ДЕПАРТАМЕНТ ПО РЕГУЛИРОВАНИЮ КОНТРАКТНОЙ СИСТЕМЫ КРАСНОДАРСКОГО КРАЯ

П Р И К А З

от 25.08.2023 № 91

г. Краснодар

О внесении изменений в приказ департамента по регулированию контрактной системы Краснодарского края от 3 февраля 2020 г. № 11 «Об утверждении Регламента работы региональной информационной системы Краснодарского края, используемой в сфере закупок для обеспечения государственных и муниципальных нужд»

В соответствии с пунктом 1.4 Порядка функционирования и использования региональной информационной системы в сфере закупок Краснодарского края, утвержденного постановлением главы администрации (губернатора) Краснодарского края от 19 января 2016 г. № 7 «Об утверждении Порядка функционирования и использования региональной информационной системы в сфере закупок Краснодарского края» п р и к а з ы в а ю:

1. Внести в приказ департамента по регулированию контрактной системы Краснодарского края от 3 февраля 2020 г. № 11 «Об утверждении Регламента работы региональной информационной системы Краснодарского края, используемой в сфере закупок для обеспечения государственных и муниципальных нужд» следующие изменения:

в приложении 1:

пункты 2-4 изложить в следующей редакции:

«2. Регламент определяет лиц, зарегистрированных в Системе и имеющих доступ к информационным ресурсам Системы в соответствии с назначенными правами (далее – пользователи Системы), устанавливает порядок формирования, размещения, обработки, хранения и представления информации, предусмотренной Федеральным законом от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» (далее – Закон № 44-ФЗ), Федеральным законом от 18 июля 2011 г. № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц» (далее – Закон № 223-ФЗ) и принятыми в соответствии с ними нормативными актами.

3. Система создана в соответствии с положениями части 9 статьи 4 Закона № 44-ФЗ, части 24 статьи 4 Закона № 223-ФЗ и в соответствии с едиными требованиями к региональным и муниципальным информационным

системам в сфере закупок, утвержденными Постановлением Правительства Российской Федерации от 27 января 2022 г. № 60 «О мерах по информационному обеспечению контрактной системы в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд, по организации в ней документооборота, о внесении изменений в некоторые акты Правительства Российской Федерации и признании утратившими силу актов и отдельных положений актов Правительства Российской Федерации».

4. Система разработана с целью автоматизации процессов размещения, координации и контроля над размещением государственных и муниципальных закупок, а также закупок отдельными видами юридических лиц, мониторинга закупок товаров, работ и услуг для нужд Краснодарского края, подготовки сведений о контрактах, договорах, контроля за соблюдением законодательства Российской Федерации и иных нормативных правовых актов о контрактной системе в сфере закупок, о закупках отдельными видами юридических лиц.»;

приложение 2 к Регламенту работы региональной информационной системы Краснодарского края, используемой в сфере закупок для обеспечения государственных и муниципальных нужд, изложить в новой редакции согласно приложению 1 к настоящему приказу;

приложение 3 к Регламенту работы региональной информационной системы Краснодарского края, используемой в сфере закупок для обеспечения государственных и муниципальных нужд, изложить в новой редакции согласно приложению 2 к настоящему приказу.

2. Отделу информационно-аналитического сопровождения (Лабунец В.С.) обеспечить размещение (опубликование) настоящего приказа на официальном сайте департамента по регулирования контрактной системы Краснодарского края в информационно-телекоммуникационной сети «Интернет» www.drcs.krasnodar.ru в подразделе «Приказы департамента», «База НПА» раздела «Документы».

3. Приказ вступает в силу со дня его подписания.

Руководитель департамента А.В. Милановић

Приложение 1
к приказу департамента по
регулированию контрактной системы
Краснодарского края
от 25.08.2023 № 91

«Приложение 2

к Регламенту работы региональной
информационной системы
Краснодарского края,
используемой в сфере
закупок для обеспечения
государственных и муниципальных нужд

РУКОВОДСТВО АДМИНИСТРАТОРА
региональной информационной системы Краснодарского края, используемой в сфере закупок для обеспечения государственных и муниципальных нужд

Перечень терминов и сокращений

В настоящем документе применены следующие термины и сокращения с соответствующими определениями, представленные в Таблице 1.

Таблица 1

Термины и определения

Термин	Определение
Автокомплит	Функция в программах, предусматривающих интерактивный ввод текста (редакторы, оболочки командной строки, браузеры и т. д.) по дополнению текста по введённой его части. В поле по введенным значениям срабатывает автоматический поиск по справочнику. Пользователь начинает вводить запрос в строку поиска, а система показывает ему найденные совпадения
БД	База данных
БИК	Уникальный идентификатор банка
ВДК	Внутридокументные контроли
ГРБС	Главный распорядитель бюджетных средств

1	2
Грид	Определение, описание, изображение какого-либо объекта или процесса внутри самого этого объекта или процесса, то есть ситуация, когда объект является частью самого себя. В программировании рекурсия — вызов функции (процедуры) из неё же самой, непосредственно (простая рекурсия) или через другие функции (сложная или косвенная рекурсия)
ЕИС	Единая информационная система в сфере закупок
Закон № 44-ФЗ	Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»
Закон № 223-ФЗ	Федеральный закон от 18 июля 2011 г. № 223-ФЗ «О закупке товаров, работ, услуг отдельными видами юридических лиц»
ИНН	Индивидуальный номер налогоплательщика
Исполнитель	Юридическое лицо или физическое лицо, в том числе зарегистрированное в качестве индивидуального предпринимателя, определенное в качестве исполнителя оказания услуг по сопровождению и технической поддержке Системы
КУ	Казенное учреждение
Маппинг	Определение соответствия информации между двумя разными семантиками как одного объекта, так и нескольких. Настройка соответствий
МДК	Междокументные контроли
МО	Муниципальное образование
ОВ	Органы власти
ОКТМО	Общероссийский классификатор территорий муниципальных образований
ОКФС	Общероссийский классификатор форм собственности
ОМСУ	Органы местного самоуправления
Оператор	Департамент по регулированию контрактной системы Краснодарского края
ОС	Операционная система
ПБС	Получатель бюджетных средств
ПК	Программный комплекс
ПК «НСИ»	Программный комплекс «Нормативно-справочная информация»
РБС	Распорядитель бюджетных средств

1	2
Рекурсия	Поля в интерфейсе, табличное представление
РМ	Рабочее место
РФ	Российская Федерация
Система	Региональная информационная система Краснодарского края, используемая в сфере закупок для обеспечения государственных и муниципальных нужд
СУБД	Система управления базой данных
ФО	Финансовый орган
ЦБ	Централизованная бухгалтерия
ЦИОГВ	Центральный исполнительный орган государственной власти
ЦСР	Код классификации целевых статей расходов бюджетов
ЭП	Электронная подпись
HID	Полностью hierarchyId – скрытое системное поле для иерархических справочников. Показывает иерархию в дереве.
Web-исполнение	Решение, предназначенное для комплексной автоматизации деятельности органов государственной власти, органов местного самоуправления, государственных и муниципальных учреждений, в рамках процессов исполнения бюджета с применением передовых web-технологий
UUID	Уникальный идентификатор

1. Введение

1.1. Область применения

Региональная информационная система Краснодарского края, используется в сфере закупок для обеспечения государственных и муниципальных нужд, функционирует на базе программного обеспечения «ПК «Региональная контрактная система» (в части автоматизации процесса закупок в соответствии с Законом № 44-ФЗ и процесса закупок товаров, работ, услуг отдельными видами юридических лиц в соответствии с Законом № 223-ФЗ).

1.2. Краткое описание возможностей

Система автоматизирует составляющие процесса закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд Краснодарского края в соответствии с Законом № 44-ФЗ:

планирование закупок, которое осуществляется исходя из целей осуществления закупок посредством формирования, утверждения и ведения планов-графиков закупок;

формирование закупок всеми способами определения поставщиков (подрядчиков, исполнителей), в том числе при участии уполномоченного органа и уполномоченного учреждения, включая проведение совместных конкурсов и аукционов;

формирование извещений о закупках, шаблонов документаций, размещение информации в ЕИС, контроль размещаемой в ЕИС информации на соответствие законодательству о контрактной системе в сфере закупок;

подготовку сведений о контрактах в соответствии с требованиями законодательства о контрактной системе в сфере закупок, размещение сведений о контрактах (их изменении) в реестре контрактов в ЕИС, подготовка бюджетных обязательств для постановки на учет, интеграция с системой автоматизации бюджетного процесса;

учет и контроль исполнения контрактов, формирование сведений об исполнении (прекращении действия) контракта в соответствии с требованиями законодательства о контрактной системе в сфере закупок, размещение сведений о контрактах (их изменении) в реестре контрактов в ЕИС, учет исполнения и оплаты бюджетных обязательств, автоматизация начисления штрафов и неустоек по несвоевременному исполнению контрактов, интеграция с системой автоматизации бюджетного процесса;

аналитику и оценку эффективности расходования бюджетных средств, мониторинг цен и формирование статистической и аналитической отчетности, обеспечение возможности всестороннего экономического анализа функционирования обеспечения закупок с использованием как регламентированной, так и нерегламентированной отчетности.

Система автоматизирует составляющие процесса закупок товаров, работ, услуг отдельных видов юридических лиц в соответствии с Законом № 223-ФЗ:

планирование закупок, которое осуществляется посредством формирования, утверждения и ведения планов закупки;

формирование закупок, осуществляемых способами закупок, предусмотренными Законом № 223-ФЗ и положениями о закупке отдельных видов юридических лиц, в том числе проведение совместных торгов;

формирование извещений об осуществлении закупки, контроль информации о закупке на соответствие законодательству, размещение информации о закупке в ЕИС;

подготовку сведений о договорах в соответствии с требованиями законодательства в сфере закупок, размещение информации в реестре договоров в ЕИС, подготовку бюджетных обязательств для постановки на учет, интеграцию с системой автоматизации бюджетного процесса;

учет и контроль исполнения договоров, формирование сведений об исполнении (расторжении) договора в соответствии с требованиями законодательства, размещение информации о договоре (их изменении) в реестре договоров в ЕИС, учет исполнения и оплаты бюджетных обязательств, интеграцию с системой автоматизации бюджетного процесса.

