RLS: ограничение доступа к данным

При работе с информационной базой пользователи должны иметь возможность получить необходимую им информацию – справочники товаров и продукции, документы клиентов, цены и т.д. Однако каждый пользователь должен иметь доступ только к той информации, которая ему требуется для выполнения своих обязанностей, и не иметь доступа к информации, ответственным за которую он не является.

> *Например, менеджеру по продажам для работы не нужна возможность доступа к бухгалтерским проводкам.*

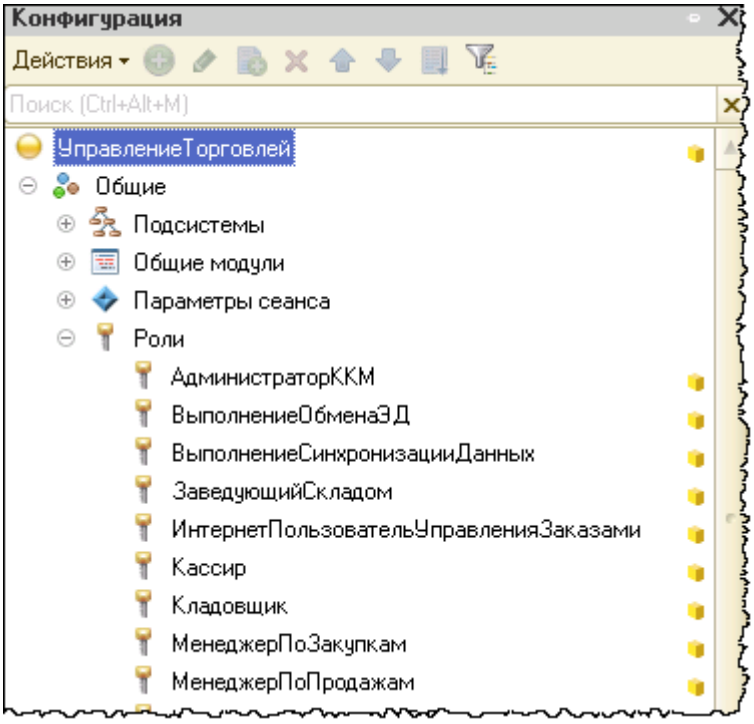
И дело тут не только в том, что он увидит финансовый результат деятельности организации, выплаченную другим сотрудникам зарплату или дивиденды учредителей. Нужно обеспечить, чтобы сотрудник без злого умысла, даже просто по случайности, не испортил данные, в которых он не разбирается и за которые не отвечает.

Платформа «1С:Предприятие 8» имеет средства для решения подобных задач.

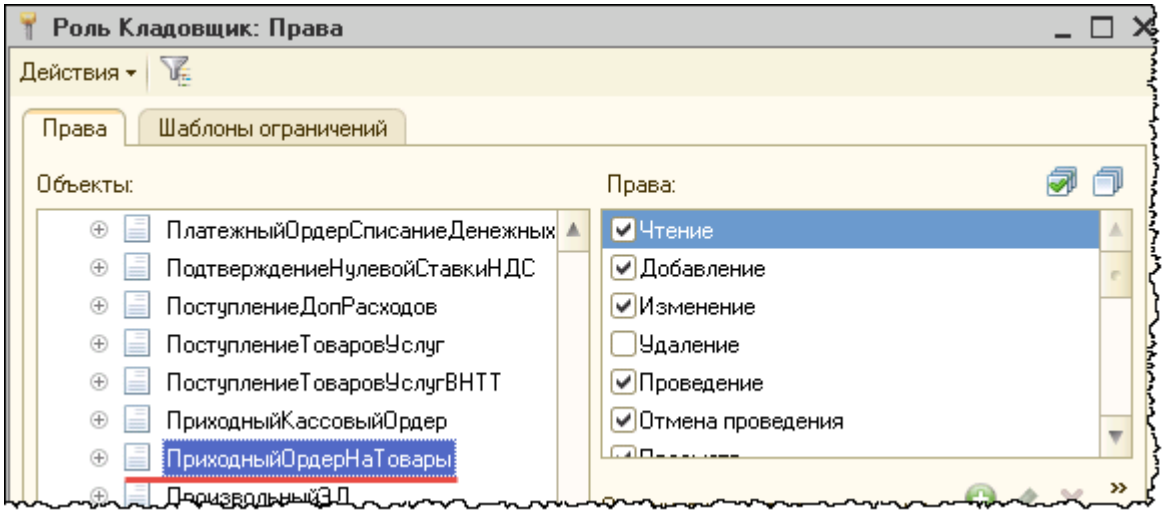
Роли

Для ограничения прав доступа в конфигурации существуют специальные объекты – **роли**. Роль соответствует конкретным должностным обязанностям, выполняемым задачам. Роли могут быть достаточно разнообразны – разрешено просматривать конкретный справочник, добавлять и изменять набор документов, разрешено просматривать и редактировать любой объект конфигурации и т.д.

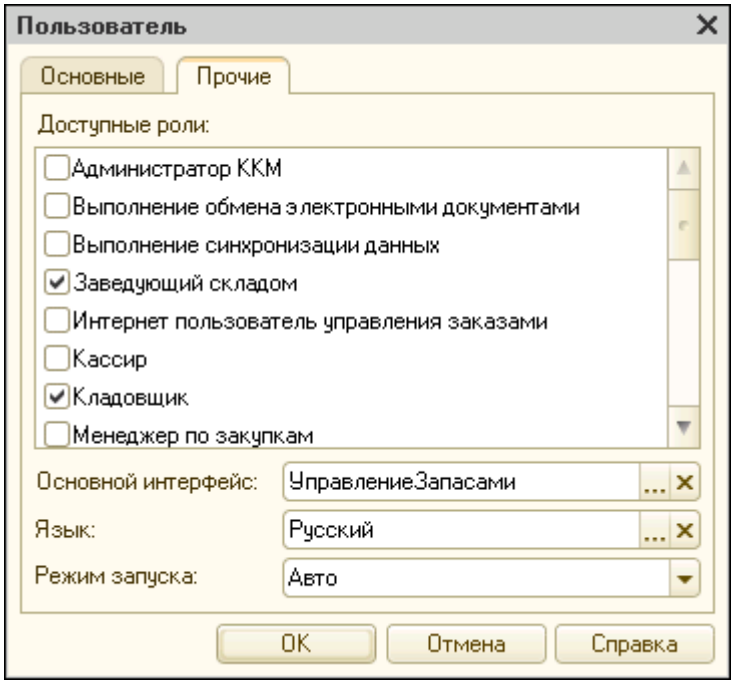
Например, в типовой конфигурации «Управление торговлей, ред. 10.3» список ролей выглядит так:



Роль в конфигурации определяет, какие действия в системе и над какими объектами может выполнять пользователь, которому назначена эта роль:



При создании пользователя в информационной базе администратор должен назначить ему требуемый набор ролей:



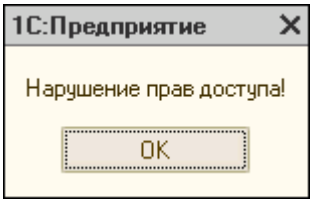
Права доступа

В платформе «1С:Предприятие 8» все доступные права доступа можно разделить на две большие группы – основные и интерактивные.

- Основные права доступа проверяются всегда, независимо от способа обращения к объектам информационной базы.
- Интерактивные проверяются только при выполнении интерактивных операций (например, просмотр или редактирование объекта в форме).

