель
        ├── Оператор
        └── Наладчик
```

Привилегии задаются для ролей. При выборе пользователя в редакторе можно просматривать его итоговые права и добавлять правила в одну из назначенных ему ролей. Отдельный независимый набор персональных правил при этом не создаётся.

Названия ролей и пользователей выбираются разработчиком. Само наименование **«Администратор»** или **«Наладчик»** не предоставляет дополнительных прав: они определяются назначенными правилами.

3 Порядок настройки

Для настройки разграничения доступа необходимо:

1. Выбрать станцию и открыть её контекстное меню с помощью клика правой кнопки мыши по имени станции.
2. Выбрать команду **«Добавить узел» → «Система» → «Система проверки прав пользователей»**.
3. Добавить в систему группу **«Роли»**, затем создать необходимые узлы **«Роль»**.
4. Добавить группу **«Пользователи»** и создать пользователей проекта.
5. Для каждого пользователя задать имя, полное имя, пароль и список ролей.
6. В свойствах системы указать **«Пользователь по умолчанию»**.
7. Вызвать команду **«Вид» → «Открыть привилегии»** и назначить ролям права на значения и окна.
8. Предусмотреть в интерфейсе проекта команды входа, выхода и, при необходимости, смены пароля.
9. Выполнить проверку проекта, сохранить изменения и загрузить проект на целевое устройство.
10. Проверить доступ для пользователя по умолчанию и каждой рабочей категории пользователей.

Для каждого действия необходимо определить как разрешённый сценарий, так и результат отказа. Например, оператор должен иметь возможность открыть рабочую мнемосхему и изменить рабочую уставку, а наблюдатель — только просматривать её значение.

4 Свойства системы

Свойства расположены в группе **«Система»**.

Свойство	Идентификатор	Назначение
Пользователь по умолчанию	`UserDefault`	Ссылка на пользователя, выбираемого при запуске системы и при штатном выходе.
Пользователь авторизованный	`UserCurrent`	Текущий пользователь; только чтение.

Имя авторизованного пользователя	`UserCurrentName`	Имя узла текущего пользователя; только чтение.
Полное имя авторизованного пользователя	`UserCurrentDesc`	Полное имя текущего пользователя; только чтение.
Действие при отказе в доступе	`AccessDeniedAction`	Выбор предусмотренной реакции на отказ. Ограничение текущей версии описано в разделе 10.

Имя и полное имя текущего пользователя могут использоваться в информационной области мнемосхемы. Это позволяет оператору проверить, под какой учётной записью выполняется работа.

4.1 Пользователь по умолчанию

При запуске система автоматически выбирает пользователя, указанного в свойстве **«Пользователь по умолчанию»**. Ввод его пароля не требуется, даже если пароль задан в свойствах учётной записи.

Штатный выход также возвращает систему к этому пользователю без запроса пароля. Поэтому его роли должны соответствовать доступу, допустимому без индивидуального входа, например просмотру основной мнемосхемы и показаний.

Ссылка на корректного пользователя по умолчанию необходима для прохождения проверки конфигурации. При её отсутствии или неверном типе узла выдаётся ошибка.

5 Пользователи и роли

5.1 Свойства пользователя

Свойство	Идентификатор	Назначение
Имя	`Name`	Имя узла пользователя в проекте.
Полное имя	`Fullname`	Представление пользователя в диалогах и информационных полях.
Роли	`Roles`	Список назначенных ролей. Порядок элементов влияет на разрешение конфликтов.
Пароль	`Password`	Пароль для входа с проверкой подлинности.
Не показывать в списке	`HideInUsersList`	Исключение пользователя из общего списка выбора в стандартных диалогах. Начальное значение — выключено.
Запретить изменение пароля	`DisablePasswordChange`	Запрет изменения пароля через стандартное действие смены пароля. Начальное значение — выключено.

В общих списках выбора отображается полное имя. Для однозначного выбора следует задавать различимые полные имена, особенно если в проекте много пользователей.