Требования к оборудованию сервера СУБД, сервера приложений и файлового сервера представлены в Таблице 2.

Таблица 2

Требования к оборудованию серверов

Вид оборудования	Аппаратное обеспечение
Сервер бизнес-логики	Аппаратная часть: – серверный процессор, ядер – 24; – оперативная память, Гб – 125; – жесткий диск (HDD), Тб – 1. Каналы связи: – пропускная способность канала связи не менее, Гбит/с – 1
Сервер СУБД	Аппаратная часть: – серверный процессор, ядер – 32; – оперативная память, Гб – 108; – жесткий диск (HDD), Тб – 1,6. Каналы связи: – пропускная способность канала связи не менее, Гбит/с – 1
Сервер репликации СУБД	Аппаратная часть: – серверный процессор, ядер – 12; – оперативная память, Гб – 39; – жесткий диск (HDD)Тб – 1. Каналы связи: – пропускная способность канала связи не менее, Гбит/с – 1
Сервер приложенных файлов	Аппаратная часть: – серверный процессор, ядер – 6; – оперативная память, Гб – 12; – жесткий диск (HDD), Тб – 14. аналы связи: – пропускная способность канала связи не менее, Гбит/с – 1
Сервер открытой части	Аппаратная часть: – серверный процессор, ядер – 16; – оперативная память, Гб – 20; – жесткий диск (HDD), Гб – 512. Каналы связи: пропускная способность канала связи не менее, Гбит/с – 1

1.3. Уровень подготовки администратора

Администраторы Системы должны обладать следующими навыками:

навыки в работе с персональным компьютером;

навыки в работе с Web-браузером MozillaFirefox, GoogleChrome, пакетом MS Office;

навыки настройки программного обеспечения;

навыки функционального администрирования программного обеспечения;

базовые знания ОС Linux: установка ОС и приложений, запуск и остановка сервисов, операции с файловой системой;

базовые знания с СУБД: запуск, остановка, резервное копирование.

2. Условия применения

Система должна включать следующие программные компоненты:

сервер СУБД;

сервер приложений (сервер среднего звена);

файловый сервер.

В качестве операционной системы для развертывания программных компонентов должна использоваться ОС AstraLinux Special Edition.

В качестве платформы сервера приложений должен использоваться JBoss (WildFly8.2.1 и выше).

В качестве сервера СУБД должен использоваться PostgreSQL 14.5 (Debian 14.5-1.pgdg90+1) on x86_64-pc-linux-gnu, compiled by gcc (Debian 6.3.0-18+deb9u1) 6.3.0 20170516, 64-bit) и выше.

СУБД, сервер приложений и файловый сервер должны быть развернуты каждый на своем хосте, удовлетворяющем соответствующим уточненным требованиям к характеристикам оборудования в соответствии с Таблицей 2.

Все сервера должны быть размещены в локальной сети и объединены высокоскоростным сетевым соединением без сетевого экрана. Сервер СУБД должен иметь возможность обрабатывать входящие подключения, поступающие от сервера приложений. Сервер приложений должен иметь возможность обрабатывать входящие подключения, поступающие от клиентов из сети Интернет по следующим портам:

2 – для удаленного управления сервером;

8080 – для подключения пользователей к приложению.

3. Подготовка к работе

3.1. Состав и содержание дистрибутивного носителя данных

Отсутствует.

3.2. Порядок загрузки данных и программ

Предварительная подготовка производится перед развертыванием Системы.

На сервере СУБД:

— должен быть установлен PostgreSQL 14.5 и выше;

— должна быть создана отдельная роль с уникальным именем для олицетворения сервера среднего звена Системы; допускается использовать существующую роль;
— должна быть создана пустая схема базы данных с уникальным именем, владельцем которой должна быть установлена роль, олицетворяющая сервер среднего звена.

На сервере среднего звена (сервере web-приложений):

— должен быть установлен bellsoft-java11-amd64 или Oracle JDK 1.8 x64;
— переменная среды JAVA_HOME должна содержать полный абсолютный путь к корневой папке установленного JDK;
— должна быть создана роль распространения (рекомендуется jboss), от имени которой будет функционировать сервер среднего звена;
— должна быть создана корневая папка для приложений Системы (рекомендуется /var/lib/jboss/), для которой пользователь, от имени которого будет функционировать сервер среднего звена, должен быть установлен в качестве владельца (owner).

3.3. Установка и настройка сервера среднего звена

Установочный код Системы поставляется на электронном носителе, содержащем все необходимые компоненты для развертывания сервера среднего звена, совмещенного с сервером web-приложений.

Установка Системы и дальнейшие действия по настройке выполняются от имени учетной записи, предназначенной для функционирования сервера среднего звена.

В корневой папке приложений (рекомендуется /var/lib/jboss/) необходимо создать папку для Системы (рекомендуется ./rcs/), далее {$install.home}.

Установочный код Системы должен быть скопирован с электронного носителя в {$install.home}.

По завершению копирования инсталляционного пакета необходимо выполнить настройку Системы согласно п.3.5

Выполнить развертывание инсталляционного пакета командой {$install.home}/install.sh. В случае успешного завершения развертывания будет выдано сообщение «BUILD SUCCESSFUL» с указанием общего времени развертывания. Для сервера среднего звена требуемых характеристик, указанных в таблице**Ошибка! Источник ссылки не найден.**,время развертывания составляет 7-10 минут.

При наличии критических ошибок: таймауте, завершении процесса развертывания с сообщением «BUILD FAILED», процесс развертывания необходимо прекратить и обратиться к поставщику программного обеспечения с предоставлением лог-файлов, содержащих ошибки.

После развертывания дистрибутива необходимо выполнить создание метаданных схемы базы данных путем выполнения команды {$install.home}/import.sh.

После создания метаданных схемы базы данных необходимо выполнить проверку Системы.

3.5. Настройка Системы

В файле настроек {$install.home}/application.properties необходимо установить значения параметров, указанные в таблице 3, путем указания имени параметра и его значения через знак «=».

Таблица 3– Параметры настройки конфигурации сервера среднего звена «application.properties»

Имя параметра	Значение параметра	Комментарии
psql.dbname	Имя схемы базы данных	
psql.host	IP-адрес сервера базы данных	если PostrgeSQL развернут на сервере с адресом порта, отличным от стандартного (5432), в адресе сервера базы данных необходимо также указывать номер порта XXX.XXX.XXX.XXX:PPPPP; при использовании PostrgeSQL на стандартном порте, указывать порт в адресе сервера базы данных не надо
psql.user	Имя роли для олицетворения сервера среднего звена на сервере базы данных	
psql.password	Пароль роли для олицетворения сервера среднего звена на сервере базы данных	
system.password	Пароль для системной учетной записи «system»	Встроенная системная учетная запись используется для первичной регистрации пользователей и выполнения через пользовательский интерфейс и сервис взаимодействия действий, требующих повышенных привилегий

Если изменение параметров конфигурации выполняется при запущенном сервере Системы, для вступления параметров в силу сервер должен быть остановлен и запущен заново.

Необходимо обеспечить достаточную сложность пароля системной учетной записи, поскольку учетная запись имеет неограниченные полномочия в Системе.

3.6. Запуск и остановка Системы

Запуск и остановка системы осуществляются от имени роли, созданной для олицетворения сервера среднего звена.

Для запуска системы необходимо выполнить команду {$install.home}/krista-updater/krupdjboss.start. Для сервера среднего звена требуемых характеристик, указанных в таблице**Ошибка! Источник ссылки не найден.**, время запуска приложения может составлять 7-10 минут в зависимости от объема хранимых данных.

В результате успешного запуска приложения выполнение команды будет завершено выдачей сообщения «BUILD SUCCESS».

В результате неуспешного запуска приложения выполнение команды будет завершено выдачей сообщения «BUILD FAILED».

В результате таймаута запуска приложения выполнение команды будет завершено без выдачи сообщения через 10 минут после подачи команды.

При неуспешном запуске или таймауте запуска ошибки, связанные с неуспехом запуска, могут быть получены в лог-файле по пути {$install.home}/jboss-bas-8.2.1.krista3/standalone/log/.

Для остановки Системы необходимо выполнить команду {$install.home}//krista-updater/krupdjboss.stop. Команда остановки не имеет таймаута. Если остановка приложения не выполнен в течение 10 минут, средствами операционной системы необходимо завершить процесс java и проверить лог-файл Системы по пути {$install.home}/jboss-bas-8.2.1.krista3/standalone/log/ на предмет наличия-отсутствия ошибок.

3.7. Критерии штатного функционирования

Пользовательский web-интерфейс Системы доступен при подключении по адресу http://localhost:8080/application/# с web-сервера или при удаленном подключении по имени сервера.

Программный интерфейс сервиса взаимодействия доступен при подключении по адресу http://localhost:8080/service/# с web-сервера или при удаленном подключении по имени сервера.

В лог-файлах {$intall.home}/jboss-bas-8.2.1.krista3/standalone/log/ отсутствуют записи ошибок уровня [fatal], [error], [severe].

Система должна функционировать непрерывно, за исключением периодов проведения профилактических и других работ, предусмотренных регламентом, а также устранения возникших нештатных ситуаций.

Система функционирует в следующих режимах:

— штатный режим;

— режим технического обслуживания;

— режим восстановления: после сбоя;

— режим восстановления: после критического отказа или аварии.