Проверку интерактивных прав доступа можно обойти. Для этого можно создать в конфигураторе собственную форму объекта и заменить стандартные команды собственными. Проверку основных (неинтерактивных) прав обойти нельзя. За это отвечают, например, такие права доступа: *Чтение*, *Изменение*, *Добавление*, *Удаление*.

Основные и интерактивные права связаны друг с другом. Если для объекта, данные которого представляются в форме, установлено право *Просмотр*, но не установлено право *Редактирование*, то в форме данный реквизит будет показан, однако редактирование будет недоступно. Если убрать право *Просмотр*, то при попытке открытия формы будет выдано предупреждение и форма не откроется:

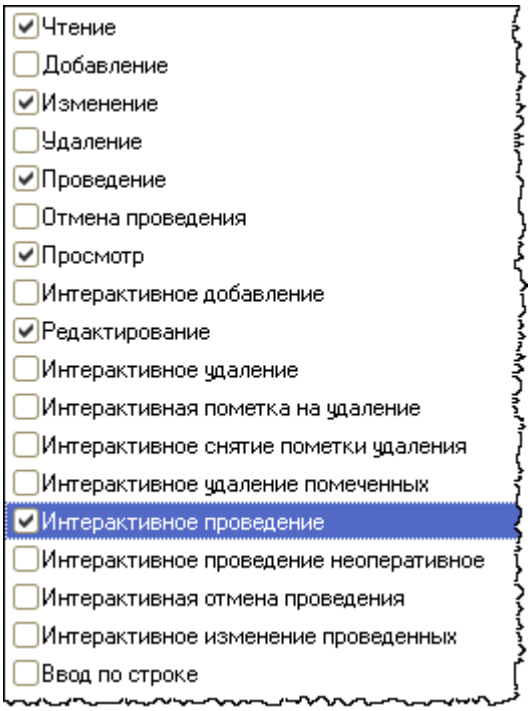


Интерактивные права напрямую зависят от их неинтерактивных аналогов. Право *Интерактивное проведение* зависит от права *Проведение*, так как если нет прав на проведение документа, то нет и возможности проводить объект интерактивно.

В конфигураторе при установке интерактивных прав аналогичные им неинтерактивные будут установлены автоматически, и, наоборот, при снятии неинтерактивных прав соответствующие им интерактивные права автоматически будут сброшены.

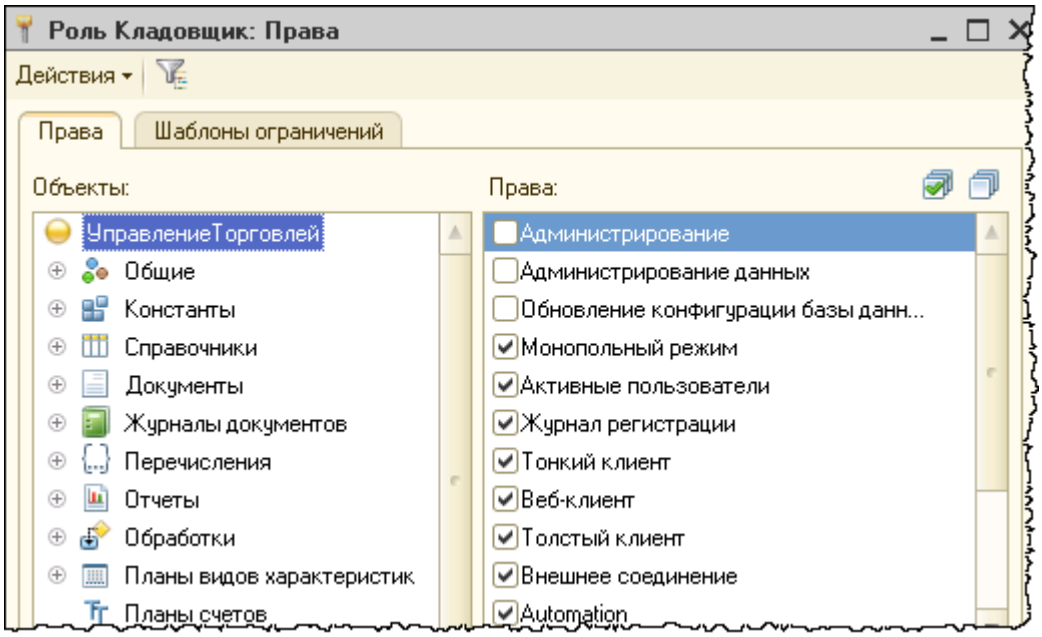
Допускается установка неинтерактивного права и сброс интерактивного, но не наоборот. Например, нельзя разрешить интерактивное право *Интерактивное проведение* и запретить неинтерактивное *Проведение*.

Цепочки зависимости прав доступа могут быть более сложными. При установке права *Интерактивное проведение* будут одновременно установлены права *Редактирование* и *Проведение*. Право *Редактирование* зависит от права *Просмотр*. Право *Проведение* зависит от основного права *Изменение*. А *Изменение* в свою очередь зависит от права *Чтение*. Кроме этого интерактивное право *Просмотр* требует наличия основного права *Чтение*. Все эти права будут установлены при установке флага *Интерактивное проведение.*



Если же снять флаг *Чтение*, то будут сняты и все остальные флаги, поскольку право на чтение является самым базовым.

На уровне корневого элемента всей конфигурации можно установить набор административных прав, определяющих, каким клиентским приложениям разрешен доступ к базе, разрешен ли доступ к журналу регистрации и т.д.:



Если пользователю назначено несколько ролей, то предоставление доступа по каждому объекту и виду права доступа (например, *Проведение*) будет работать следующим образом:

- Если хотя бы в одной роли есть разрешение, то доступ будет разрешен
- Если во всех ролях есть запрещение, то доступ будет запрещен.

Ограничение доступа к данным на уровне записей (RLS)

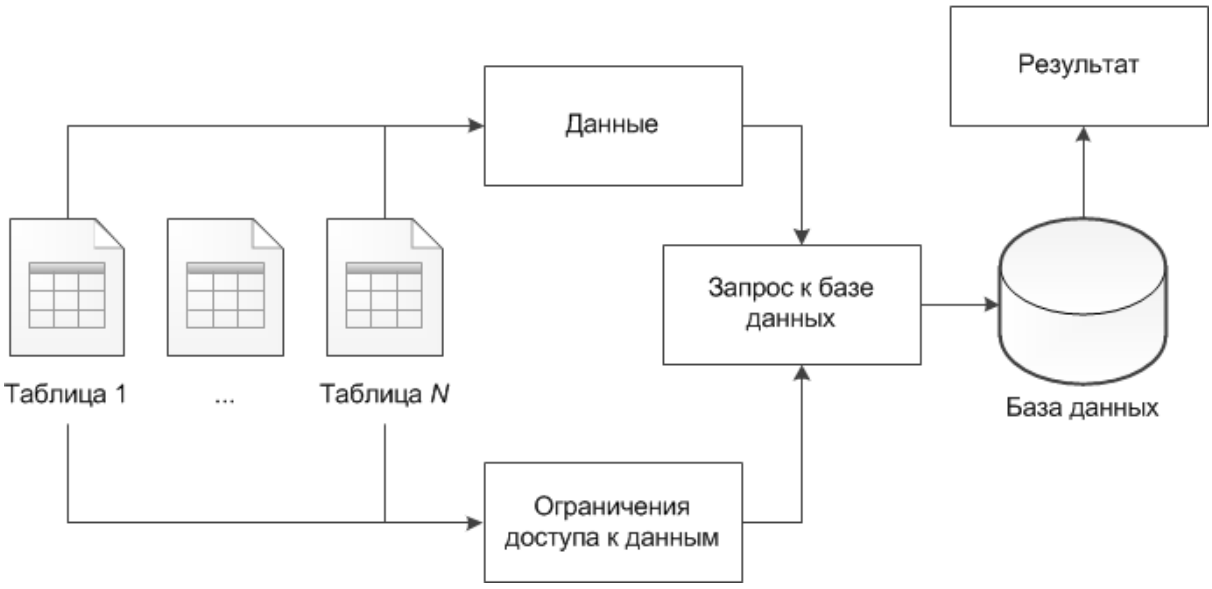
Рассмотренные выше механизмы позволяют разрешить или запретить доступ к данным для объекта метаданных целиком. То есть ко всем элементам справочника *Контрагенты* или ко всем документам *ПриходТовара*.