Флаг **«Не показывать в списке»** управляет отображением в общем списке. Он не удаляет учётную запись и не исключает её использование как пользователя по умолчанию или как заранее заданного пользователя действия входа.

Пользователю без ролей не предоставляются разрешения на проверяемые операции. При проверке проекта для такого пользователя выдаётся замечание **«Не заданы роли»**.

5.2 Свойства роли

Для роли задаются имя и описание. Свойство **«Привилегии»** (`Privileges`) представляет назначенные правила и доступно только для чтения в обычной панели свойств. Изменение правил выполняется в окне **«Привилегии»**.

Роль может назначаться нескольким пользователям. Изменение её правил влияет на всех пользователей, у которых эта роль участвует в определении доступа.

Пустой набор привилегий роли считается ошибкой конфигурации. Если роль больше не используется, следует удалить её либо завершить её настройку.

6 Виды привилегий

В текущей системе предусмотрены четыре вида привилегий:

Привилегия	Назначение
Чтение значения	Получение значения узла при обращении от имени текущего пользователя.
Запись значения	Изменение значения узла при обращении от имени текущего пользователя.
Открытие окна	Открытие окна штатным действием интерфейса с проверкой доступа.
Закрытие окна	Закрытие окна штатным действием интерфейса с проверкой доступа.

Доступный список определяется выбранным узлом. Для окон и фреймов предлагаются привилегии открытия и закрытия, для узлов со значениями — соответствующие операции над значением.

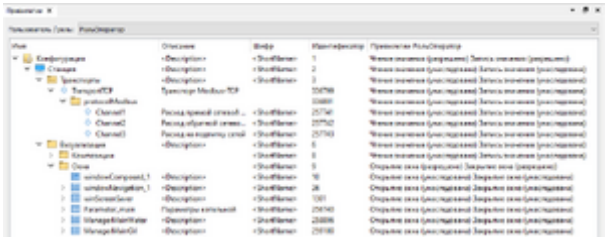
Чтение и запись настраиваются независимо. Разрешение записи не следует использовать вместо разрешения чтения, а разрешение открытия окна не предоставляет автоматически доступ ко всем значениям, показанным на нём.

Если в проекте есть система проверки прав, проверяемая операция разрешается при непосредственном или унаследованном разрешении. Явный запрет и отсутствие применимого разрешения приводят к отказу. Отдельного переключателя этой политики в обычной панели свойств текущей версии нет.

Привилегии относятся к операциям, выполняемым с проверкой текущего пользователя. Автоматическое обновление технологических значений, выполнение программ и обмен с оборудованием могут выполняться как системные операции. Наличие системы прав само по себе не запрещает такие операции.

Если система проверки прав отсутствует, описанные ограничения чтения, записи и штатных действий открытия и закрытия окон не применяются. Поэтому отсутствие пользователя и отсутствие самой системы имеют различный результат.

7 Окно «Привилегии»



Окно привилегий

7.1 Просмотр

Окно открывается командой **«Вид» → «Открыть привилегии»**. В поле **«Пользователь / роль»** выбирается роль для настройки либо пользователь для просмотра результата назначения его ролей.

В дереве проекта отображается состояние доступных привилегий:

Состояние	Значение
Разрешено	На узле задано непосредственное разрешение.
Запрещено	На узле задан непосредственный запрет.
Разрешено, унаследована	Разрешение получено от родительского узла.
Запрещено, унаследована	Запрет получен от родительского узла.
Правило не отображается	Для выбранной привилегии применимое правило не найдено.

Отсутствие записи не является непосредственным запретом в роли: при нескольких ролях поиск может продолжиться в следующей роли. Если ни одна роль не предоставляет применимого правила, проверяемая операция не разрешается.

7.2 Добавление правила

1. В поле «Пользователь / роль» выбрать настраиваемую роль либо пользователя с назначенными ролями.
2. В дереве выбрать узел, к которому должно относиться правило.
3. Открыть контекстное меню и выбрать **«Добавить привилегию…»**.
