Дата и место проведения мероприятия

Новый RLS в БСП 3.0: быстрее, проще и перспективней

Докладчик
Должность

Старый RLS (в формате БСП 2.0)

- Существующий механизм имеет ряд проблем.
  - Низкая производительность по сравнению с полноправным пользователем:
    - Список документов может открываться слишком долго:
      - от нескольких секунд в самых хороших случаях,
      - до многих минут в самых плохих случаях.
    - Отчеты могут формироваться в 2–10 раз дольше.

  - Очень сложно создавать ограничения доступа и редактировать их.
  - Практически невозможно отлаживаться.
  - Плохая диагностика ошибок нехватки доступа для пользователей.

Новый RLS (в формате БСП 3.0)

- Что хотим достичь?
  - Существенно повысить производительность под неполноправным пользователем:
    - Список документов открывается и обновляется за 1 секунду или меньше.
    - Отчеты формируются не более чем на 30 % медленнее, чем в режиме без RLS.
  - Упростить процесс создания и редактирования ограничений.
  - Упростить отладку ограничений.
  - Сделать более внятную диагностику ошибок нехватки доступа для пользователей.

Основа решения

- RLS в формате БСП 2.0 (старый)
  - Логика ограничения реализуется на языке запросов:
    - Сложность запроса зависит от сложности ограничения.
    - Производительность почти непредсказуема.
- RLS в формате БСП 3.0 (новый)
  - На языке запросов универсальное ограничение:
    - Сложность запроса почти неизменна.
    - Производительность предсказуема.
  - Логика ограничения:
    - Описывается в модуле менеджера объекта метаданных на специальном диалекте языка ограничения доступа.
    - Реализуется путем расчета прав (заполнения специальных регистров в фоновом задании).

Новый RLS (в формате БСП 3.0)

- В РЕЗУЛЬТАТЕ:
  - Производительность стала выше от 2 до 1000 раз
    - За счет того, что права (в сложной части) теперь рассчитываются не в СУБД при каждом запросе, а в фоновом задании 1 раз сразу для всех пользователей (без избыточных расчетов).
    - Кроме того, реализована гибкая автоматическая адаптация к настройкам администратора (если ограничение отключено по виду доступа, то его как будто не указывал разработчик).
  - Описание логики ограничения стало проще.
    - Теперь описание в модуле менеджера 1 раз в 1 месте, а не в виде нескольких точных копий в ролях.
    - Контроль ошибок в ограничении доступа не хуже, чем у платформы для языка запросов.
    - Предусмотрена возможность переопределения на встроенном языке (необходимо при использовании библиотек).

Новый RLS (в формате БСП 3.0)

- ДОПУЩЕНИЯ:
  - Немного замедляется запись в режиме полноправного пользователя (на 0.005-0.05 сек на документ).
    - При записи требуется обновление прав доступа к документу.
  - После изменения настроек прав пользователей, изменения вступают в силу не сразу (от 1 сек до 5–20 мин).
    - Какое-то время выполняется обновление прав в фоновом задании.

Новый RLS (в формате БСП 3.0)

- Полученное ускорение чтения:
  - ERP, Приходные кассовые ордера (разрешено 20 из 100 000), MS SQL 2008 R2
    - в 7 раз - открытие списка: было – 9 сек, стало 1.25 сек
    - в 46 раз - запрос «Выбрать Разрешенные Первые 1000 Ссылка Из Документ.ПриходныйКассовыйОрдер» было – 2.9 сек, стало 0.063 сек
  - ERP, Контрагенты (разрешено 6 из 8 000), MS SQL 2008 R2
    - в 30 раз - открытие списка: было – 3 сек, стало 0.1 сек
    - в 16 раз - запрос «Выбрать Разрешенные Первые 1000 Ссылка Из Справочник.Контрагенты» было – 0.24 сек, стало 0.015 сек

Новый RLS (в формате БСП 3.0)

- Полученное ускорение чтения (продолжение):
  - ERP, Реализация товаров и услуг (разрешено 4 из 128 396), MS SQL 2008 R2
    - в 7 раз – открытие списка: было – 9 сек, стало 1.25 сек
    - в 36 раз – запрос «Выбрать Разрешенные Первые 1000 Ссылка Из Документ.РеализацияТоваровУслуг» было – 2.8 сек, стало 0.078 сек
  - ERP, Задачи (без отбора по автору и исполнителю, разрешено 37 из 80 000), MS SQL 2008 R2
    - в > 300 раз – открытие формы списка: было >10 мин, стало 2 сек
  - БСП, Взаимодействия по предметам (разрешено 100 из 50 000), Файловая ИБ
    - в 6.5 раз – открытие списка: было 80 сек, стало 12 сек (без RLS – 9 сек)

Новый RLS (в формате БСП 3.0)

- Побочное небольшое замедление записи:
  - При параллельной работе пользователей (создание новых документов).
    - В клиент-серверном режиме без изменилась – активная работа не отличается для нового и старого RLS.
    - В файловой ИБ при средней активности без изменений, но при высокой конкурентной программной записи возникает взаимоблокировка (решено в более старших версиях платформы).
  - При массовой загрузке данных (загрузка документов из XML)
    - В полноправном режиме замедление на 5–50 мс на документ.
      - Предусмотрен API для временного отключения обновления прав при пакетной обработке данных, чтобы убрать эту задержку.
    - В неполноправном режиме наблюдается, как ускорение, так и замедление, при этом в среднем, изменения незначительны в обе стороны.