Основным режимом функционирования Системы является штатный режим. Штатный режим предусматривает непрерывную круглосуточную работу Системы в режиме 24x7x365 с учетом перерывов на техническое обслуживание.

Режим технического обслуживания предназначен для проведения запланированных работ по обслуживанию программных и аппаратных средств Системы и может сопровождаться частичной или полной недоступностью функциональности Системы. Необходимость и время проведения технического обслуживания согласовывается Заказчиком и Исполнителем не менее чем за 1 рабочий день до начала проведения работ.

Режим восстановления предназначен для проведения работ по обеспечению полной работоспособности Системы после сбоя, критического отказа или аварии.

4. Описание операций

4.5. Порядок восстановления работоспособности

При условии выполнения требований к аппаратному обеспечению, представленных в таблице2, и снижении эксплуатационных характеристик Системы (увеличение времени отклика Системы на команды пользователей, поданные посредством web-интерфейса Системы) необходимо выполнить останов и повторный пуск приложения.

Сведения о причинах отказа Системы могут быть получены в лог-файлах {$intall.home}/jboss-bas-8.2.1.krista18/standalone/log/.

При аварийном останове Системы необходимо выполнить проверку:

— работоспособности и доступности для среднего звена сервера СУБД;

— целостность и работоспособности java.

После восстановления работоспособности необходимых компонентов необходимо выполнить старт Системы.

4.6. Резервное копирование

Резервному копированию подлежит:

— СУБД;

— корневой каталог установки приложения {$install.home}.

Резервное копирование выполняется в целях восстановления работоспособности Системы в случае сбоев.

Резервное копирование должно выполняться путем архивации и копирования объектов резервного копирования на отдельный файловый сервер.

При выполнении восстановления резервных копий необходимо соблюдать соответствие версии резервной копии СУБД и версии сервера приложений. Не допускается восстанавливать СУБД на версию приложения среднего звена, если резервная копия СУБД была снята для другой версии приложения среднего звена. Соответствие версии резервной копии СУБД и версии сервера приложений определяется датой и временем резервных копий.

4.6.1. Резервное копирование сервера приложения

Резервное копирование папок etcи var/lib/jbossвыполняется:

— раз в неделю (в воскресенье): полное копирование;

— раз в день (с понедельника по субботу): инкрементальное копирование.

Хранение резервных копий папок должно выполняться не более чем двухнедельной давности.

Создание резервной копии выполняется с помощью bash-скрипта, который использует программы tar и gzip для создания файлов архива. Резервные копии хранятся в папке backup.

Восстановление из резервной копии должно выполняться путем восстановления объектов файловой Системы.

4.6.2. Резервное копирование сервера СУБД

Резервное копирование СУБД должно выполняться средствами оснастки СУБД (shellscript и pg_dump):

— раз в день (с понедельника по воскресенье): полное копирование.

Хранение резервных копий СУБД должно выполняться не более чем однонедельной давности.

Восстановление резервных копий СУБД производится средствами оснастки СУБД при остановленном сервере приложений.

4.7. Обновление Системы

Обновление Системы выполняется путем копирования новых версий компонентов в папку {$intall.home}/jboss-bas-8.2.1.krista18/standalone/development.

4.8. Регламентное обслуживание

Необходимо вручную или с помощью средств инструментального наблюдения, например, Системы мониторинга и отслеживания статусов разнообразных сервисов компьютерной сети, серверов и сетевого оборудования «Zabbix» контролировать наличие свободного места на диске установки {$install.home} не менее 20% от указанного в требованиях к аппаратному обеспечению. При необходимости следует выполнять очистку каталога лог-файлов приложения {$install.home}/jboss-bas-8.2.1.krista3/standalone/log/.

Вне зависимости от показателей текущих эксплуатационных характеристик не реже 1 раз в месяц необходимо выполнять останов и повторный пуск приложения с целью очистки файлового кэша.

5. Обеспечение безопасности

Выбор мер защиты информации для их реализации в информационной системе осуществляется в ходе проектирования системы защиты информации информационной системы в соответствии с техническим заданием на создание информационной системы и техническим заданием на создание системы защиты информации информационной системы.

6. Парольная аутентификация

6.1. Основные уязвимости

Парольная аутентификация – это процедура аутентификации пользователя с помощью логина/пароля. Пользователю создается учетная запись, которая активируется паролем. Далее пользователь для входа в систему использует свою пару логин/пароль.

Считается, что парольная аутентификация – это не лучший способ аутентификации и лучше использовать другие способы аутентификации. Однако парольная аутентификация на данный момент является основным и практически единственным способом аутентификации. Соответственно необходимо знать основные уязвимости для выработки способов защиты от этих уязвимостей.

Основные уязвимости:

— использование однофакторной аутентификации, основанной на долговременных паролях, потенциально уязвимо ввиду использования социотехники, внедрения клавиатурных шпионов, возможности перехвата и т.п.;
— предоставление информации о существовании/отсутствии логина может быть использовано злоумышленником для получения списка логинов путем подбора по словарю с использованием ботов;
— слабые пароли существенно упрощают задачу подбора пароля методом перебора (словарь + эвристика);
— отсутствие защиты от автоматизированного перебора паролей существенно упрощает задачу подбора даже относительно сложного пароля;
— использование незащищенных протоколов.

6.2. Направления защиты

6.2.1. Защита от перебора

Если злоумышленник пытается с помощью ботов, средств автоматизации подобрать пароль пользователя, то система должна препятствовать такому подбору. При этом с одной стороны должны обеспечиваться требования безопасности, с другой сохраняться удобства работы для честного пользователя.

Рассмотрим действия системы по защите от подбора паролей.

В системе ведется журнал попыток аутентификации для анализа признаков перебора паролей. Этот журнал доступен администратору безопасности на интерфейсе «Журнал попыток входа», показанный на рисунке 1. В системе ведется учет всех попыток входа: удачных и неудачных.

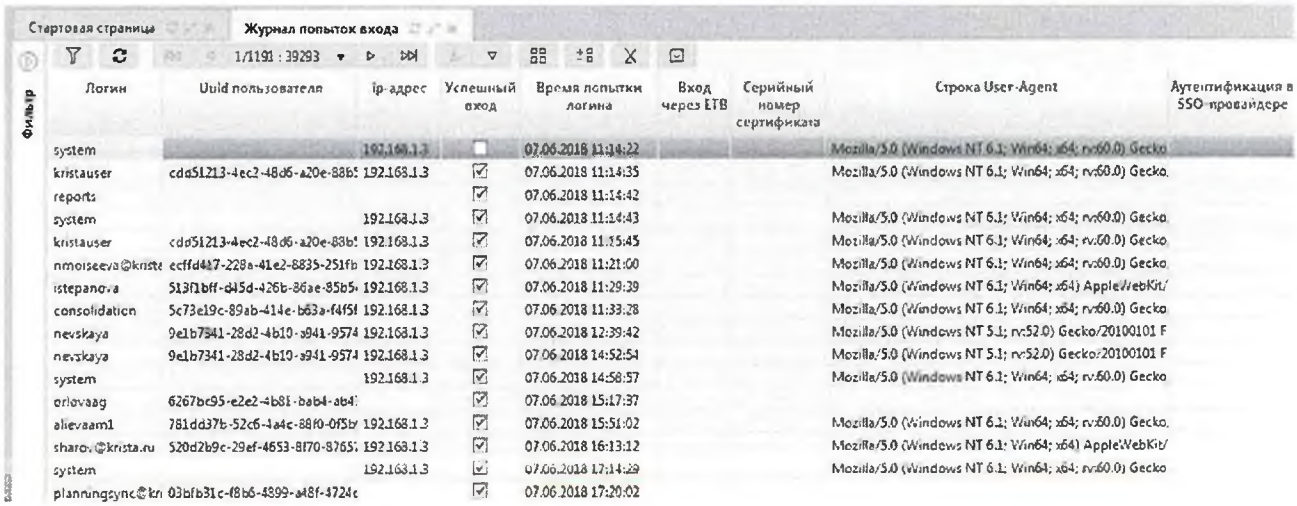


Рисунок 1 – Интерфейс «Журнал попыток входа»

В случае срабатывания контроля защиты от перебора, пользователь блокируется. Заблокированных пользователей администратор безопасности может увидеть на интерфейсе «Блокировки пользователей», представленный на рисунке 2.

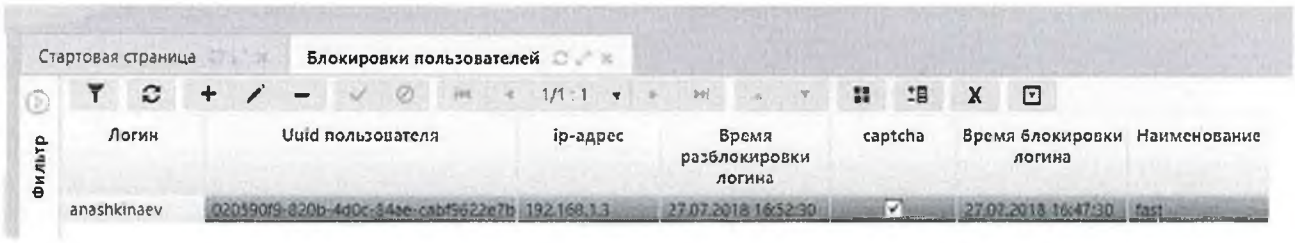


Рисунок 2 – Интерфейс «Блокировки пользователей»

Журнал ведется в разрезе ip-адресов, чтобы предотвратить блокировку честных пользователей. Когда злоумышленник, зная логин пользователя, пытается подобрать его пароль, система не должна блокировать честного пользователя, работающего под этим логином.