Зачастую возникает необходимость разрешить доступ пользователя не вообще ко всем контрагентам, а только к определенной группе, с которой работает пользователь. Остальных контрагентов пользователю не нужно даже видеть в списке контрагентов и в любых отчетах.

Т.е. доступ на таблицу у пользователя должен быть, но не целиком, а только по некоторому условию. Такие задачи решаются при помощи механизма ограничения доступа на уровне записей (RLS – Record Level Security).

Ограничения доступа к данным могут применяться в следующих операциях с данными: *Чтение*, *Добавление*, *Изменение* и *Удаление*. Ограничения доступа на уровне записей представляют собой дополнительные условия, накладываемые на данные.

Действие над конкретным объектом может быть выполнено, если значение дополнительного условия (ограничения) для этого объекта истинно.



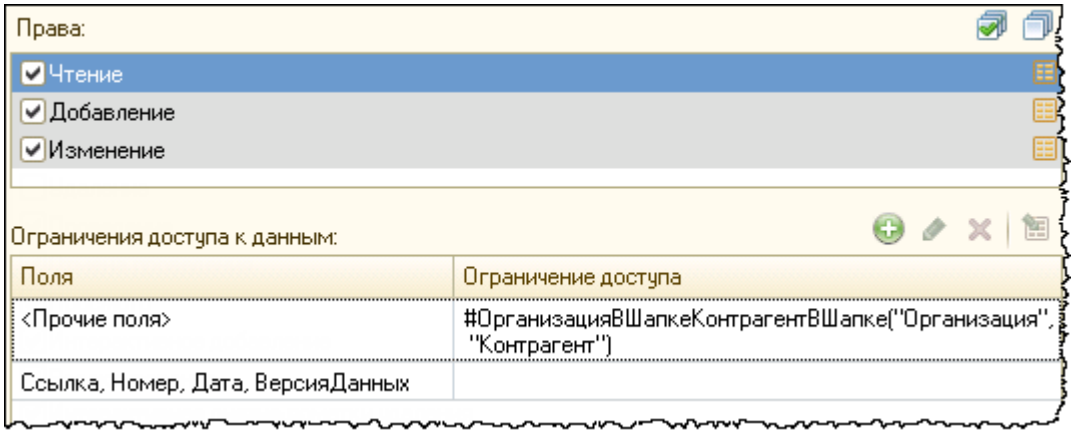
Для операции *Изменение* ограничению доступа к данным должен соответствовать объект как до изменения (чтобы объект был прочитан), так и после изменения (чтобы объект был записан).

Важно, что для операций изменения, добавления и удаления можно задать только одно условие, а для операции чтения можно задать несколько ограничений доступа на уровне записей.

Механизм позволяет накладывать ограничение не только на всю запись базы данных целиком, но и на отдельные ее поля. При этом можно указать имя конкретного поля или специальное поле *Прочие поля*.

В первом случае условие будет накладываться только в том случае, если в запросе присутствует поле, для которого задано ограничение.

Во втором случае ограничение будет накладываться для всех полей объекта, кроме полей, для которых ограничения заданы явным образом:



При задании ограничения на конкретное поле это поле будет прочитано в том случае, если ограничение выполняется, а при задании ограничения на *Прочие поля* данные объекта будут прочитаны только в том случае, если ограничение выполняется для всех полей объекта, попавших в запрос чтения данных.

Данные могут быть выбраны из базы запросом или при помощи объектной техники.

При использовании объектного чтения объект всегда будет считан из базы целиком. А при использовании запроса есть возможность явно указать только необходимые поля. Нужно учитывать эту особенность при работе с ограничениями доступа на уровне записей.

Язык ограничения доступа к данным

Ограничения доступа на уровне записей задаются в конфигураторе в ролях.

Описываются они на специальном языке, который представляет собой подмножество языка запросов. В этом запросе необходимо описать условие (секцию ГДЕ запроса). Такая секция будет добавляться к любым запросам, обращающимся к этому объекту. Это может быть запрос, выбирающий данные для построения списка контрагентов на форме, или запрос, формирующий отчет по продажам. Если условие для объекта базы данных принимает значение *Истина*, значит, у текущего пользователя есть права на выполнение операции над этим объектом базы данных, и операция выполняется, в противном случае операция не выполняется.

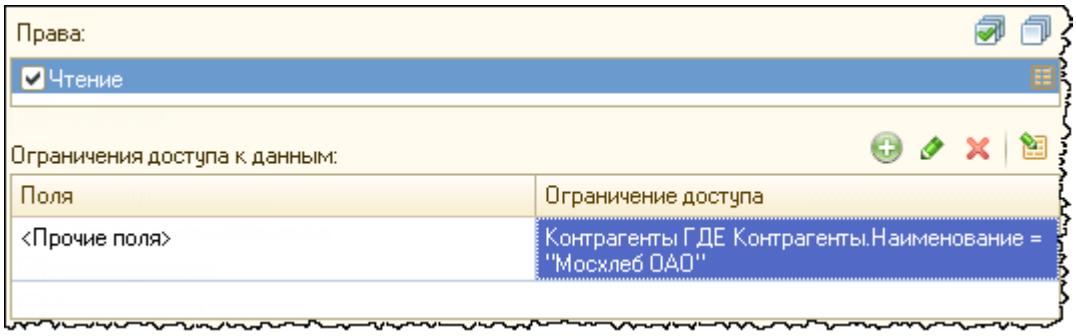
Хотя язык ограничения доступа на уровне записей похож на обычный язык запросов платформы «1С:Предприятие 8», он имеет ряд особенностей и ограничений:

- В запросе всегда присутствует одна таблица в качестве источника данных – это таблица объекта, на который накладывается ограничение
- В запросе доступны только секции `ИЗ` и `ГДЕ` языка запросов

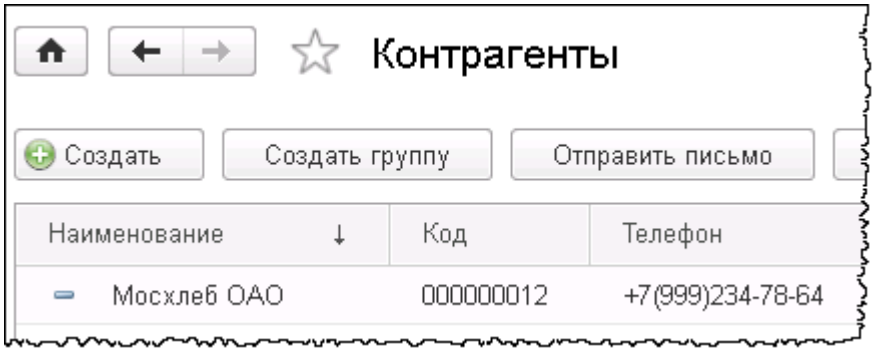
- В условиях можно указывать параметры сеанса и функциональные опции в качестве параметров запроса
- Не допускается применение оператора `В ИЕРАРХИИ` и предложения `ИТОГИ`
- Нельзя использовать виртуальные таблицы регистров (например, `СрезПоследних` или `ОстаткиИОбороты`)
- В запросе можно использовать шаблоны, упрощающих написание ограничений.