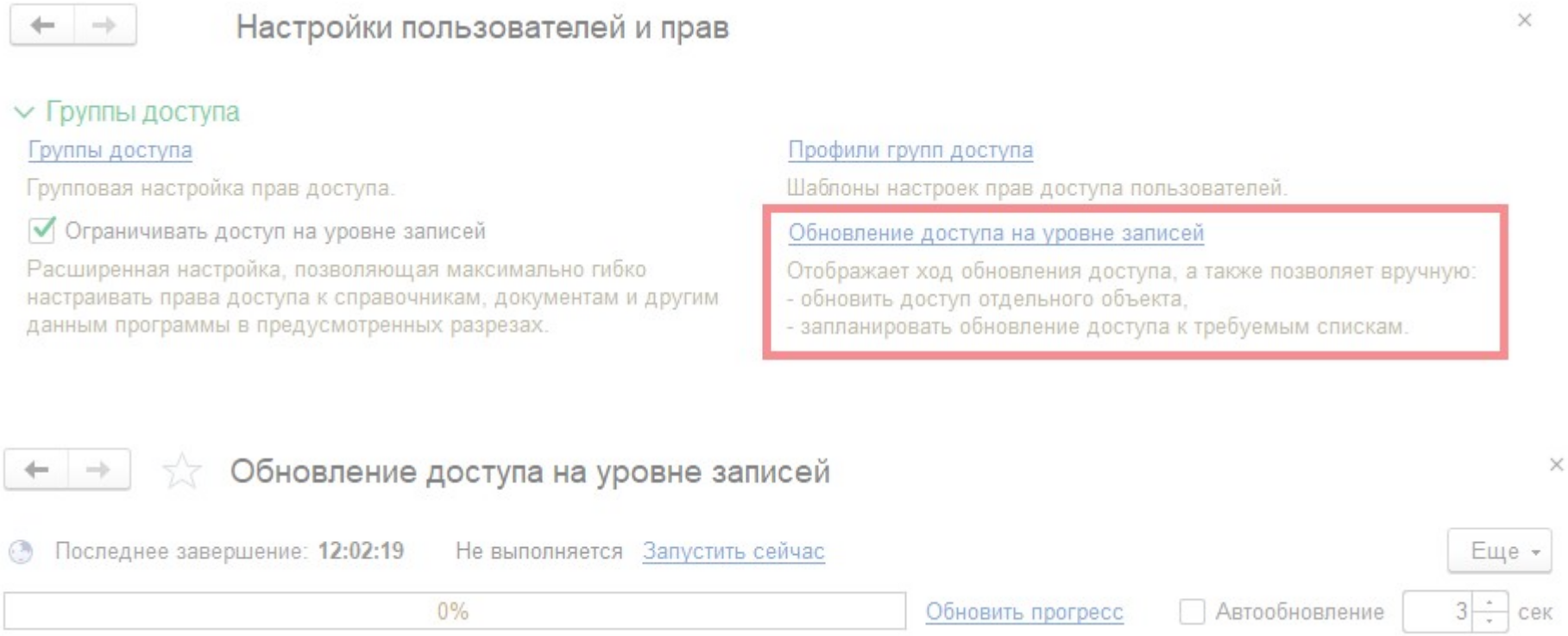
Новый RLS (в формате БСП 3.0)

- Оценка времени, когда права вступят в силу, после изменения настроек прав пользователей.
  - ERP (**1ГБ .dt**), HDD, MS SQL 2008R2 (как и PostgreSQL 10.3.2)
    - Заполнение (обновление «с нуля») **~ 10 минут**, повторное обновление («холостой» ход) **~ 2.5 минут**
    - 7.3 тыс. ключей на 1.1 млн объектов и 39 тыс. групп записей регистров, 110 тыс. записей прав наборов групп доступа, 80 тыс. записей прав пользователей
  - ЗУП (**3ГБ .dt**), HDD, MS SQL 2008R2 (как и PostgreSQL 10.3.2)
    - Заполнение (обновление «с нуля») **~ 20 минут**, повторное обновление («холостой» ход) **~ 5.5 минут**
    - 17.7 тыс. ключей на 0.5 млн. объектов и 1 млн. групп записей регистров, 171 тыс. записей прав наборов групп доступа, 37 тыс. записей прав пользователей

Обновление в 12 потоков, процессор 6 ядер 4.5 ГГц, 32 Гб ОЗУ

Включение RLS в формате БСП 3.0

- По умолчанию включен старый RLS (в формате БСП 2.0).
- Для включения нового RLS (в формате БСП 3.0) нужно через **Все функции** включить константу **Ограничивать доступ на уровне записей универсально** и выполнить обновление доступа.



Формат RLS: как БЫЛО и как СТАЛО

- БЫЛО (RLS в формате БСП 2.0):
  - Логика ограничения указывалась в правах роли:

```
#ПоЗначениям( "Документ._ДемоЗаказПокупателя", "","",
"_ДемоОрганизации", "Организация",
"_ДемоГруппыПартнеров","Партнер", "","", "","", "","", "","",
"","", "","", "","", "","", "","", "","", "","", "","")
```

- СТАЛО (RLS в формате БСП 3.0):
  - В правах роли указывается только универсальный шаблон:

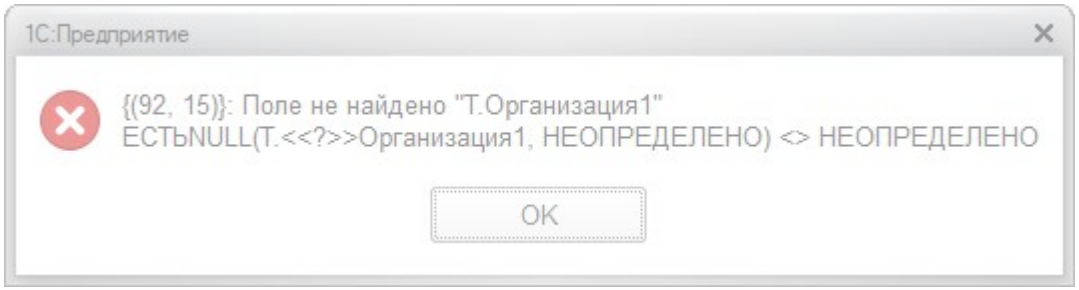
```
#ДляОбъекта("")
```

  - Логика ограничения указывается в модуле менеджера объекта:

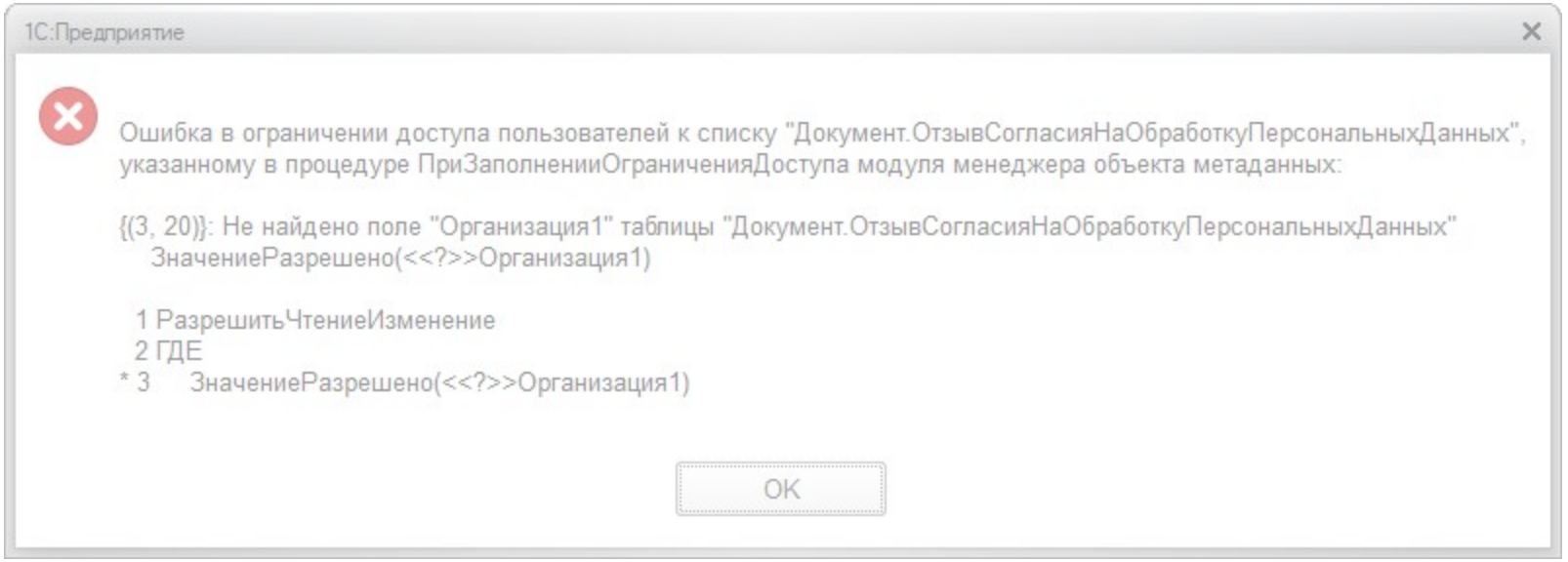
```
Процедура ПриЗаполненииОграниченияДоступа(Ограничение) Экспорт
    Ограничение.Текст =
    "РазрешитьЧтениеИзменение
    |ГДЕ
    |    ЗначениеРазрешено(Организация)
    |    И ЗначениеРазрешено(Партнер)";
КонецПроцедуры
```