Для того, чтобы система заблокировала только злоумышленника, работающего с его уникального ip-адреса, в журнале попыток входа регистрируется ip-адрес, с которого был сделан запрос на аутентификацию. Система пытается заблокировать работу злоумышленника в разрезе ip, то есть блокируется вход под определенной учетной записью с определенногоip-адреса. Честный пользователь при этом пострадать не должен.

Особенностью блокировки паролей является то, что поддерживается несколько (обычно 2) уровней опасности, в зависимости от оценки вероятности попытки взлома пароля, которая определяется автоматически.

Если уровень опасности низкий, то применяется метод ввода капчи. То есть пользователь не блокируется, а дополнительно запрашивается подтверждение, что пользователь не является ботом. На рисунке 3 представлен пример использования капчи. То есть система за диагностировала низкий уровень опасности и включила капчу. В этом случае пользователь, который ввел несколько раз неуспешно пароль, должен будет при следующей попытке ввести еще и капчу правильно. При этом его учетная запись не будет заблокирована, и ему не нужно будет обращаться к администратору безопасности. Пользователь ввел капчу, вспомнил пароль – работает дальше без привлечения администратора.

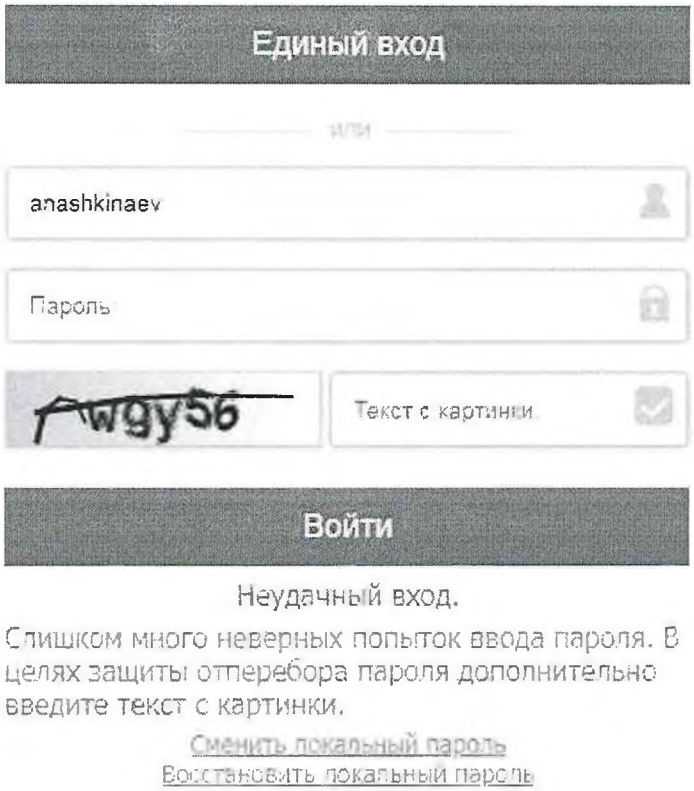


Рисунок 3 – Ввод капчи для защиты от перебора

– При высоком уровне опасности осуществляется физическая блокировка пользователя, работающего с данного ip.

В том случае, когда системой диагностирован высокий уровень опасности, когда идет явный перебор, большое число неверных попыток пароля, включается уже блокировка учетной записи. Пользователь видит сообщение, что данная учетная запись заблокирована до определенного времени, как показано на рисунке 4. Время блокировки может настраиваться.

Рисунок 4 – Блокировка пользователя

Администратор при этом видит факт блокировки пользователя в журнале блокировок пользователей, как было показано на рисунке 2.

Параметры, относящиеся к способу выделения уровней опасности, относятся в целом ко всему серверу и могут быть настроены только разработчиком или администратором сервера. Администратор один раз задает параметры этих уровней и после этого требуется перезапуск сервера. Пример настройки политик блокировки пользователей и пример настройки домена безопасности для поддержки политик блокировки представлены в конце документа.

После перезапуска сервера на основании настроек уровней опасности система при регистрации опасности включает капчу или блокировку.

6.2.2. Контроль сложности пароля

Обязательно при парольной аутентификации требуется контролировать сложность пароля. Пользователь не должен использовать простых паролей. То есть необходимо запретить пользователю указывать простые пароли.

Администратор безопасности определяет правила сложности. Система автоматически проверяет пароль на соответствие этим правилам. Если пароль слишком простой, то есть не подходит под правила сложности, то пользователь не может использовать этот пароль.

Параметры сложности пароля могут быть настроены через браузер глобальным администратором. Параметры сложности могут настраиваться в любое время, не требуют перезапуска сервера.

Настройки сложности пароля можно делать не для всех пользователей системы, а для пользователей конкретных бюджетов. Если определенный бюджет по каким-либо причинам требует более жесткие параметры безопасности, то это доступно для задания администратору безопасности.

Параметры настраиваются на интерфейсе «Редактор настроек» РМ «Администрирование» в разделе «Безопасность». Внешний вид раздела «Безопасность» интерфейса «Редактор настроек» представлен на рисунке5.

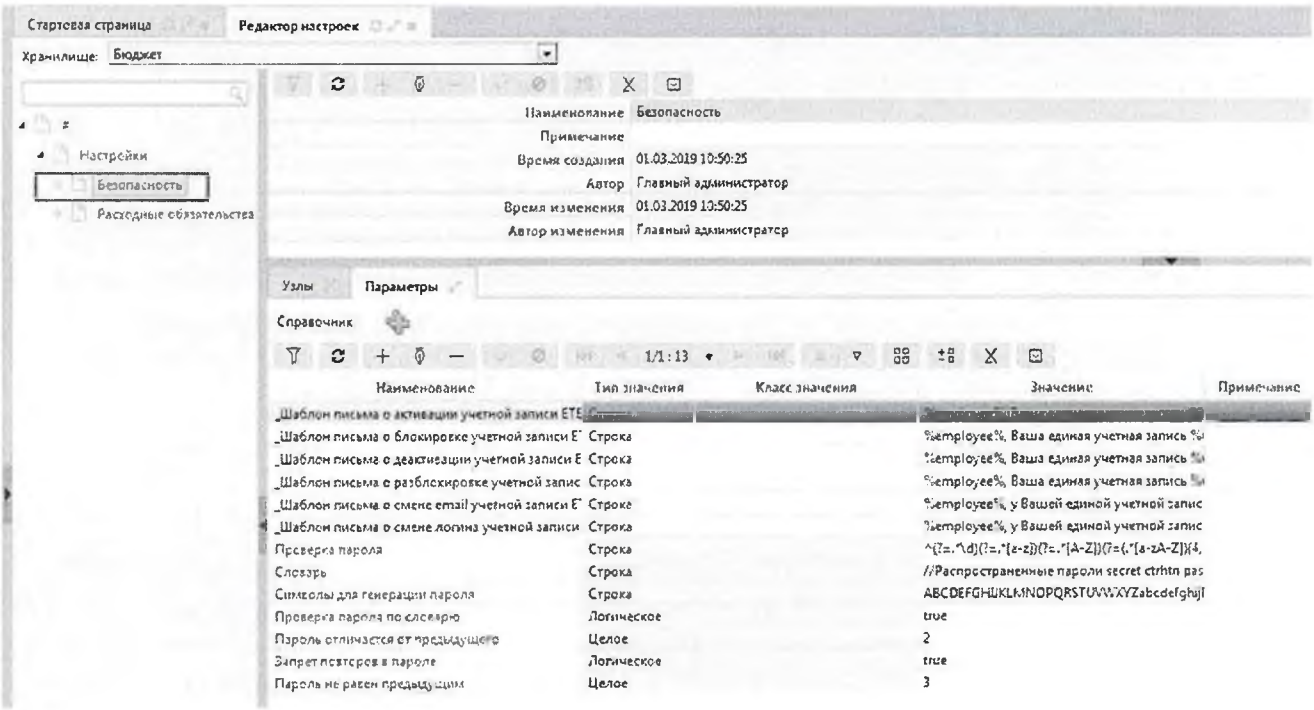


Рисунок 5 – Раздел «Безопасность» интерфейса «Редактор настроек»

В разделе «Безопасность» есть перечень параметров, которые глобальный администратор может перекрыть. Здесь используется принцип многоуровневости настроек. Администратор безопасности может работать с разными уровнями настроек. Администратор может работать с базовым уровнем, который общий для всех заказчиков. На этом уровне прописаны дефолтные значения всех параметров. А может работать на уровне конкретного региона. Уровень настроек задается в поле «Хранилище» в верхней части интерфейса «Редактор настроек».

После установки экземпляра системы на конкретный сервер, администратор может перекрыть значения по умолчанию. Администратору нужно перекрыть только необходимые для перекрытия значения. Остальные параметры остаются без изменения. Это достаточно удобно. То есть, система поставляется с включенной по умолчанию защитой с настройками по умолчанию. Администратор не тратит силы на включение этой защиты, так как она уже есть.

Настройка требуется, если политика безопасности региона отличается от стандартной. В этом случае настраивается политика безопасности в той части параметров, которые отличаются от стандартных параметров по умолчанию. В этом случае выбирается либо хранилище всего уровня, либо хранилище конкретного бюджета и там перекрываются необходимые параметры.

Перекрытие делается достаточно просто. Есть специальный функционал, который упрощает перекрытие настроек. Администратор безопасности может добавить настройку по кнопке «Добавить из родительского хранилища» из настроек более высокого уровня путем выбора из списка настроек, как показано на рисунке 6.