4. Указать **«Тип привилегии»**, **«Режим»** — «Разрешить» или «Запретить» — и **«Роль»**.
5. Подтвердить выбор кнопкой **OK**.
6. Проверить правило на узле и результат наследования у его потомков.

При выборе пользователя правило добавляется в указанную роль этого пользователя. Если роль у него одна, выбор роли в диалоге недоступен.

Для одновременного назначения нескольким узлам допускается их множественное выделение при совместимых наборах доступных привилегий.

7.3 Удаление и замена правила

Для удаления непосредственной записи используется контекстное меню **«Удалить привилегию»**. В подменю указываются операция, режим и роль; перед удалением следует проверить все три признака.

Удаление разрешения не создаёт запрет. После удаления может начать действовать правило родителя или другой роли. Унаследованное правило следует изменять на узле, где оно назначено, либо переопределять непосредственным правилом на нужном потомке.

Для замены разрешения запретом или обратной замены рекомендуется сначала удалить прежнюю непосредственную запись этой роли для данной операции, затем добавить новую. Не следует оставлять противоречащие непосредственные правила одной привилегии на одном узле.

8 Наследование и порядок ролей

8.1 Наследование по дереву

Правило, назначенное родительскому узлу, распространяется на его потомков. В пределах одной роли правило более близкого узла имеет приоритет перед правилом более удалённого предка.

Например, роли оператора можно разрешить запись для группы технологических сигналов, а для отдельного калибровочного параметра этой же роли задать запрет записи. Обычные параметры наследуют разрешение, калибровочный параметр получает непосредственный запрет.

Наследуются как разрешения, так и запреты. Непосредственное разрешение на потомке может переопределить запрет предка в той же роли; непосредственный запрет — разрешение предка.

8.2 Несколько ролей

При нескольких ролях используется **первое применимое правило в порядке списка «Роли» пользователя**. Результатом первой подходящей роли может быть как разрешение, так и запрет. Если правило в роли отсутствует, рассматривается следующая роль.

Правило первой роли	Правило следующей роли	Итог
Не найдено	Разрешение	Разрешено.
Не найдено	Запрет	Запрещено.
Разрешение	Запрет	Разрешено по первой роли.
Запрет	Разрешение	Запрещено по первой роли.
Не найдено	Не найдено	Разрешение отсутствует.

Это правило применяется и к унаследованным результатам. Например, унаследованный запрет первой роли может определять итог раньше непосредственного разрешения второй роли.

При настройке нескольких ролей следует избегать противоречий и проверять итоговые права именно для пользователя. Проверка одной роли отдельно не отражает результат всего списка ролей.

9 Вход, выход и смена пароля

9.1 Действие входа

В интерфейсе проекта используется **«Действие „Авторизация пользователя“»**. Обычно оно назначается кнопке входа.

Свойство действия	Идентификатор	Назначение
Пользователь	`User`	Заранее выбранная учётная запись. Если не задана, стандартный интерфейс открывает общий диалог выбора.
Запрашивать пароль	`RequestPassword`	При заданном пользователе включает проверку пароля через диалог. Начальное значение — выключено.

Поведение стандартного действия зависит от настроек:

Настройка	Результат
Пользователь не задан	Открывается общий диалог «Проверка подлинности» с выбором пользователя и вводом пароля.
Пользователь задан, запрос пароля включён	Открывается диалог для указанного пользователя; выбор другой учётной записи недоступен.
Пользователь задан, запрос пароля выключен	Выполняется вход указанного пользователя без проверки пароля.

Для индивидуального входа в защищённую учётную запись необходимо использовать диалог с проверкой пароля. Само наличие пароля в свойствах пользователя не изменяет режим действия с выключенным запросом.

9.2 Работа с диалогом

1. Нажать предусмотренную проектом кнопку входа.
2. В диалоге **«Проверка подлинности»** выбрать пользователя, если выбор доступен.
3. Ввести пароль и нажать **OK**.