Улучшение диагностики ошибок для разработчика

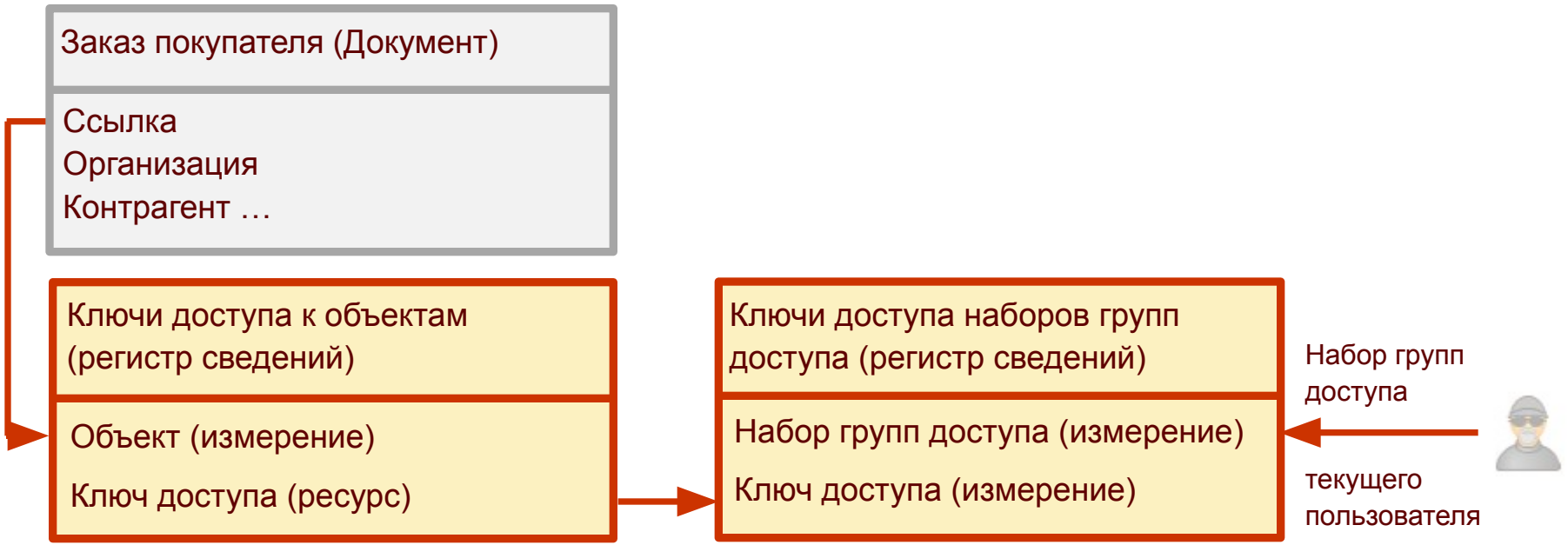
- БЫЛО (ошибка RLS в режиме 1С:Предприятия):



- СТАЛО (ошибка RLS в режиме 1С:Предприятия):

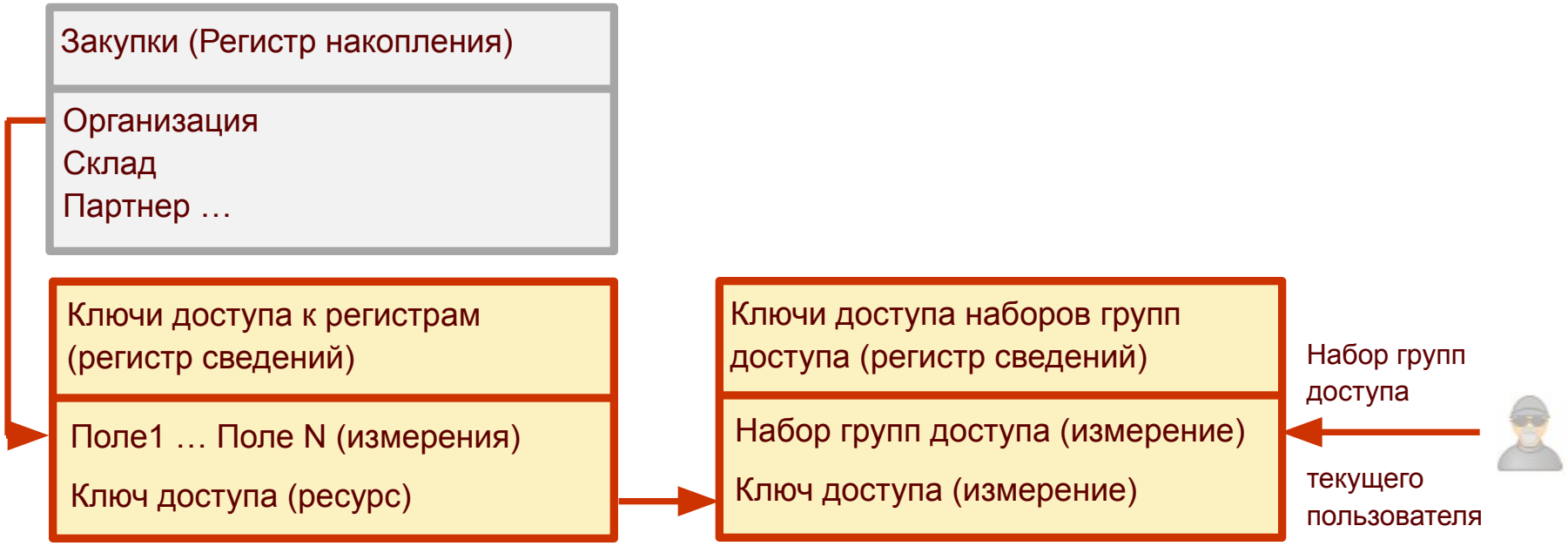


Шаблон #ДляОбъекта(…)
RLS для ссылочных таблиц




```
Документ ГДЕ ИСТИНА В (
  ВЫБРАТЬ ПЕРВЫЕ 1 ИСТИНА
  ИЗ РегистрСведений.КлючиДоступаКОбъектам КАК КлючиДоступаКОбъектам
  ВНУТРЕННЕЕ СОЕДИНЕНИЕ РегистрСведений.КлючиДоступаНаборовГруппДоступа КАК РазрешенныеКлючи
  ПО
     КлючиДоступаКОбъектам.Объект        = Документ.Ссылка
   И КлючиДоступаКОбъектам.КлючДоступа   = РазрешенныеКлючи.КлючДоступа
   И РазрешенныеКлючи.НаборГруппДоступа В (&РазрешенныйНаборГруппДоступа,
                                           &РазрешенныйПустойНаборГруппДоступа) )
```