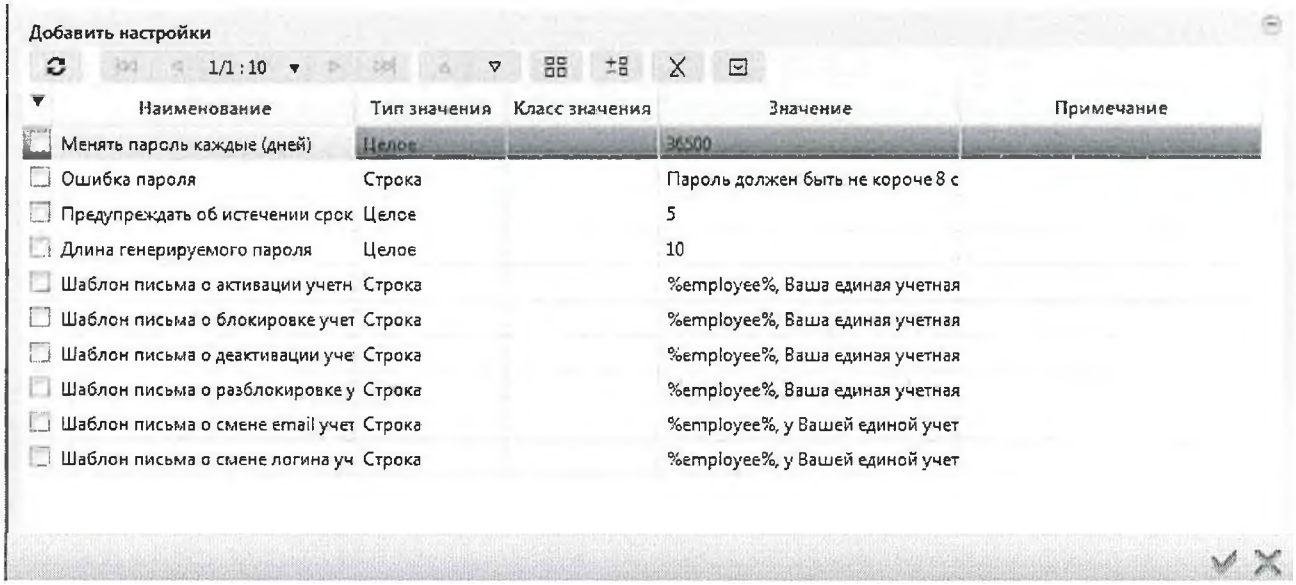


Рисунок 6 – Окно «Добавить настройки»

Система при этом выделит перекрытый параметр другим цветом и предоставит информацию о первоначальном значении и о новом значении. Администратор может всегда посмотреть, что он перекрыл: что было изначально и что стало после изменения.

Параметры сложности пароля, которые могут настраиваться администратором безопасности, представлены в таблице4.

Таблица 4 – Параметры сложности пароля

Параметр	Значение по умолчанию	Описание
Проверка пароля	^(?=.*\\d)(?=.*[a-z])(?=.*[A-Z])(?=(.*[a-zA-Z]){4,}).{8,}$	Проверка сложности пароля по регулярному выражению
Ошибка пароля	Текстовое описание требований регулярного выражения для пользователя	Пароль должен быть не короче 8 символов, содержать не менее 4х латинских букв в верхнем и нижнем регистре и хотя бы 1 цифру.
Запрет повторов в пароле	true	Регистр независимый контроль. Запрет повторяющихся подряд одинаковых символов (три и более раз) и последовательностей (длиной два символа и более).
Проверка пароля по словарю	true	Регистр независимый контроль. Перечисление запрещенных вхождений, определенных в словаре. Если такая последовательность окажется в пароле, то пароль будет считаться ненадежным. Запрет вхождения логина пользователя в пароль.
Словарь	Значения словаря в стандартной поставке представлены в конце документа	Перечисление запрещенных вхождений, разделенных переносом строки Можно расширить словарь. В стандартной поставке идет стандартный словарь и его можно расширять собственными запрещенными словами, например, аббревиатуры учреждений, министерства и т.д.
Пароль не равен предыдущим	3	Проверка на то, что хэш пароля не равен последним Nхэшам прошлых паролей этого пользователя. Необходима для того, чтобы пользователь при обязательной смене пароля не указывал тот пароль, который у него был в прошлом. Система сами пароли не хранит, а хранит только хэши паролей, и по хэшам проверяет, что пароль ранее использовался. Можно указать количество предыдущих паролей, с которыми не должно быть пересечений.

6.2.3. Генерация пароля

Пароль в системе может быть сгенерирован с помощью генератора паролей. Пользователю стандартно предлагается сгенерировать пароль, как показано на рисунке 7.

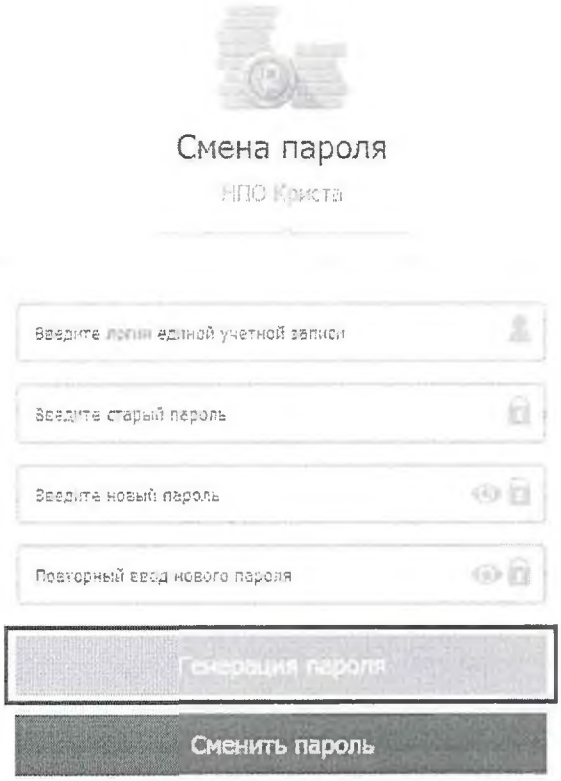


Рисунок 7 – Генерация пароля

Пароль генерируется всегда соответствующий политике безопасности.

Параметры для генерации пароля, так же, как и параметры сложности пароля, могут быть настроены через браузер глобальным администратором. Механизм администрирования параметров генерации полностью аналогичен механизму администрирования параметров сложности пароля.

Параметры для генерации пароля, которые могут настраиваться администратором безопасности, представлены в таблице 5.

Таблица 5 – Параметры для генерации пароля

Параметр	Значение по умолчанию	Описание
1	2	3
Длина генерируемого пароля	10	Длина генерируемого пароля

1	2	3
Символы для генерации пароля	ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+.@#%*&_	Символы для генерации пароля

6.2.4. Поддержка одноразовых паролей при активации учетных записей администратором

При парольной аутентификации так же используется подход с одноразовыми паролями. Администратор безопасности, чтобы не скомпрометировать пароль, может сам сгенерировать пароль, поставив галку «Одноразовый пароль».

В этом случае пользователь при входе в систему обязан будет сменить одноразовый пароль на свой пароль, который администратору уже неизвестен.

6.2.5. Администрирование периодичности смены паролей

Очень важная настройка – это контроль периодичности смены паролей для единых учетных записей.

В связи с ужесточением политики безопасности стали ставиться дополнительные ограничения, что пароль должен меняться с определенной периодичностью, например, раз в 3 месяца. Это система позволяет делать автоматически. Можно задать число дней, через которые пароль должен быть изменен. В качестве сервисной функции, можно задать возможность предупреждения пользователя об истечении срока действия пароля за указанное число дней. Пользователь будет получать сообщение, как показано на рисунке 8, что через столько дней его пароль истечет, чтобы для пользователя не было неожиданностью, когда он попытается войти в систему, а система выдаст ошибку.

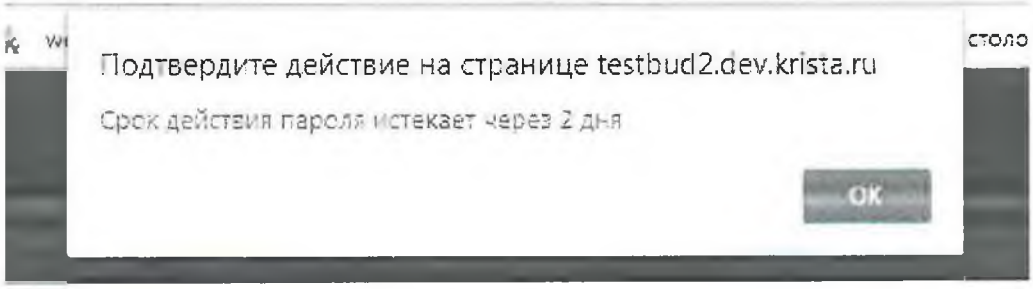


Рисунок 8 – Предупреждение об истечении срока действия пароля

Параметры смены паролей для единых учетных записей, которые могут настраиваться администратором безопасности, представлены в таблице6.

Таблица 6 – Параметры смены паролей для единых учетных записей

Параметр	Значение по умолчанию	Описание
Менять пароль каждые (дней)	Не задано	Длительность действия пароля в днях. На основании нее и даты последнего изменения пароля вычисляется время завершения действия пароля.
Предупреждать об истечении срока действия пароля за (дней)	Не задано	Влияет на формирование предупреждения при аутентификации. Предупреждение будет появляться, начиная с указанного числа дней до окончания времени завершения действия пароля.

6.2.6. Журнализация операций с паролями

Журнализация операций с паролями представлена на интерфейсе «Единые учетные записи» РМ «Управление пользователями», детализация «История обработки», как показано на рисунке 9.