4. После успешного входа проверить имя пользователя в информационной области интерфейса.

При неверном пароле отображается сообщение **«Неверный пароль»**, при отсутствующем пользователе — **«Пользователь не найден»**. Неудачная попытка не заменяет ранее выбранного текущего пользователя. Кнопка **«Отмена»** закрывает диалог без смены пользователя.

При успешном входе доступность виджетов пересчитывается. Однако уже открытое окно не следует считать автоматически закрываемым при переходе к пользователю с меньшими правами. Для такого сценария необходимо предусмотреть переход интерфейса к подходящему экрану.

9.3 Выход

В проекте следует предусмотреть отдельную команду выхода. Для прикладной функции доступна команда **`Logout()`**; она возвращает систему к пользователю по умолчанию и обновляет состояние интерфейса.

Если корректный пользователь по умолчанию отсутствует, штатный выход снимает текущего пользователя и очищает его информационные поля. Такая конфигурация требует исправления, поскольку проверка проекта предусматривает корректного пользователя по умолчанию.

Для переключения на пользователя по умолчанию также может использоваться действие авторизации с явно выбранной соответствующей учётной записью и выключенным запросом пароля.

9.4 Смена пароля

Для стандартного диалога используется **«Действие „Смена пароля пользователя“»**.

Свойство	Идентификатор	Назначение
Пользователь	`User`	Учётная запись для смены пароля, если не выбран текущий пользователь.
Текущий	`Current`	Использование текущего пользователя вместо заранее заданного.

Если пользователь не определён настройками действия, стандартный интерфейс предоставляет общий список доступных пользователей. Учётные записи с флагом **«Не показывать в списке»** исключаются из общего списка, а с флагом **«Запретить изменение пароля»** недоступны для смены пароля.

Для изменения необходимо:

1. Открыть диалог **«Смена пароля»**.
2. Проверить выбранного пользователя.
3. Ввести **«Старый пароль»**, **«Новый пароль»** и **«Новый пароль повторно»**.
4. Нажать **OK**.

Диалог проверяет старый пароль и совпадение двух новых значений. При ошибке выводится **«Неверный старый пароль»** или **«Новый пароль не совпадает»**.

Действие **«Смена пароля пользователя»** предназначено для изменения известного пароля с подтверждением старого. Отдельная операция административного сброса пароля в этом диалоге не предусмотрена.

10 Отказ в доступе и поведение интерфейса

Свойство системы **«Действие при отказе в доступе»** содержит варианты:

- **«Отобразить диалог аутентификации»**;
- **«Отобразить сообщение об ошибке»** — начальное значение;
- **«Ничего не делать»**.

В текущей реализации штатного открытия окна при отказе выводится сообщение **«Недостаточно прав для выполнения действия»**, после чего окно не открывается. Автоматический вызов диалога входа по первому варианту не выполняется; вариант «Ничего не делать» также не отменяет это сообщение в данном сценарии. Следует предусмотреть самостоятельную доступную кнопку входа.

Для ввода значения важно проверять права на узел, являющийся источником данных виджета. В поле ввода предусмотрено свойство **«Проверять права доступа»** (`CheckAccessRights`) в группе **«Проверка прав»**. При его включении допуск к вводу учитывает привилегию записи источника; начальное значение свойства — выключено.

Это свойство задаёт поведение поля ввода. Итоговая операция записи дополнительно зависит от назначения виджета, целевого узла и используемого действия. Доступность поля сама по себе не подтверждает разрешение любой связанной операции.

11 Пример разграничения доступа

Пусть проект содержит рабочую мнемосхему, технологические сигналы, рабочие уставки и калибровочный параметр.

1. Создать роль **«Наблюдение»**. Разрешить чтение технологических сигналов, открытие и закрытие рабочих окон.
2. Создать роль **«Оперативное управление»**. Разрешить запись рабочих уставок. Для калибровочного параметра не предоставлять разрешение либо задать явный запрет в пределах этой роли.