Шаблон # ДляРегистра(…)
RLS для регистров




```
Регистр ГДЕ ИСТИНА В (
  ВЫБРАТЬ ПЕРВЫЕ 1 ИСТИНА
  ИЗ РегистрСведений.КлючиДоступаКРегистрам КАК КлючиДоступаКРегистрам
  ВНУТРЕННЕЕ СОЕДИНЕНИЕ РегистрСведений.КлючиДоступаНаборовГруппДоступа КАК РазрешенныеКлючи
  ПО
     КлючиДоступаКРегистрам.Регистр = Значение(Справочник.ИдентификаторыОбъектовМетаданных.<Имя>)
   И КлючиДоступаКРегистрам.Поле1   = Регистр.Организация
   И КлючиДоступаКРегистрам.Поле2   = Регистр.Склад
   …
   И КлючиДоступаКОбъектам.КлючДоступа  = РазрешенныеКлючи.КлючДоступа
   И РазрешенныеКлючи.НаборГруппДоступа В (&РазрешенныйНаборГруппДоступа,
                                           &РазрешенныйПустойНаборГруппДоступа) )
```

Переход на версию БСП 3.0

- Для конвертации старого RLS в новый формат предусмотрен инструмент разработчика **ПереходНаВерсию301.epf**
  - Обработка анализирует роли делает вставку в переопределяемый модуль и модуль менеджера объекта:

```
Процедура ПриЗаполненииСписковСОграничениемДоступа(Списки) Экспорт
    Списки.Вставить(Метаданные.Документы._ДемоЗаказПокупателя, Истина);
КонецПроцедуры
Процедура ПриЗаполненииОграниченияДоступа(Ограничение) Экспорт
    Ограничение.Текст =
    "РазрешитьЧтениеИзменение
    |ГДЕ
    |    ЗначениеРазрешено(Организация)
    |    И ЗначениеРазрешено(Партнер) ";
КонецПроцедуры
```

- Если конвертация не удалась, тогда вставляется комментарий с ограничением из роли и отметкой «todo» для конвертации вручную. В ERP только 2 % конвертировано вручную из > 1000 * 3 ограничений.

Поддержка нового и старого RLS

- Некоторое время в типовых решениях будут использоваться оба варианта RLS (старый и новый). Они будут изменяться синхронно.
  - Для этого в ролях RLS будет построен через условие:

```
#Если &ОграничениеДоступаНаУровнеЗаписейУниверсально #Тогда
#ДляОбъекта("")
#Иначе
#ПоЗначениям( "Документ._ДемоЗаказПокупателя","","",
"Организации","Организация", "ГруппыПартнеров","Партнер", "","", …)
#КонецЕсли
```

  - А в модуле менеджера логика нового RLS будет точно совпадать с логикой старого RLS, указанного в ролях (во второй части условия):

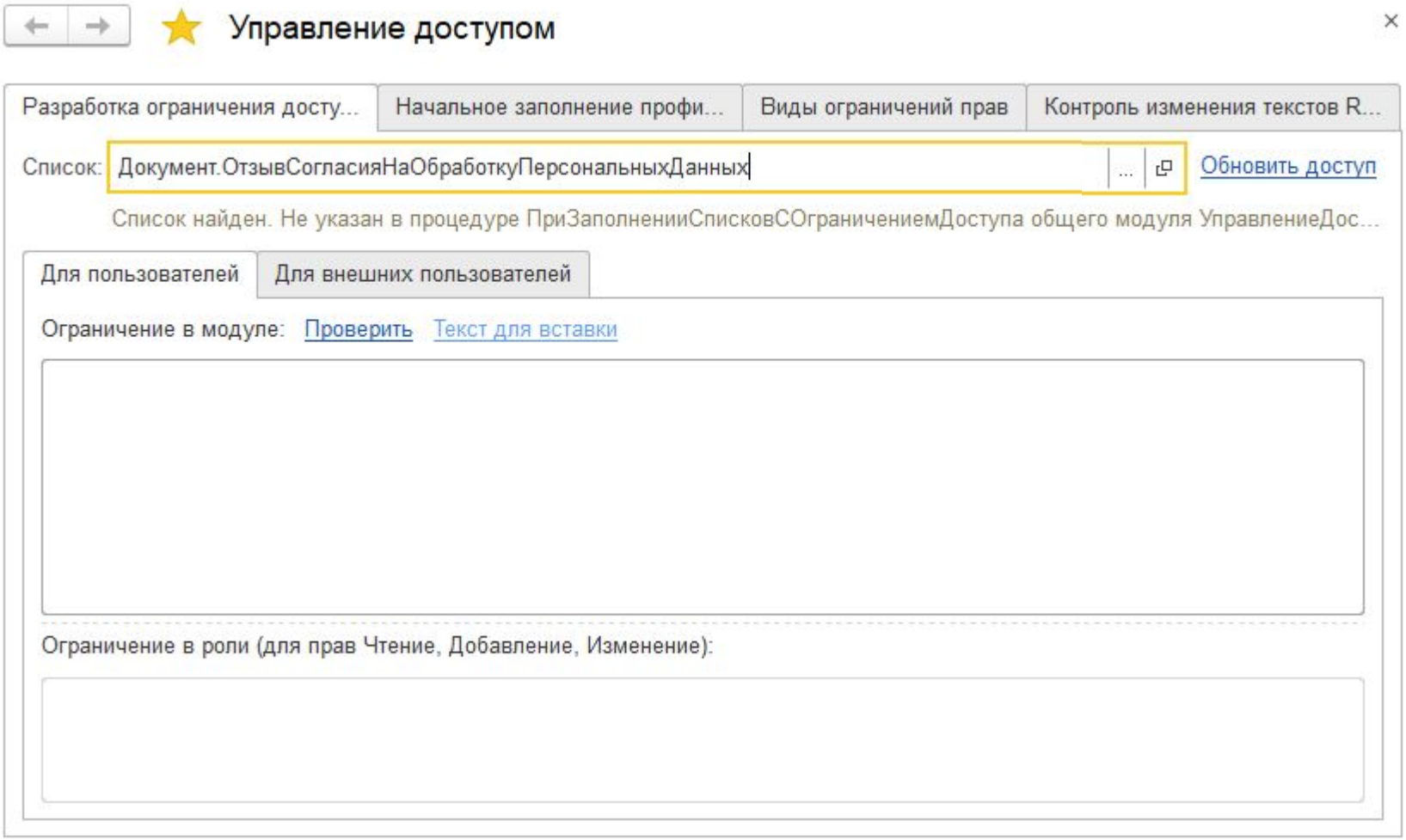
```
"РазрешитьЧтениеИзменение
|ГДЕ
|      ЗначениеРазрешено(Организация)
|    И ЗначениеРазрешено(Партнер) ";
```