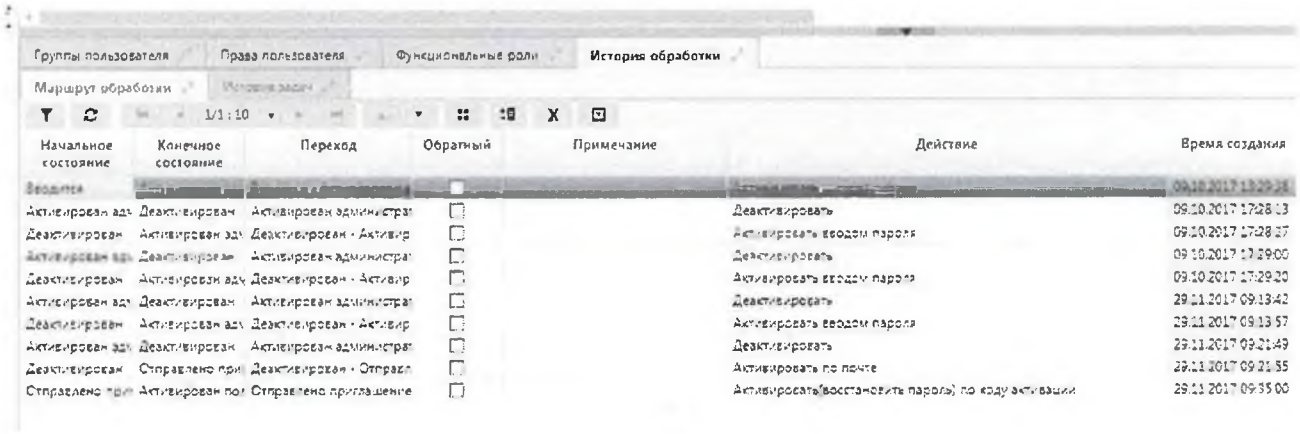


Рисунок 9 – Детализация «История обработки» интерфейса «Единые учетные записи»

Когда пользователь меняет пароль, администратор может это увидеть. Можно настроить и почтовые оповещения о наиболее важных событиях.

6.2.7. Использование защищенных протоколов

Важным направлением защиты является использование защищенных протоколов, препятствующих перехвату пароля. Если протокол незащищенный, то пароль тоже передается от пользователя к серверу в незащищенном виде.

Для передачи данных необходимо использовать защищенные протоколы httpsили vpn. Администратору необходимо обращать внимание, чтобы защищенные протоколы были не только от клиента к серверу, но и от клиента к серверу аутентификации. Допустим, если используется единая точка входа и основной сервер работает по https, а для аутентификации по единым учетным записям система перенаправляет на сервер аутентификации, то этот канал тоже должен быть защищен. Администратор должен это контролировать.

6.3. Рекомендации для обеспечения безопасности решений при использовании аутентификации по паролю

Рекомендации для обеспечения безопасности решений при использовании аутентификации по паролю:

- использовать https протокол вместо http;
- подключать в проекты политики блокировки ботов подбора паролей (реализовано в CommonUtils) с настройками, аналогичными настройкам в ПК «НСИ»;
- реализовывать контроль сложности паролей с настройками, аналогичными настройкам в ПК «НСИ» для единых учетных записей;
- реализовывать журнализацию операций с паролями (установка, изменение пароля, изменение почты) с возможностью оповещения пользователя – владельца учетной записи по почте;
- прорабатывать единый умалчиваемый регламент в части периодичности смены паролей;
- использовать одноразовые пароли при активации учетных записей администратором;
- подключать в проекты генераторы паролей, удовлетворяющие требованиям безопасности.

7. Аутентификация по сертификату электронной подписи (ЭП)

Сейчас ведутся работы по поддержке аутентификации по ЭП. В ПК «НСИ» уже реализована поддержка возможности входа по ЭП.

В ПК «НСИ» для единой учетной записи может быть зарегистрирован единый сертификат ЭП. Если сертификат зарегистрирован, то предметные системы могут его получать через общий механизм синхронизации. Пользователь, если он работает в нескольких системах, где требуется использование ЭП, может регистрировать свой сертификат не в каждой прикладной системе, как раньше, а единожды в ПК «НСИ» как единый сертификат. Остальные прикладные системы, в которых он работает, будут получать этот сертификат вместе с синхронизацией данных из ПК «НСИ».

Пользователь, зарегистрировавший единый сертификат ЭП, может его использовать для входа, для аутентификации с использованием ЭП. В окне входа ему будет выведено уже не предложение ввода единого логина/пароля, а предложение использовать единый сертификат. Пользователь нажимает на соответствующую кнопку, у него вставлен носитель ключа, будет произведена аутентификация с использованием ЭП. Обычно пользователь все равно что-то вводит, так как ключ идет в паре с пин-кодом (пользователь вводит пин-код).

При аутентификации с использованием сертификата ЭП уровень безопасности значительно повышается, так как нет недостатков парольной аутентификации, перечисленных в пункте 6.1

Рекомендуется переходить к аутентификации по сертификату ЭП.

8. Блокировка пользователей

8.1. По расписанию

Планируется ввести расписание, по которому автоматически будут блокироваться пользователи, которые не работали в системе больше указанного времени. По умолчанию будет настроена блокировка при отсутствии активности длительностью в 1 год.

Эту длительность администратор безопасности сможет изменить на ту, которая требуется в регионе. Исключение будет сделано для учетных записей администраторов, которые не будут блокироваться при отсутствии активности.

8.2. Администратором безопасности

На интерфейсе «Пользователи системы» РМ «Управление пользователями» добавилось поле «Последний вход систему», в котором указывается время последнего успешного входа в систему, как показано на рисунке10.

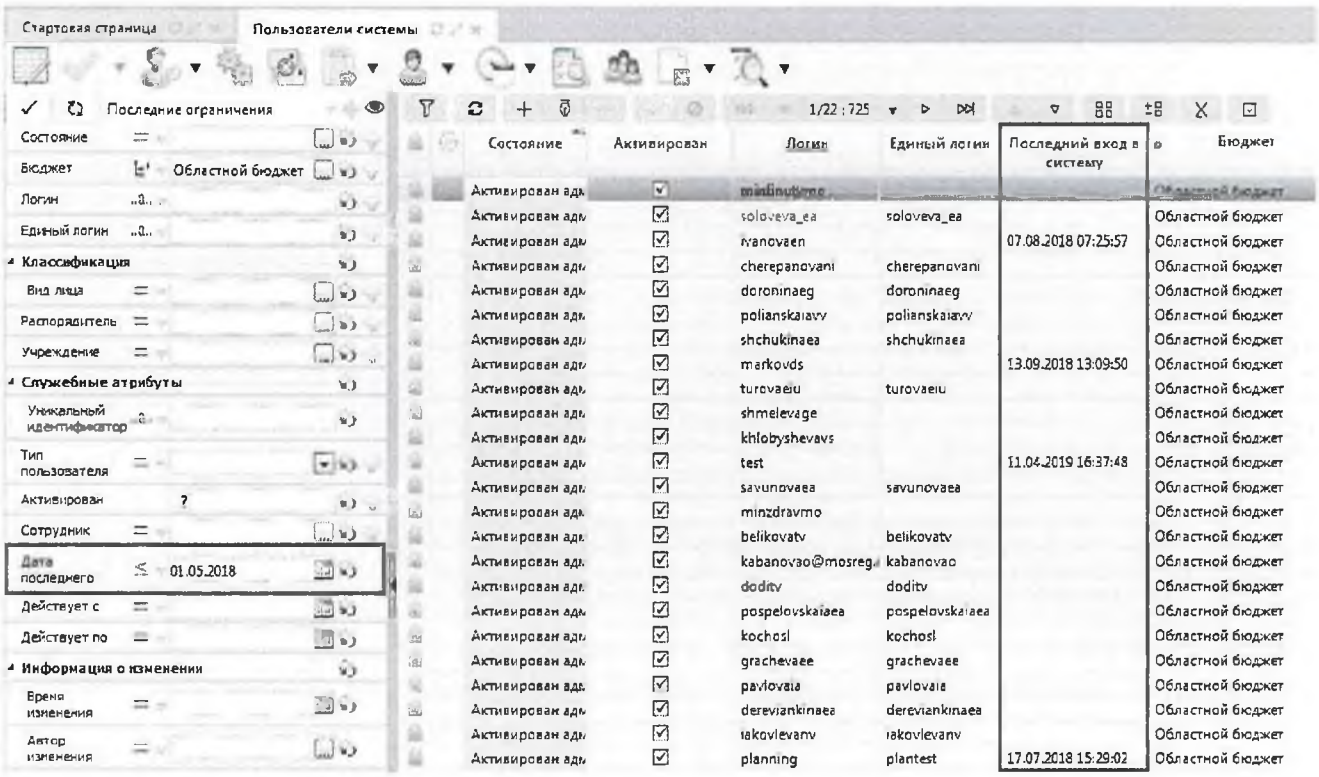


Рисунок 10 – Поле «Последний вход в систему» на интерфейсе «Пользователи системы»

По этим данным тоже легко можно найти пользователей с отсутствием активности. На панели фильтрации, есть специальное поле «Дата последнего входа в систему». По этому параметру можно отфильтровать активных пользователей от неактивных.

9. Основы подсистемы прав

В Web-системах используется классическая подсистема прав. Классическая подсистема прав состоит из трех сущностей: субъект права, объект права и операция. Для настройки права требуется указать субъект права (кто имеет право на операцию), объект права (над чем выполняется операция), операцию.

10. Настройка субъектов права

10.1. Настройка пользователей и групп пользователей

Субъекты права это два справочника: «Пользователи» и «Группы пользователей».

В системе существуют сотрудники и пользователи. Сотрудники – это справочник сотрудников учреждений, он не является справочником субъектов права. Субъектами права являются пользователи.

Пример. Учетная запись администратора. Могут быть учетные записи администраторов, которые не связаны с сотрудниками, они могут быть связаны либо с учреждениями в целом, без привязки к конкретному сотруднику, либо вообще не связаны ни с сотрудником, ни с учреждением. В этом случае пользователь есть, а сотрудника нет.

В системе сначала осуществляется ввод сотрудника в справочнике «Сотрудники», потом создается учетная запись в справочнике «Пользователи».