Воспользуемся демонстрационной конфигурацией «Управляемое приложение» фирмы «1С».

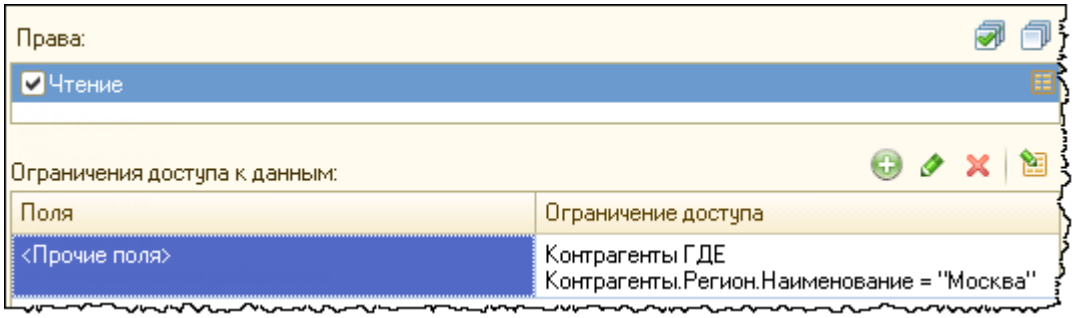
Самое простое ограничение доступа выглядит таким образом:



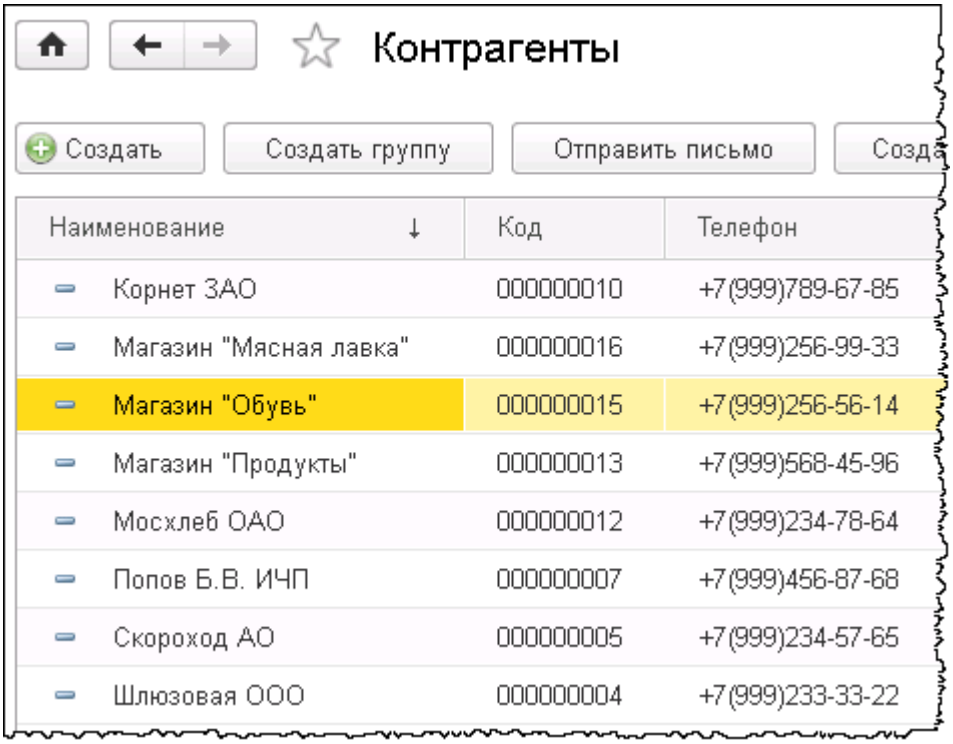
В таком случае будут доступны для чтения только контрагенты, у которых наименование равно заданной строке «Мосхлеб ОАО». В списке контрагентов будет отображаться только одна запись, остальных просто не будет видно:



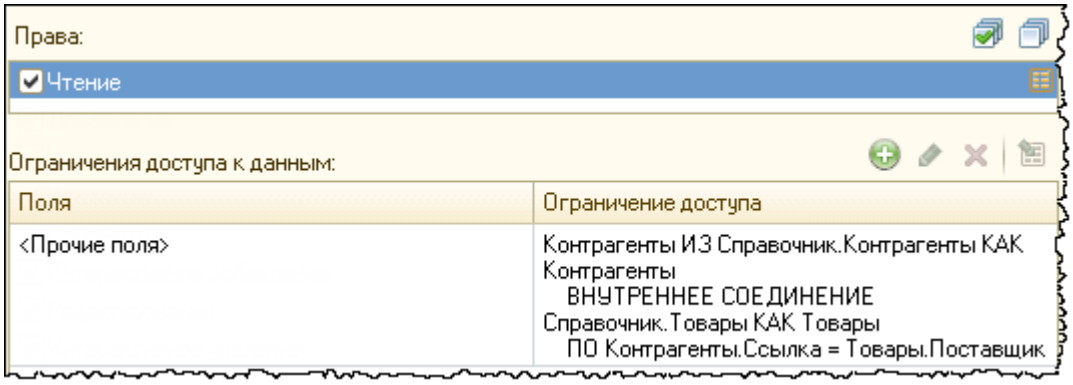
В условии ограничения доступа можно также обращаться через точку к полям реквизитов основной таблицы:



В этом случае в списке отображается большее количество контрагентов:



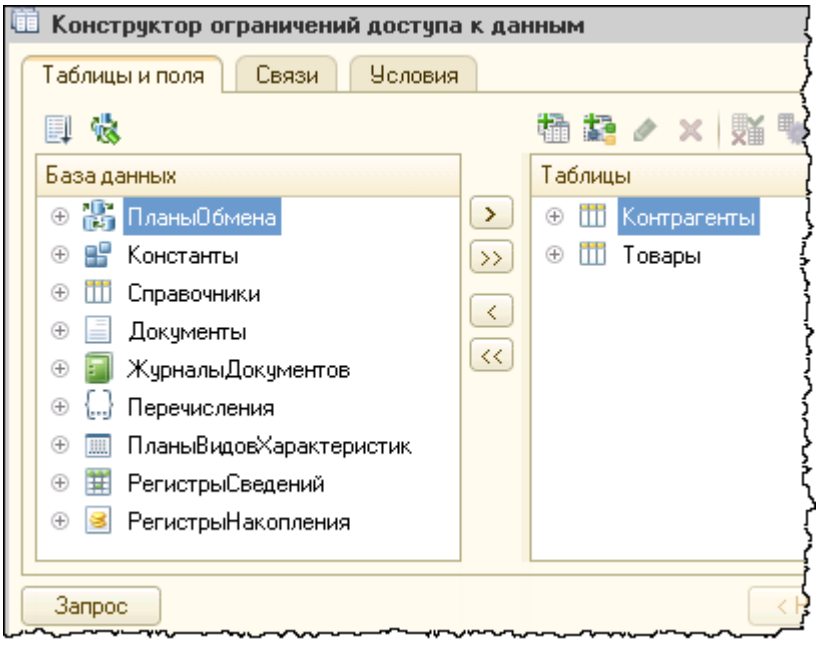
Кроме этого в условии можно использовать соединения нескольких таблиц. Например, необходимо иметь доступ только к тем контрагентам, которые указаны как основной поставщик в каком-либо товаре:



Обратите внимание, что в этом примере явно нет секции `ГДЕ`, однако такое ограничение работает. Если быть более точным, то применяется следующая трактовка истинности подобного условия:

- Запись считается доступной в том случае, если в результате работы условия для одной записи таблицы основного объекта ограничения получена непустая таблица (т.е. таблица, содержащая не менее одной записи).
- Если в результате работы условия получается пустая таблица, то запись считается недоступной.