Разработка RLS в БСП 3.0.1 в новом формате

- Описания синтаксиса нового формата ограничения доступа приведено в документации к БСП 3.0.1
- Инструмент разработчика **УправлениеДоступом.epf** теперь позволяет следующее.
  - С помощью вкладки **Разработка ограничения доступа** можно отладить синтаксис ограничения доступа в новом формате.
  - С помощью вкладки **Контроль изменения текстов RLS** можно сравнить тексты RLS текущей конфигурации с текстами, сохраненными при предыдущем сравнении, или с текстами указанной (старой) конфигурации.

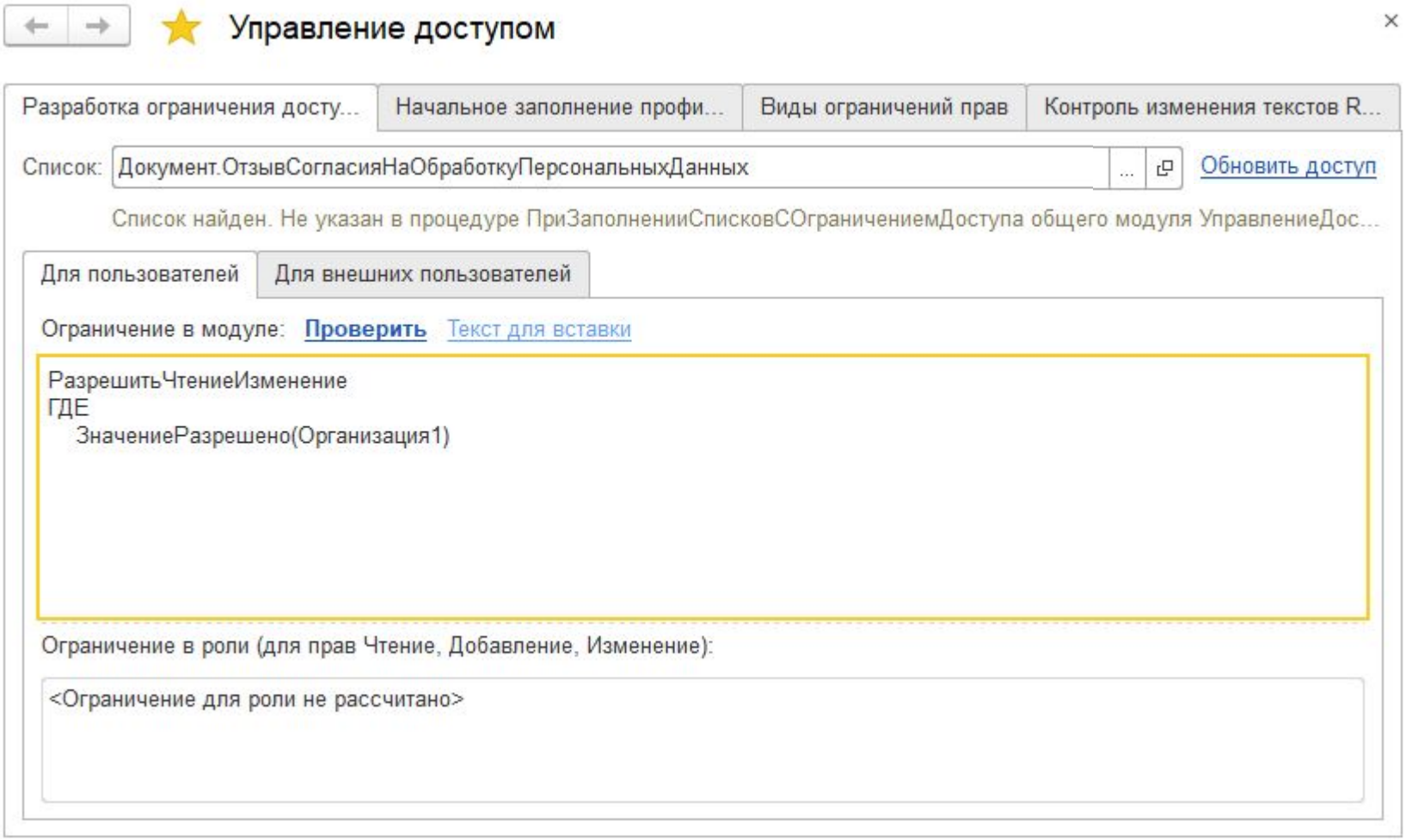
Отладка синтаксиса ограничения доступа в новом формате БСП 3.0