Пользователей в системе очень много. Если обслуживается группа бюджетов, то их может быть тысячи и десятки тысяч пользователей. Соответственно, надо стремиться, чтобы было меньше работы по администрированию. В этом случае надо работать по шаблонам, когда права один раз настраиваются для одного пользователя, потом определяется «для всех остальных также». Проблему шаблонов решают группы пользователей.

Интерфейс «Группы пользователей» – это базовый интерфейс субъектов права и в большинстве случаев права даются именно на группы, а не на конкретных пользователей, потому что так меньше трудозатрат.

Атрибуты, которые важны с точки зрения администратора.

«Признак централизованности». Этим признаком группы делятся на централизованные (стоит галка) и нецентрализованные (нет галки). Под системной учетной записью дан полный доступ, поэтому все группы доступны для редактирования (белого цвета). Под учетной записью администратора заблокированы централизованные группы пользователей (имеют желтый цвет). На самом деле это не совсем так, региональный администратор может делать такие операции с группами пользователей, как расширение или сужение.

Централизованные группы одинаковы для предметной системы во всех регионах (группа «Все сотрудники», «Сотрудники финансового органа» и т.д.), нецентрализованные группы – это региональные группы, специфичные для каждого региона. Региональный администратор может добавить свою нецентрализованную группу пользователей для конфигурирования прав. Ее в других регионах нет, это сразу видно по атрибуту «Признак централизованности».

Атрибут «Закрыта для изменений». Если системный администратор хочет сделать группу, которую нельзя расширять, то ставит галочку «Закрыта для изменений». В этом случае региональные администраторы не смогут расширить или сузить эту группу, группа фиксируется, она останется точно такой же какой ее определил системный администратор. Если у группы такой галочки нет, то региональный администратор может группу расширять, даже в том случае, если она централизованная.

Рассмотрим на примере централизованной группы «Сотрудники ФО», как региональный администратор расширяет или сужает группу. Наполнение групп осуществляется в детализации интерфейса «Группы пользователей» несколькими способами.

Первый способ – явно задаются пользователи, входящие в группу, по кнопкам + «Добавить запись» или «Добавить пользователей».

Замечание! Колонка «Исключить из группы» позволяет выборочно исключать конкретных пользователей из группы, как показано на рисунке 11.

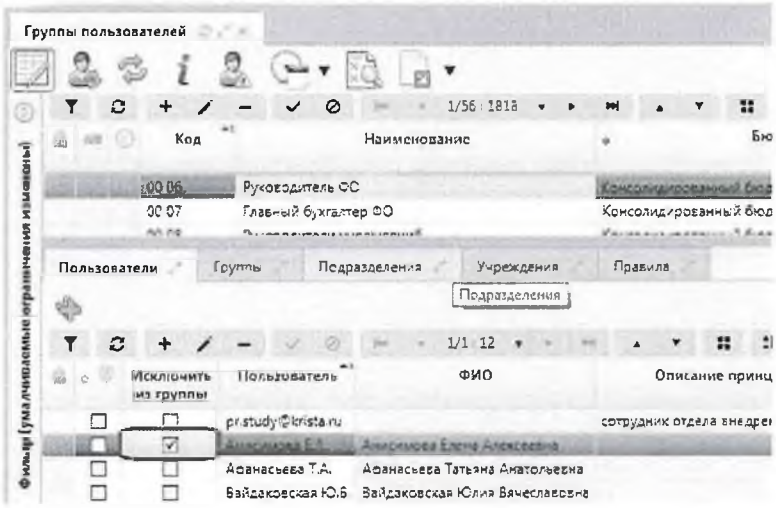


Рисунок 11 – Исключение пользователя из группы пользователей «Руководитель ФО»

Второй способ – вхождение в группу на основе других групп пользователей (вложенные группы). Этот способ широко используется в системах.

На закладке «Группы» есть поле «Применимость». Региональный администратор конкретного бюджета хочет расширить группу и возникает вопрос: администратор бюджета СП расширил одну группу для своего СП, но есть другие бюджеты, на которые он прав не имеет и остальные бюджеты не должны увидеть изменений группы. Поэтому администратор при добавлении вложенной группы обязательно должен указать применимость, причем применимость будет отфильтрована в соответствии с его правами, он не сможет указать другой бюджет, на который у него нет прав. Далее система, когда подсчитывает вхождения в группу использует эту информацию. Для пользователей, входящих в бюджет СП, добавленная группа возьмется, а для пользователей других бюджетов, группа не будет использована и для них не будет никаких изменений. Такие группы расширений можно легко отличить– «признак централизованности» не установлен, это пользовательская строчка, как показано на рисунке 12. Расширять можно даже централизованные группы, но это расширение будет действовать только в рамках конкретного бюджета.

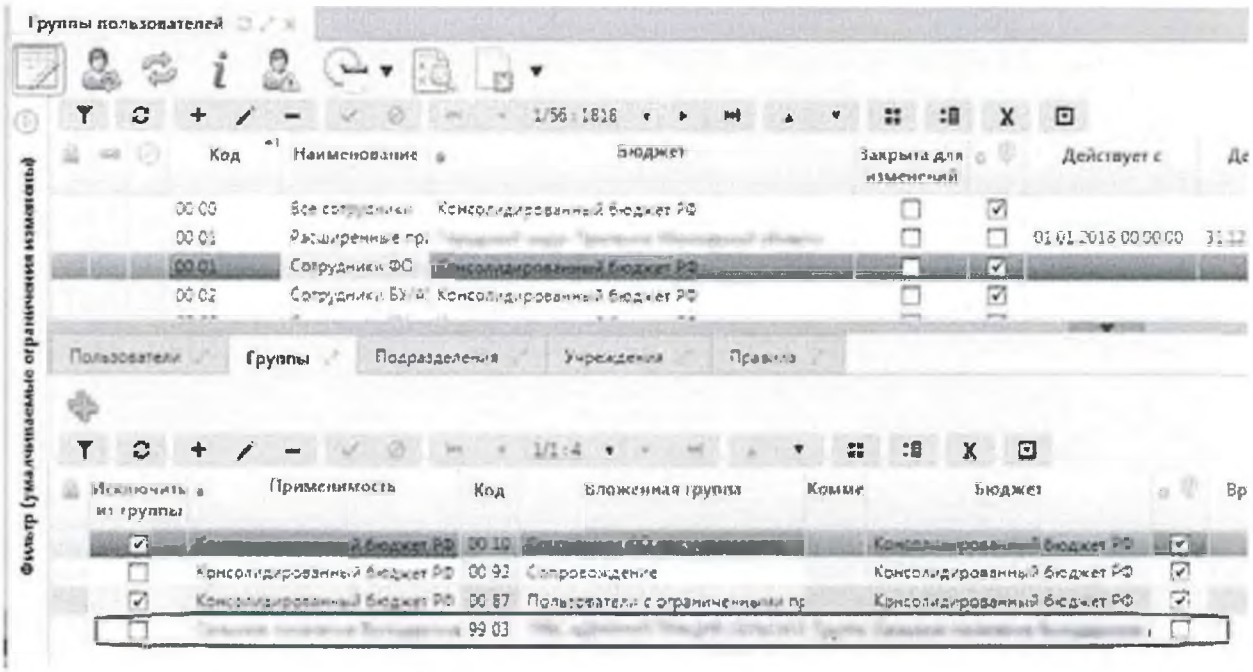


Рисунок 12– Пример расширения группы пользователей клиентской группой

Третий способ – на закладке «Подразделения» расширение групп подразделениями учреждения (всеми сотрудниками этого подразделения). Синоним подразделения –это отдел, то есть это какой-то отдел учреждения.

Четвертый способ – аналогичен третьему. На закладке «Учреждения» указывается учреждение, и группа расширяется всеми сотрудниками этого учреждения.

Пятый способ расширения групп – вкладка детализации «Правила». Благодаря правилам можно динамически расширять группы. Правила достаточно широко используются. Подробнее про правила в пункте 10.2. «Задание правил». Администратор должен помнить, что после внесения изменений в права необходимо нажимать кнопки обновления прав  «Обновить группы пользователей» и «Обновить права и группы». Это делается по той причине, что в системе реализован принцип разделения кэшей прав от редакторов прав. Все редакторы прав сохраняют изменения в базу, а кэши прав работают независимо. Кэши прав наполняются специальными алгоритмами, функционируют независимо от редакторов. Редактор сохраняет изменения в базу, а дальше алгоритм наполнения кэша берет информацию из базы и формирует по нему кэш прав. Что это дает? Первое –увеличивается скорость работы. Вся информация о правах находится в памяти системы и система достаточно быстро определяет наличие или отсутствие права на нужный нам объект. Второе преимущество –можно достаточно просто и быстро добавлять новые редакторы прав, при этом не надо вносить изменения в базовые структуры, которые отвечают за определение наличия или отсутствия права.

Важный момент, касающийся настройки групп: в том случае, если есть настройки и по пользователям и по группам, то общее правило приоритета отдается пользователям. Например, если администратор настроил право, что через группу у пользователя, входящего в эту группу право отобрали, но пользователя добавили явно, то явное указание пользователя более приоритетно. Пользователь в этом случае получит необходимое право.

То же самое правило распространяется и на конфигурацию групп пользователей. При конфигурировании групп пользователей можно как расширять группу, так и сужать ее. В «Группах пользователей» в детализациях, конфигурирующих наполнение группы, есть колонка «Исключить из группы». При конфигурировании группы может возникнуть та же самая ситуация, когда администратор включил пользователя в группу, но при этом через другую вложенную группу пользователь может быть исключен. То есть система должна принять решение: такой пользователь, который явно указан как участник группы и явно указан как участник другой вложенной группы, которая исключена из нашей, должен ли он входить в группу? В этом случае система принимает решение по тому же правилу: явно указанный пользователь будет всегда добавлен в группу. Если пользователь явно исключен из группы, то он не войдет в группу, даже если он входит в ту группу, которая расширяет нашу базовую группу. Конфигурирование пользователей всегда преобладает над конфигурированием через группы.