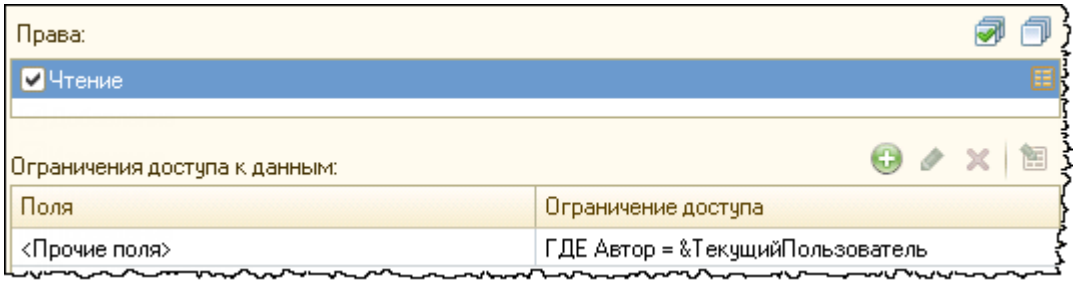
Текст ограничения доступа можно набирать вручную, а можно воспользоваться конструктором ограничения доступа к данным, который очень похож на обычный конструктор запроса:



В ограничениях доступа к данным можно использовать вложенные запросы, но результаты вложенных запросов не должны содержать табличные части.

Бесплатные материалы проекта:
http://курсы-по-1с.рф/free/
Электронная почта: support@Kursy-po-1C.ru
Телефоны: **8-800 1000-613**, +7(495) 7777-096

В качестве параметров в тексте запроса допустимо использовать параметры сеансов и не зависящие от параметров функциональные опции. Например, чтобы каждому пользователю разрешить доступ только к собственным заказам, можно использовать следующий текст ограничения:



Здесь `ТекущийПользователь` – имя параметра сеанса.

Применение ограничений доступа

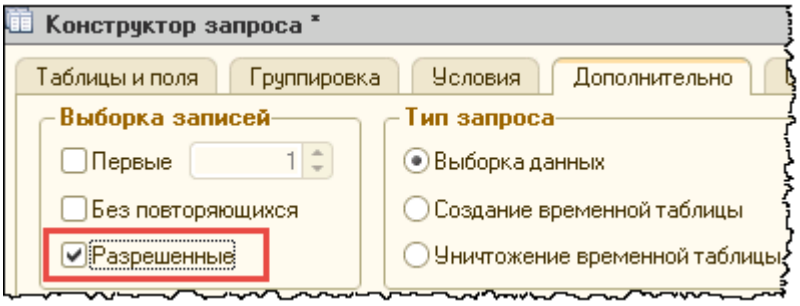
Ограничения доступа срабатывают при любом обращении к объекту (при помощи запросов, при программном доступе, при отображении на форме). Существует два способа функционирования ограничений доступа:

- ***Все***. Операция должна быть выполнена над всеми подразумеваемыми данной операцией объектами базы данных. Если при выполнении такой операции должны быть прочитаны или изменены объекты базы данных, для которых не выполняются соответствующие ограничения доступа, то операция завершается аварийно из-за нарушения прав доступа
- ***Разрешенные***. При выполнении операции над данными должны быть прочитаны только те объекты базы данных, которые удовлетворяют соответствующим ограничениям доступа. Объекты базы данных, не удовлетворяющие ограничениям доступа, при выполнении такой операции считаются отсутствующими и на результат операции не влияют.

Например, при отображении динамических списков используется способ «Разрешенные», а при получении объектов средствами встроенного языка и при записи объектов в базу данных применяется способ «Все».

А вот в запросах способом функционирования ограничений можно управлять. Если в тексте запроса используется ключевое слово `РАЗРЕШЕННЫЕ`, то работа ограничений выполняется в соответствии с одноименным способом, в противном случае используется способ «Все». Это является значительным преимуществом использования запросов для получения данных.

В конструкторе запроса для включения ключевого слова РАЗРЕШЕННЫЕ используется одноименный флаг на закладке *Дополнительно*:



Важно, что при использовании объектного доступа к данным получить только разрешенные данные нельзя. Платформа «1С:Предприятие 8» таких возможностей не предоставляет.

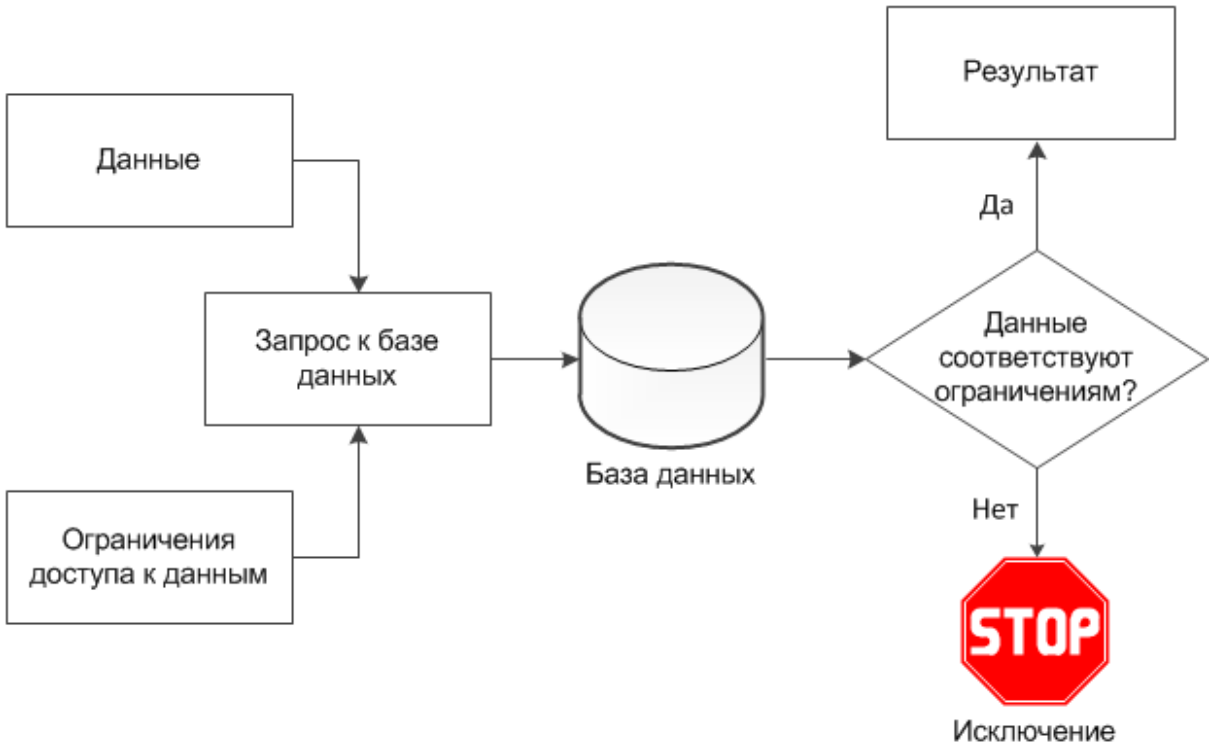
Наложение ограничений доступа к данным

Все операции с данными, выполняемые как при помощи запросов, так и при помощи объектного подхода, преобразуются в низкоуровневый SQL-запрос к базе данных, который передается на выполнение серверу СУБД. При подготовке результирующего текста запроса платформа «1С:Предприятие 8» накладывает использующиеся ограничения доступа. Происходит это следующим образом:

1. Формируется список прав (чтение, добавление, изменение, удаление), список таблиц базы данных и список полей, используемых этим запросом
2. Из всех ролей текущего пользователя выбираются ограничения доступа к данным для всех прав, таблиц и полей, задействованных в запросе. При этом если какая-нибудь роль не содержит ограничений доступа к данным какой-нибудь таблицы или поля, то это значит, что в данной таблице доступны значения требуемых полей из любой записи. Отсутствие ограничения доступа к данным означает наличие ограничения `ГДЕ Истина`
3. Получаются текущие значения всех параметров сеанса и функциональных опций, участвующих в выбранных ограничениях. Значения параметров сеанса должны быть установлены, иначе произойдет ошибка и запрос к базе данных выполнен не будет.
4. Ограничения, полученные из одной роли, объединяются операцией И
5. Ограничения, полученные из разных ролей, объединяются операцией ИЛИ
6. Построенные условия добавляются к SQL-запросам, передаваемыми платформой серверу СУБД. Механизм добавления условий зависит от выбранного способа действия ограничений «все» или «разрешенные».

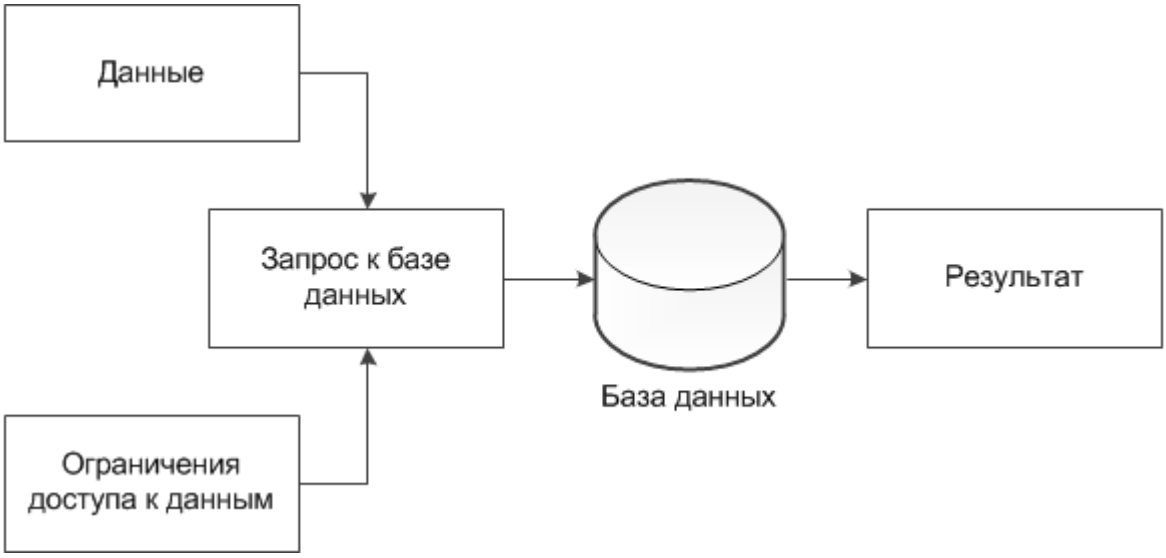
Способ ВСЕ

В этом случае в SQL-запрос добавляются условия и поля так, чтобы платформа «1С:Предприятие» могла получить информацию о том, были ли в процессе исполнения запроса к базе данных использованы запрещенные данные. Если запрещенные данные были использованы, то произойдет ошибка при выполнении запроса. Другими словами, запрос без ключевого слова РАЗРЕШЕННЫЕ завершится с ошибкой, если его результат содержит недоступные для текущего пользователя данные.

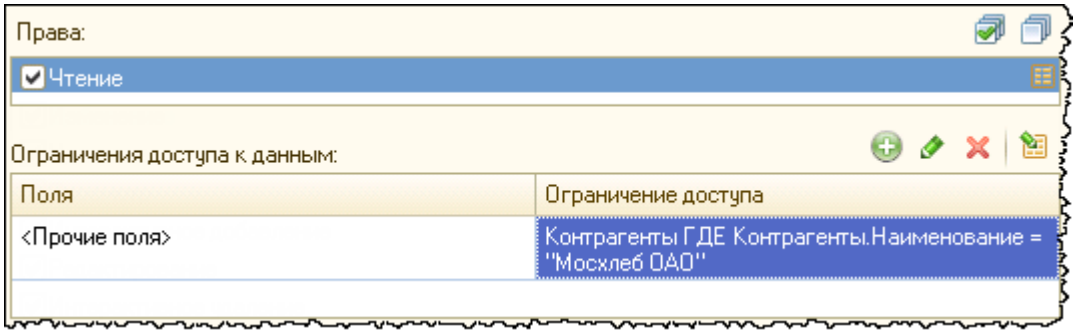


Способ РАЗРЕШЕННЫЕ

В этом случае в SQL-запрос добавляются такие условия, чтобы запрещенные данному пользователю записи не попали в результат запроса. При этом исключительная ситуация при выполнении запроса не генерируется, в результат запроса включаются только такие записи, для которых ограничение доступа к данным выполняется.



Рассмотрим, какие запросы на низком уровне будут получены при наличии ограничения доступа на уровне записей. Пусть на справочник *Контрагенты* наложено следующее ограничение доступа на чтение:



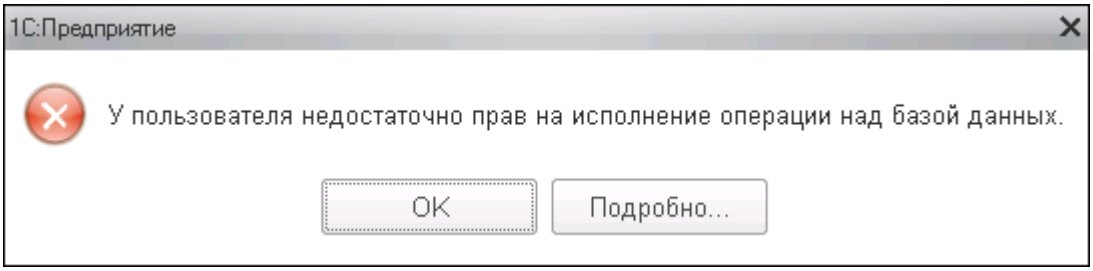
Выполняем следующий запрос:

```
ВЫБРАТЬ

    Контрагенты.Наименование КАК Наименование

ИЗ

    Справочник.Контрагенты КАК Контрагенты
```

Поскольку в запросе отсутствует ключевое слово РАЗРЕШЕННЫЕ, наложение ограничений доступа будет выполняться способом «все». SQL-запрос на уровне СУБД получится следующим:

```
SELECT

CASE WHEN ((T1.Наименование = ?)) THEN 0x01 ELSE 0x00 END,

T1.Наименование

FROM Справочник.Контрагенты T1

p_0: 'Мосхлеб ОАО'
```