- Выбор таблицы для разработки ограничения



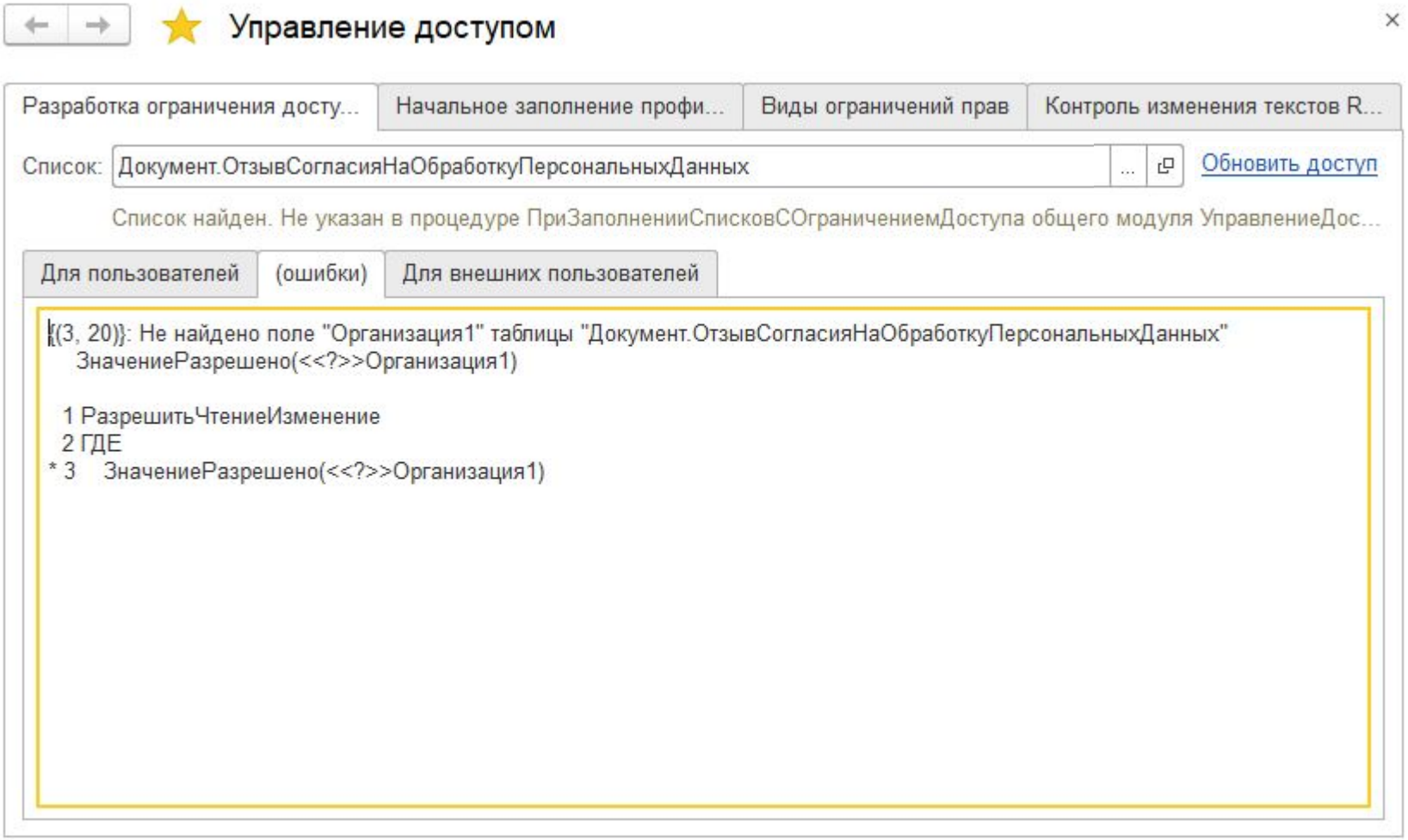
Отладка синтаксиса ограничения доступа в новом формате БСП 3.0

- Ввод ограничения (можно скопировать имеющееся).



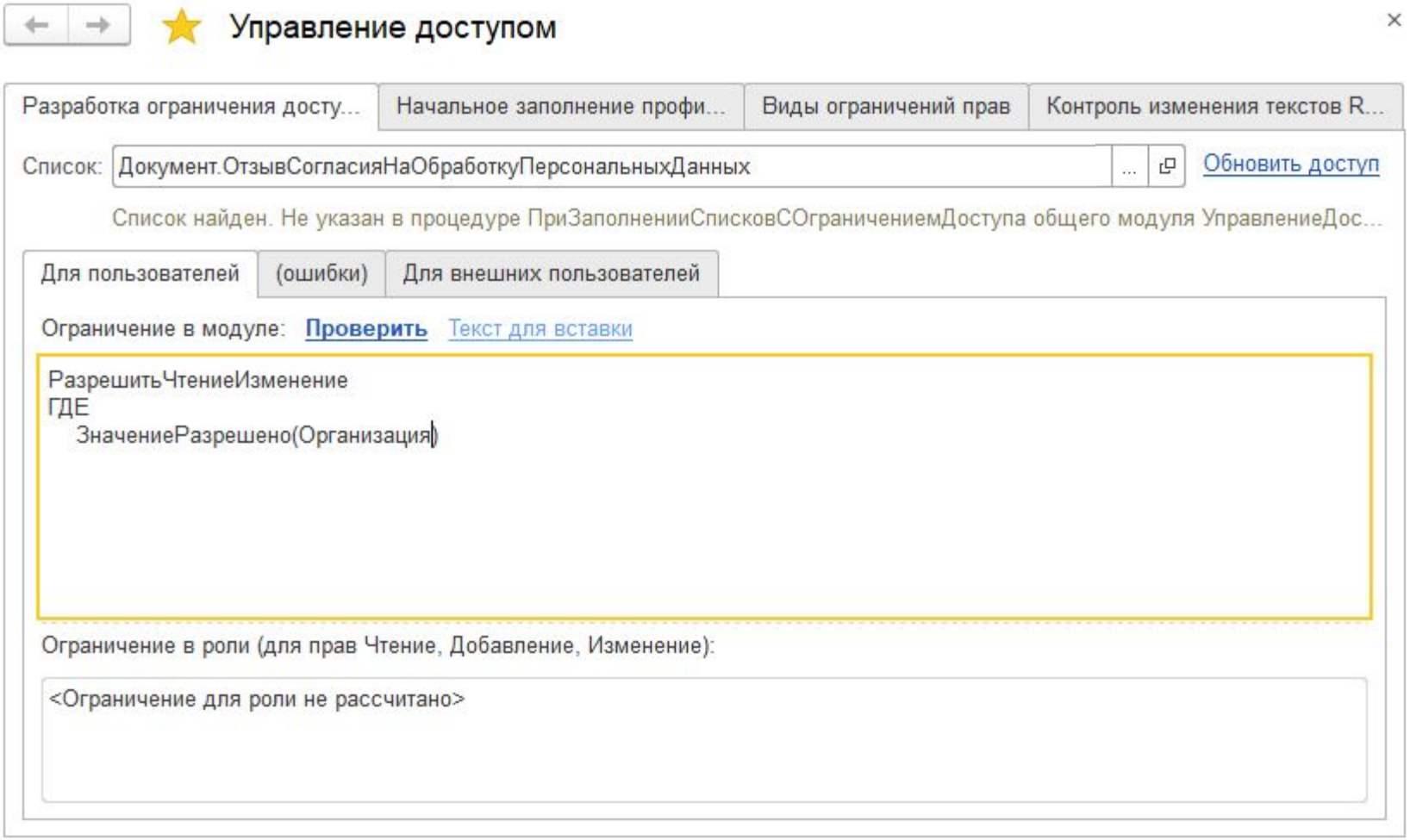
Отладка синтаксиса ограничения доступа в новом формате БСП 3.0

- Анализ найденных ошибок.