3. Создать роль **«Наладка»**. Разрешить предусмотренные наладочные операции, включая запись калибровочного параметра и доступ к наладочному окну.
4. Создать пользователя **«Наблюдатель»** с ролью «Наблюдение» и назначить его пользователем по умолчанию.
5. Пользователю **«Оператор»** назначить роли «Наблюдение» и «Оперативное управление».
6. Пользователю **«Наладчик»** назначить роли «Наблюдение» и «Наладка».
7. Проверить, что роль «Наблюдение» не содержит запретов, которые должны переопределяться последующими ролями. Отсутствие разрешения записи в этой роли позволяет продолжить поиск в следующей роли.
8. Настроить кнопку общего входа, команду выхода и информационное поле текущего пользователя.
9. Загрузить проект и проверить ожидаемый результат для каждой учётной записи.

Операция	Наблюдатель	Оператор	Наладчик
Просмотр рабочих показаний	Разрешён	Разрешён	Разрешён
Открытие рабочей мнемосхемы	Разрешено	Разрешено	Разрешено
Запись рабочей уставки	Не разрешена	Разрешена	По настройкам роли «Наладка»
Запись калибровочного параметра	Не разрешена	Не разрешена	Разрешена
Открытие наладочного окна	Не разрешено	Не разрешено	Разрешено

Пример предполагает, что привилегии назначены именно узлам, к которым обращаются виджеты и действия. Если элемент интерфейса записывает значение в другой узел, необходимо проверить права на фактическую цель записи.

12 Проверка и диагностика

12.1 Проверка конфигурации

Проверка проекта выявляет, в частности:

- отсутствующего или некорректного пользователя по умолчанию;
- пользователя без назначенных ролей;
- ссылку пользователя на несуществующую роль;
- роль без привилегий;
- привилегию, назначенную удалённому узлу.

После изменения структуры проекта следует повторно проверить ссылки правил и источники виджетов. Перемещение узла может изменить набор унаследованных прав.

12.2 Проверка при выполнении

1. Запустить проект и проверить выбор пользователя по умолчанию.
2. Проверить разрешённые операции просмотра и отказ в изменении защищённых значений.
3. Выполнить вход оператором, проверить чтение, запись и доступ к окнам.
4. Проверить заведомо неверный пароль: текущий пользователь должен остаться прежним.
5. Выполнить выход и проверить возврат к пользователю по умолчанию.
6. Проверить наследование и исключения на отдельных узлах.
7. Для пользователей с несколькими ролями проверить итоговый доступ с учётом их порядка.

12.3 Диагностические ситуации

Ситуация	Что следует проверить
Пользователь отсутствует в общем списке	Наличие узла и флаг «Не показывать в списке».
Вход выполняется без пароля	Назначение пользователя по умолчанию либо настройки действия «Пользователь» и «Запрашивать пароль».
После ошибки входа доступ остался прежним	Неудачная попытка не снимает ранее выбранного пользователя; проверить его имя.
Правило роли разрешает операцию, пользователь получает отказ	Роли пользователя, их порядок, правила предков и фактический целевой узел операции.
Запрет одной роли не действует	Наличие применимого разрешения в более ранней роли списка.
После удаления правила доступ изменился неожиданно	Унаследованное правило или следующую применимую роль.
Окно открывается, показания недоступны	Отдельные привилегии чтения источников, используемых на окне.
Поле ввода доступно, запись не выполняется	Права на фактическую цель записи и настройку «Проверять права доступа».
При отказе не открывается диалог входа	Ограничение текущей реакции на отказ; использовать отдельную кнопку входа.

Смена пароля недоступна	Флаг «Запретить изменение пароля» и пользователя, выбранного действием.
После выхода отображается другая учётная запись	Штатный возврат к пользователю по умолчанию.

Система формирует сообщения об успешном входе и отказах, включая неверный пароль или отсутствие пользователя. Для сохранения этих сообщений следует настроить систему журналирования с подходящим уровнем. Наличие системы проверки прав само по себе не создаёт долговременный журнал.