В запросе в выходных полях появилось поле, которое явно в запросе на языке «1С:Предприятие 8» отсутствует. Это вспомогательное поле (флаг), показывающее, доступна или нет эта запись. Если хотя бы одна запись является запрещенной, то генерируется исключительная ситуация. Ограничение доступа в нашем примере построено так, что разрешен только один элемент справочника. Поэтому получение запросом всех записей из справочника *Контрагенты* завершается ошибкой:



Изменим немного текст запроса:

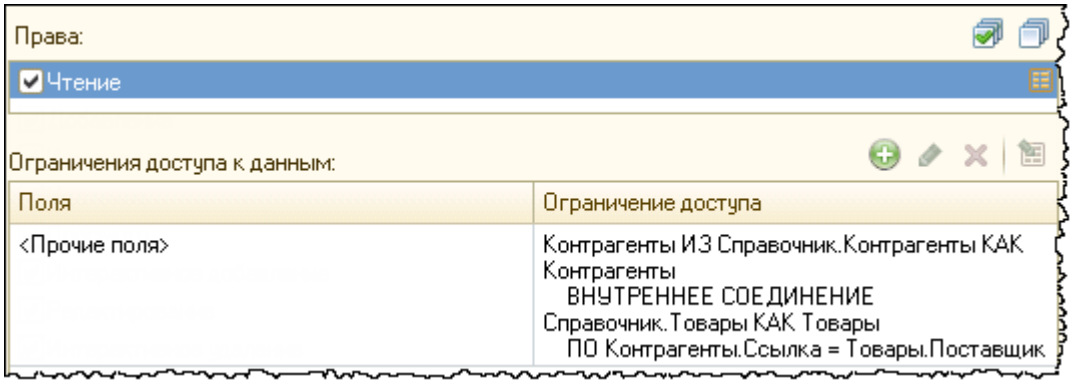
```
ВЫБРАТЬ РАЗРЕШЕННЫЕ

Контрагенты.Наименование КАК Наименование

ИЗ

Справочник.Контрагенты КАК Контрагенты
```

Теперь наложение ограничений доступа будет выполняться способом «разрешенные». SQL-запрос на уровне СУБД получится следующим:

```
SELECT

Т1.Наименование

FROM Справочник.Контрагенты Т1

WHERE ((Т1.Наименование = ?))

p_0: 'Мосхлеб ОАО'
```

Ограничение доступа было добавлено в секцию ГДЕ запроса. Таким образом СУБД вернет только те записи, на которые у пользователя есть права доступа. В нашем случае это будет только одна строка с контрагентом «Мосхлеб ОАО».

Теперь усложним задачу и в качестве ограничения доступа зададим условие с несколькими таблицами:



Запрос к таблице *Контрагенты* с ключевым словом РАЗРЕШЕННЫЕ на сервер СУБД поступает в следующем виде:

```
SELECT

Т1.Наименование

FROM Справочник.Контрагенты Т1

WHERE (EXISTS(SELECT

1

FROM (SELECT 1 AS SDBL_DUMMY) SDBL_DUAL

INNER JOIN Справочник.Товары Т2

ON (Т1.Ссылка = Т2.Поставщик)))
```

Запрос усложнился. Ограничение доступа попадало в запрос к СУБД в виде подзапросов. Этот пример показывает, как транслируется ограничение доступа, если секция ГДЕ в ограничении явно не прописана.

Рассмотренные примеры демонстрируют, что ограничения доступа усложняют текст запросов, которые передаются на сервер СУБД, что может негативно сказаться на производительности. Поэтому к разработке ограничений следует подходить очень внимательно.

Инструкции препроцессора

В тексте запроса на ограничение доступа к данным можно использовать инструкции препроцессора. Выглядят они следующим образом:

```
#Если <Выражение> #Тогда

#ИначеЕсли <Выражение> #Тогда

#Иначе

#КонецЕсли
```

Выражения должны иметь тип `Булево`. В них можно использовать параметры сеанса, обозначать их нужно амперсандом (`&Параметр`), как и параметры в тексте запроса. В зависимости от истинности, в текст запроса будет включено то или иное выражение. Если текст ограничения доступа содержит инструкции препроцессора, то его нельзя будет редактировать при помощи конструктора.

Шаблоны ограничений доступа

При разработке ограничений доступа на уровне записей может потребоваться для различных объектов написать похожие ограничения, отличающиеся какими-нибудь деталями.

Если бы мы разрабатывали программный код на встроенном языке, то повторяющийся фрагмент следует оформить как процедуру, а различия в реализации для разных объектов задать при помощи параметров процедуры:

- Это уменьшит размер программного кода, позволит избежать дублирования.

- В случае необходимости внесения изменений, потребуется отредактировать только текст процедуры, при этом сами вызовы процедуры останутся без изменений.

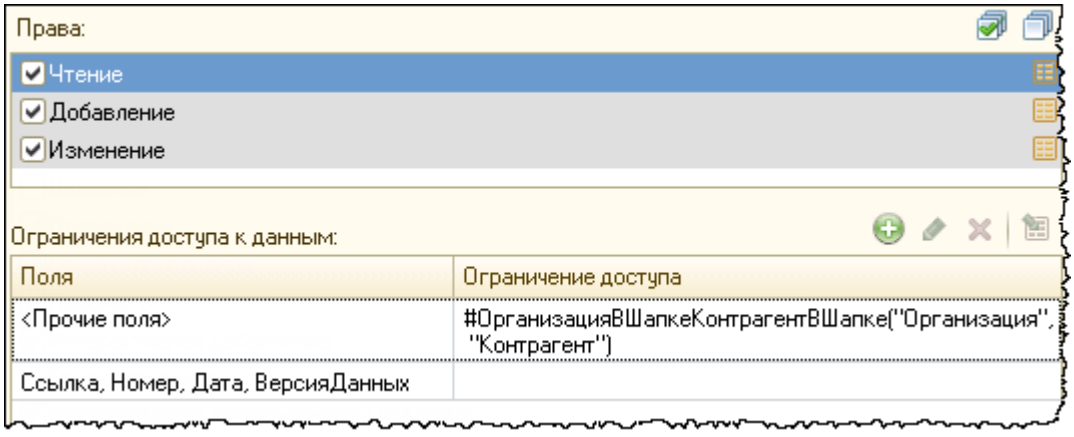
Аналогичный прием можно применить и при разработке ограничений доступа.

Фрагменты, которые можно использовать повторно, называются ***шаблонами ограничений***. Шаблон ограничения имеет имя и текст. В качестве имени можно использовать любой допустимый в платформе «1С:Предприятие 8» идентификатор.

Текст шаблона содержит фрагмент ограничения доступа. В нем, как и в процедуре во встроенном языке, можно использовать параметры. Параметры в шаблоне выделяются символом «#». После этого символа далее можно использовать:

- Ключевое слово `Параметр`, после которого в скобках указывается номер параметра в шаблоне
- Ключевое слово `ТекущаяТаблица` – обозначает вставку в текст полного имени таблицы, для которой строится ограничение
- Ключевое слово `ИмяТекущейТаблицы` – обозначает вставку в текст полного имени таблицы (как строковое значение, в кавычках), к которой применяется инструкция, на текущем варианте встроенного языка
- Ключевое слово `ИмяТекущегоПраваДоступа` – содержит имя права, для которого выполняется текущее ограничение: ЧТЕНИЕ, ДОБАВЛЕНИЕ, ИЗМЕНЕНИЕ, УДАЛЕНИЕ
- Имя параметра шаблона – означает вставку в текст ограничения соответствующего параметра шаблона
- Символ "#" – обозначает вставку в текст одного символа "#".