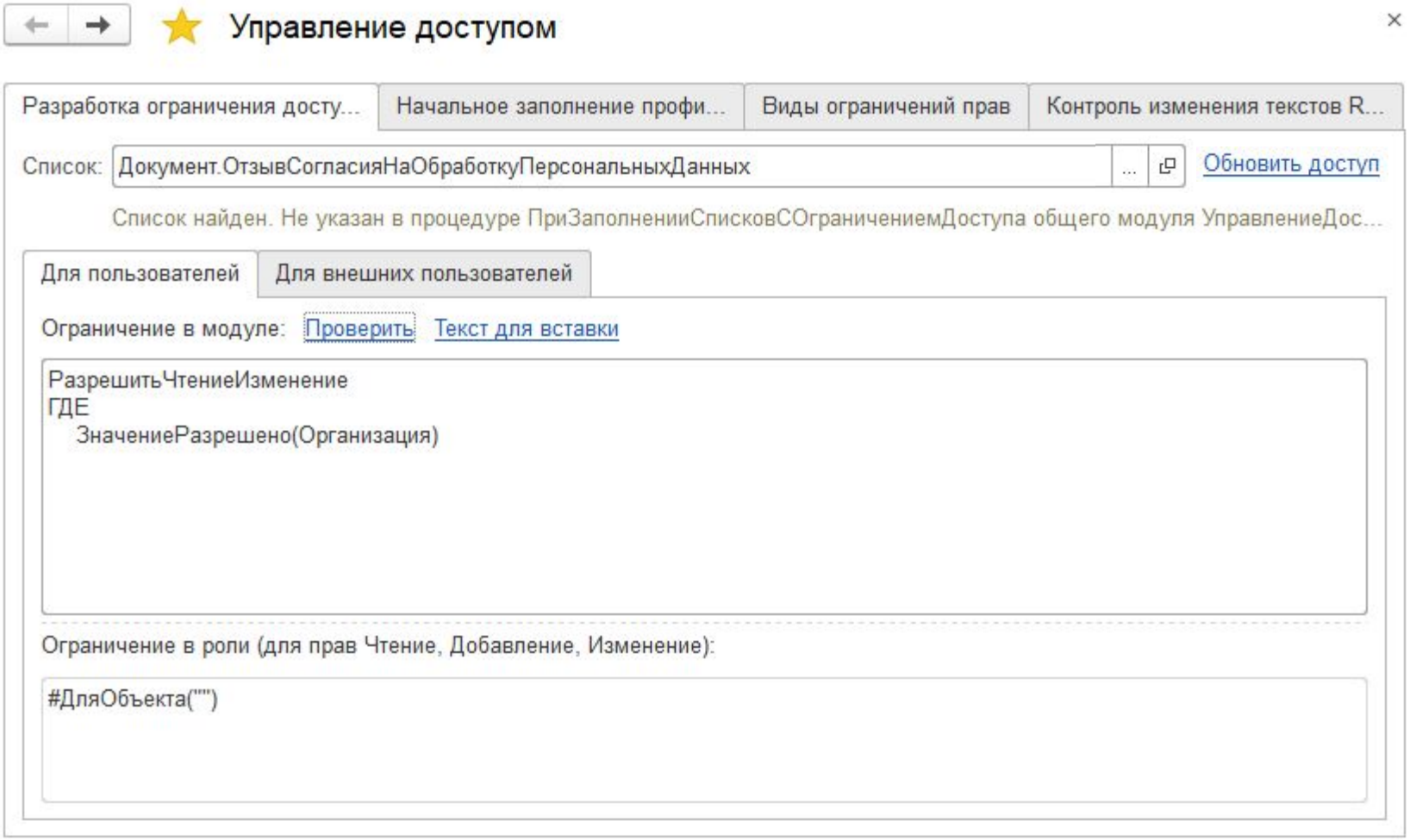
Отладка синтаксиса ограничения доступа в новом формате БСП 3.0

- Исправление найденных ошибок.



Отладка синтаксиса ограничения доступа в новом формате БСП 3.0

- Перенос в конфигурацию (кнопка Текст для вставки).



Отладка синтаксиса ограничения доступа в новом формате БСП 3.0

- Перенос в конфигурацию.

Тексты для вставки в модуль и в роли

```
1. В процедуру ПриЗаполненииСписковСОграничениемДоступа
   общего модуля УправлениеДоступомПереопределяемый добавить строку:

    Списки.Вставить(Метаданные.Документы.ОтзывСогласияНаОбработкуПерсональныхДанных, Истина);

2. В модуле менеджера объекта метаданных Документы.ОтзывСогласияНаОбработкуПерсональныхДанных вста

#Если Сервер Или ТолстыйКлиентОбычноеПриложение Или ВнешнееСоединение Тогда
#Область ПрограммныйИнтерфейс
#Область ДляВызоваИзДругихПодсистем
// СтандартныеПодсистемы.УправлениеДоступом

// См. УправлениеДоступомПереопределяемый.ПриЗаполненииСписковСОграничениемДоступа.
Процедура ПриЗаполненииОграниченияДоступа(Ограничение) Экспорт

    Ограничение.Текст =
    "РазрешитьЧтениеИзменение
    |ГДЕ
    |   ЗначениеРазрешено(Организация)";

КонецПроцедуры

// Конец СтандартныеПодсистемы.УправлениеДоступом
#КонецОбласти
#КонецОбласти
#КонецЕсли

3. В процедуре ПриЧтенииНаСервере формы элемента данных (если есть)
   следует сделать вставку кода (для библиотек проверка подсистемы обязательна):
```

Отладка синтаксиса ограничения доступа в новом формате БСП 3.0

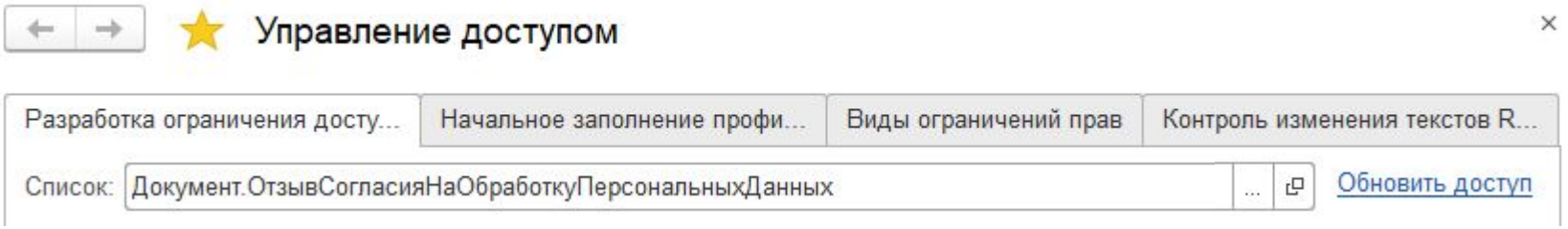
- Перенос в конфигурацию.

Тексты для вставки в модуль и в роли

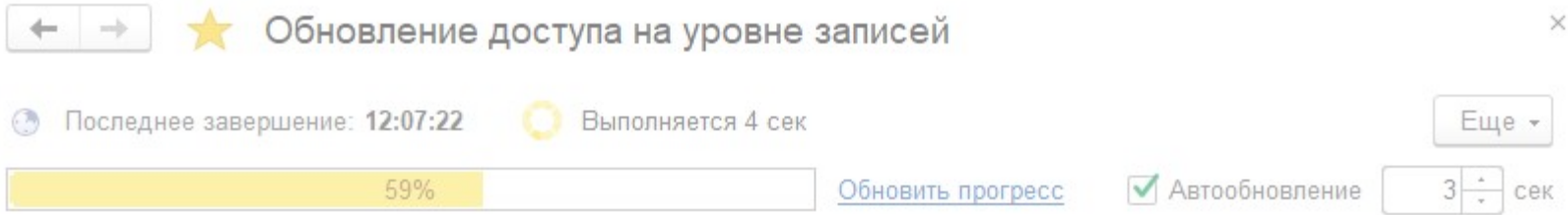
```
// СтандартныеПодсистемы.УправлениеДоступом
Если ОбщегоНазначения.ПодсистемаСуществует("СтандартныеПодсистемы.УправлениеДоступом") Тогда
    МодульУправлениеДоступом = ОбщегоНазначения.ОбщийМодуль("УправлениеДоступом");
    МодульУправлениеДоступом.ПриЧтенииНаСервере(ЭтотОбъект, ТекущийОбъект);
КонецЕсли;
// Конец СтандартныеПодсистемы.УправлениеДоступом

4. Запустить отчет ПроверкаВнедренияБСП.epf в режиме исправления с отбором по подсистеме
   Управление доступом, чтобы проверить и обновить внедрение после изменения текста ограничения.

   Либо обновить внедрение вручную:
   - в роли с назначением для пользователей на права Чтение, Добавление, Изменение
     объекта метаданных Документы.ОтзывСогласияНаОбработкуПерсональныхДанных установить ограничен
     (и добавить соответствующий шаблон ограничения, если его еще нет в роли):

     #ДляОбъекта("")

   - в роли с назначением для внешних пользователей на права Чтение, Добавление, Изменение
     объекта метаданных Документы.ОтзывСогласияНаОбработкуПерсональныхДанных установить ограничен
     (и добавить соответствующий шаблон ограничения, если его еще нет в роли):

     <Очистить ограничение, если указано и удалить шаблон, если не используется в роли>

   - в определяемый тип ВладелецЗначенийКлючейДоступа добавить типы:
       - ДокументСсылка.ОтзывСогласияНаОбработкуПерсональныхДанных

   - в определяемый тип ВладелецЗначенийКлючейДоступаДокумент добавить типы:
       - ДокументОбъект.ОтзывСогласияНаОбработкуПерсональныхДанных
```

Отладка синтаксиса ограничения доступа в новом формате БСП 3.0

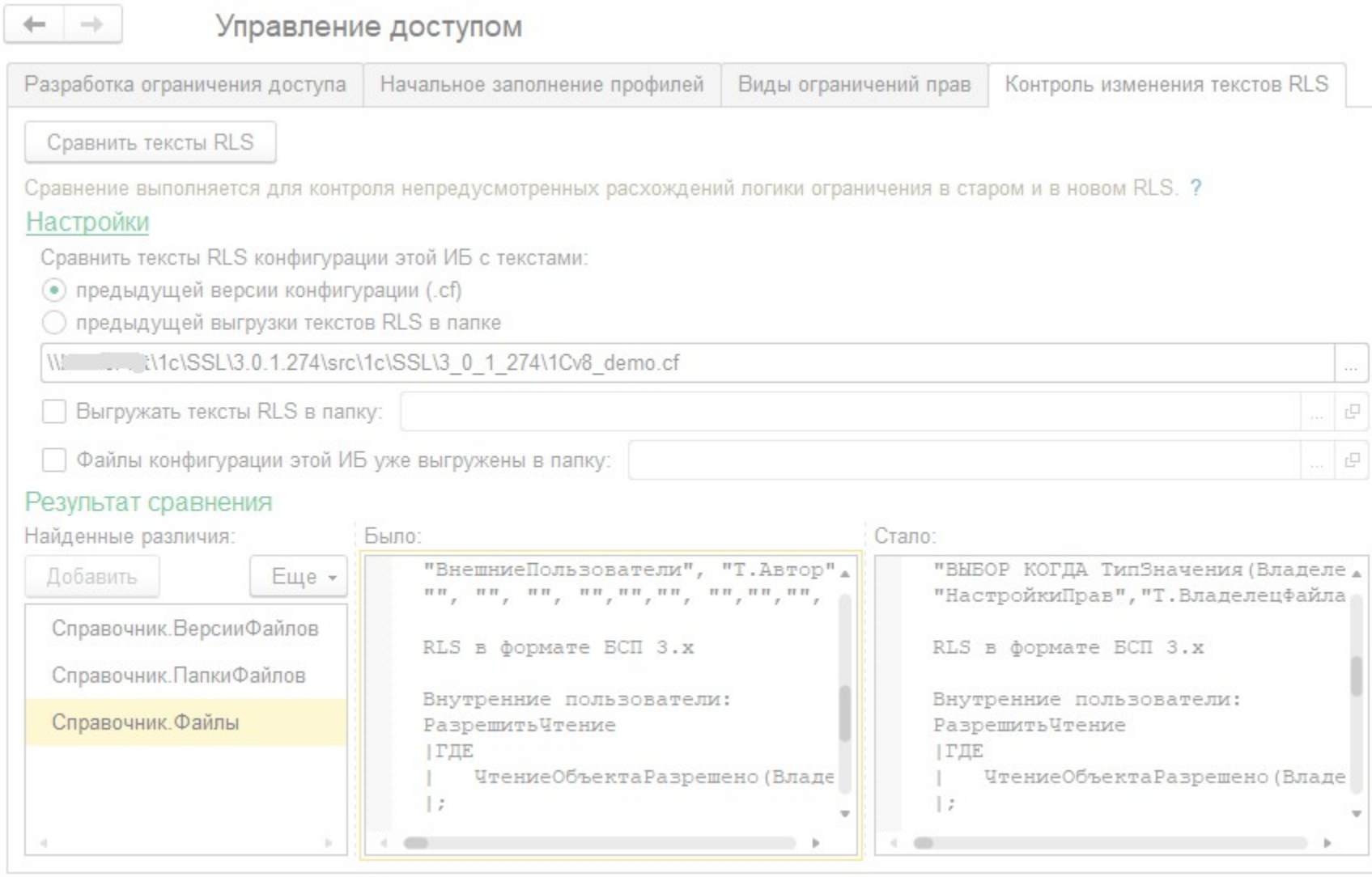
- Проверка разработанного ограничения в режиме **1С:Предприятия**.
  - Добавить роль с правами на документ в профиль и настроить группу доступа, если это не было сделано ранее.
  - Войти под администратором, открыть инструмент разработчика и нажать **Обновить доступ**:



  - После завершения обновления можно запустить сеанс под пользователем с RLS и посмотреть разрешенные документы.



Анализ изменений в текстах RLS



Новый RLS в БСП 3.0: быстрее, проще и перспективней

Спасибо за внимание!

Докладчик
Должность