Тогда в самом тексте ограничения нужно вызвать сам шаблон и передать в него параметры:



При наложении такого ограничения доступа платформа «1С:Предприятие 8» производит замену параметров в шаблоне на фактически использованные выражения в ограничении

доступа, а также подстановку полученного текста шаблона в результирующий текст запроса для ограничения доступа.

Рассмотрим пример. Пусть шаблон ограничения имеет имя `ОграничениеПоАвтору`. Текст шаблона выглядит следующим образом:

```
ГДЕ #Параметр(1) = &ТекущийПользователь
```

В самом ограничении доступа используется выражение:

```
#ОграничениеПоАвтору("Автор")
```

Тогда при наложении такого ограничения, при макроподстановке шаблона текст результирующего запроса будет следующий:

```
ГДЕ Автор = &ТекущийПользователь
```

Если в другом документе вместо реквизита `Автор` используется реквизит с именем `Ответственный`, то текст шаблона менять не нужно, достаточно в ограничении доступа прописать:

```
#ОграничениеПоАвтору("Ответственный")
```

Рекомендации по разработке ограничений доступа

В ограничениях доступа на уровне записей в качестве параметров запроса можно использовать параметры сеанса. Здесь они могут использоваться как заранее подготовленная информация, на которую опирается логика ограничения прав. Поэтому необходимо добавить в конфигурацию необходимые параметры сеанса и установить их значения в процедуре `УстановкаПараметровСеанса()` модуля сеанса.

Необходимо помнить, что использование ограничений доступа может привести к замедлению любого обращения к этим данным. Также сложные конструкции в ограничениях доступа плохо сказываются на производительности.

Если необходимо часть действий выполнять без учета установленных ограничений, а полные права на эти объекты давать из соображений безопасности не стоит, следует

вынести эти действия в привилегированные модули или явно включать и выключать привилегированный режим в соответствующих местах программного кода.

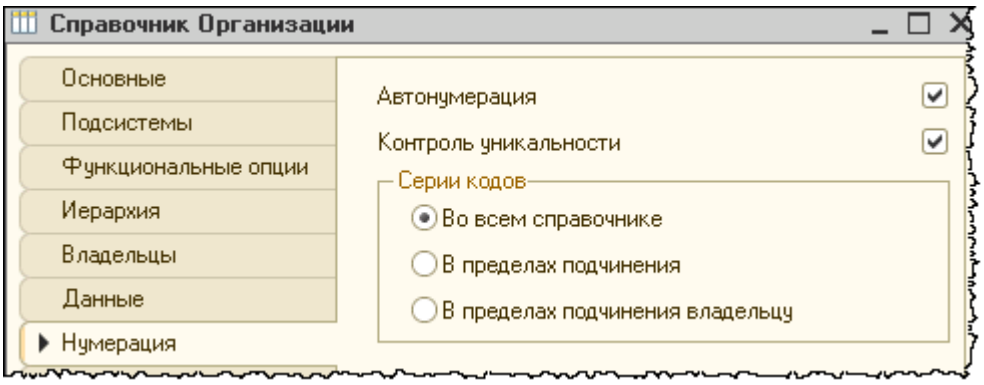
При разработке ограничений прав доступа важно учитывать, что объекты конфигурации могут выполнять обращения к некоторым полям базы данных неявно. При этом наложение ограничений доступа выполняется способом «все», что может приводить к неожиданным сообщениям о нарушении прав доступа. Поэтому ограничивать доступ к таким полям нельзя.

Включение автонумерации или контроля уникальности номеров объектов приводит к неявному чтению поля *Код* (для документов, бизнес процессов и задач – *Номер*) при создании нового объекта и при его записи.

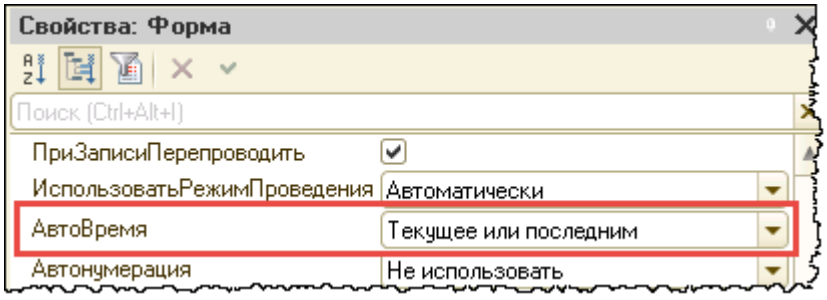
Если в справочниках в качестве серии кодов выбрано «в пределах подчинения», то происходит неявное чтение полей *Код*, *Родитель*. Если используется иерархия групп и элементов, то кроме этого неявно считывается поле *ЭтоГруппа*.

При выборе в качестве серии кодов «в пределах подчинения владельцу» неявно будет выполняться чтение полей *Код* и *Владелец*.

Поэтому не стоит устанавливать ограничения на чтение перечисленных полей.



Если при записи документа, бизнес-процесса или задачи установлен режим автоматического определения времени, то при записи будет неявно выполняться чтение полей *Дата* и *Ссылка*. Поэтому чтение полей *Дата* и *Ссылка* должно быть разрешено.



Бесплатные материалы проекта:
http://курсы-по-1с.рф/free/
Электронная почта: support@Kursy-po-1C.ru
Телефоны: **8-800 1000-613**, +7(495) 7777-096

Также рекомендуется проиндексировать реквизиты, которые используются в ограничениях доступа. Это даст возможность СУБД использовать индекс для поиска записей, удовлетворяющих условию ограничения доступа.

Ускорение работы с использованием индексов достигается в первую очередь за счет того, что индекс имеет структуру, оптимизированную под поиск, например, сбалансированного дерева. Но индексы занимают дополнительный объем памяти, поэтому перед созданием индекса следует убедиться, что планируемый выигрыш в производительности запросов превысит дополнительную затрату ресурсов компьютера на поддержание индекса.

Использование нескольких таблиц и соединений в ограничениях доступа приводят к усложнению запроса. Поэтому рекомендуется реквизиты, на которые опирается определение доступности записей, включать в состав самого объекта конфигурации, а не обращаться к ним через точку. Это приведет к хранению избыточной информации, но позволит увеличить скорость выполнения запроса.

Дополнительные видеоуроки по теме

Открытый просмотр без регистрации

Перечень видеоуроков:

- Ограничение доступа к данным при помощи ролей
- Ограничение доступа на уровне записей (RLS)
- Реализация ограничения доступа на уровне записей для справочника Контрагенты
- Принцип работы ограничений доступа на уровне записей на низком уровне
- Совместное применение нескольких ограничений доступа на уровне записей
- Наложение ограничений методом ВСЕ
- Наложение ограничений методом РАЗРЕШЕННЫЕ
- Исправление ошибки, возникающей из-за наложения прав доступа на уровне записей

Видеоматериалы опубликованы по адресу:

http://Курсы-по-1С.рф/news/rls-data-access-restrictions/

Считаем, что «увидеть» даже важнее, чем «прочесть».

Бесплатные материалы проекта:
http://курсы-по-1с.рф/free/

Электронная почта: support@Kursy-po-1C.ru
Телефоны: **8-800 1000-613**, +7(495) 7777-096