Вопросы по конфигурированию групп пользователей в интерфейсе «Группы пользователей»:

1. Если пользователя добавили в группу, а затем исключили из группы, то он будет включен или исключен? Он будет исключен из группы, т.к. исключение является более приоритетным, чем включение. Тоже самое распространяется на исключение в детализациях «Группы», «Подразделения».

2. Что будет, если через подразделения пользователя исключим, а явно включим в закладке «Пользователи»? Пользователь будет включен в группу, т.к. закладка «Пользователи» более приоритетна, чем остальные закладки.

3. Что будет, если в группу явно включить пользователя? Пользователь попадет в группу, но только при условии, что бюджет группы и бюджет пользователя совпадают. На рисунке 13 показан пример, где сотрудники автоматически отметились красным цветом, т.к. бюджет группы и бюджет пользователей не совпадает. Они в группе есть, но на самом деле их там нет.

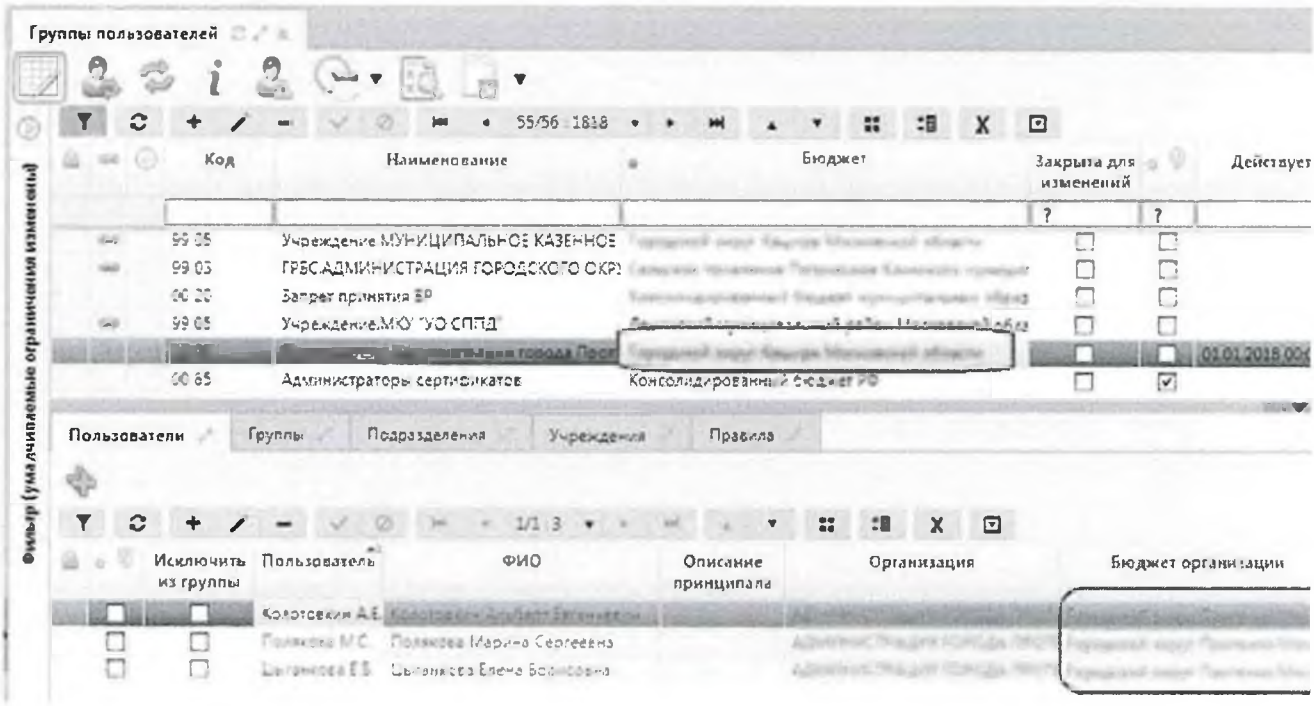


Рисунок 13 – Пример несоответствия бюджета группы и бюджета пользователя

4. Есть пользователь, который входит в группу «Все сотрудники», и есть другой пользователь, который входит в группу «Все сотрудники» и ещё в какую-то вторую группу. У кого больше прав? У того, у которого одна группа, или у того, у которого две группы? На самом деле, у кого будет больше прав неизвестно.

Потому что есть права, которые выдаются, и есть права, которые отбираются. Так что количество групп у пользователя не показатель того, как много у него прав.

10.2. Задание правил

Правило задается на декларативном языке. Все функции разделены на классы, зная назначение функции можно найти, как она называется в системе. Для этого есть функционал, который позволяет быстро ориентироваться в доступных функциях. Например, требуется найти функции, которые работают с подстрокой, как показано на рисунке 14.

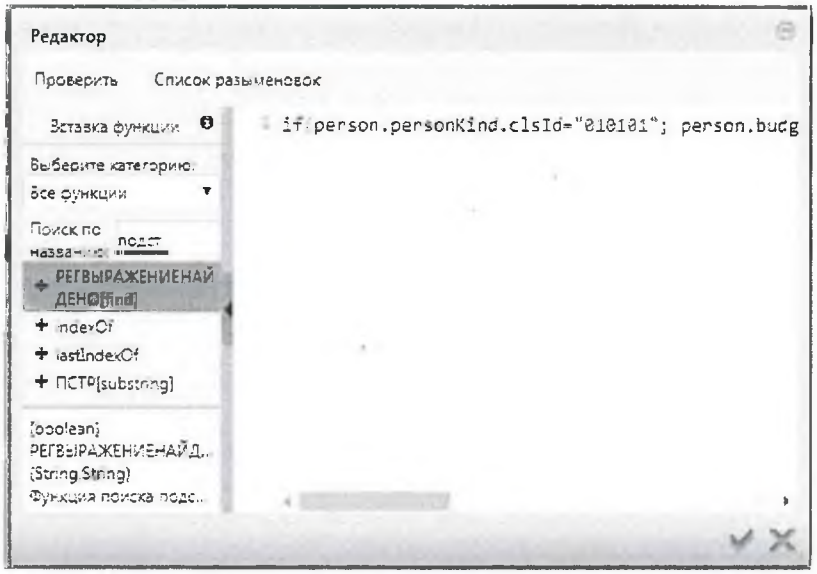


Рисунок 14 – Пример поиска в редакторе правил

Система нашла функцию, причем она ищет не только по названию, но и по описанию функции. Для отладки декларативных правил есть специальная кнопка проверки правильности декларативного правила Проверить «Проверить». Декларативные правила рекомендуются к использованию.

Самое простое правило – это правило для группы пользователей «Все сотрудники». Оно просто возвращает нам истину для каждого пользователя, как показано на рисунке 15. Согласно правилу, каждый сотрудник будет входить в группу «Все сотрудники».

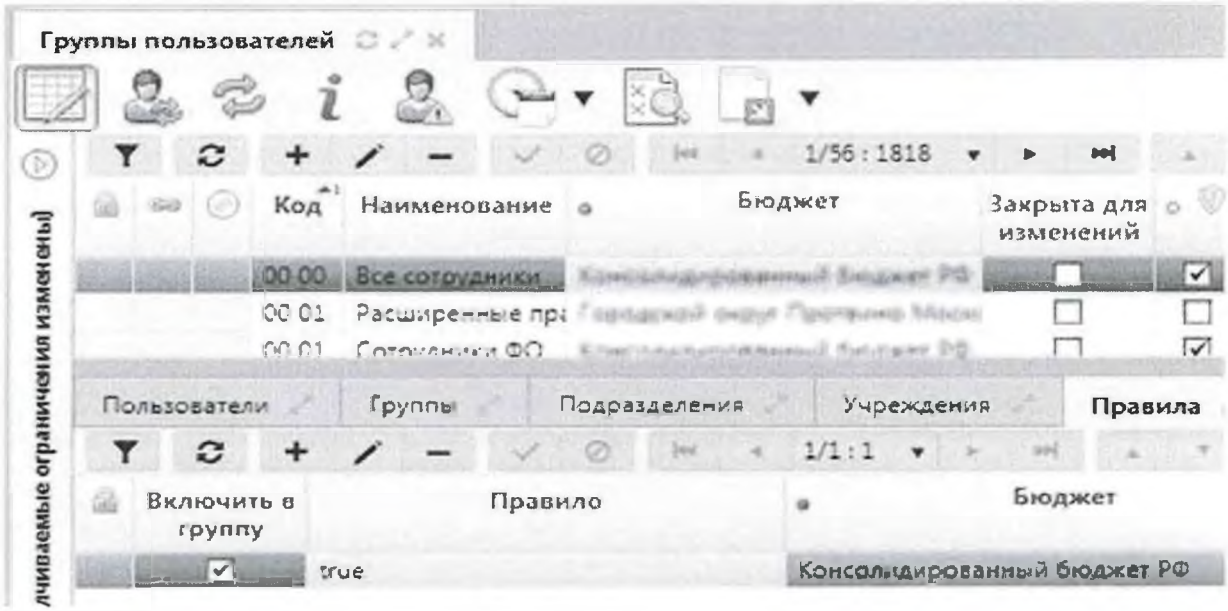


Рисунок 15 – Правило для группы пользователей «Все сотрудники»

Правило для группы «Сотрудники ФО», как показано на рисунке 16, уже несколько сложнее: если вид лица у организации, в которой работает пользователь, финансовый орган, и организация, в которой работает сотрудник является обслуживающим учреждением для бюджета сотрудника, тогда считается, что этот сотрудник является сотрудником финансового органа.

Также если у пользователя есть функциональная роль администратор или локальный администратор, то тогда тоже является сотрудником финансового органа.

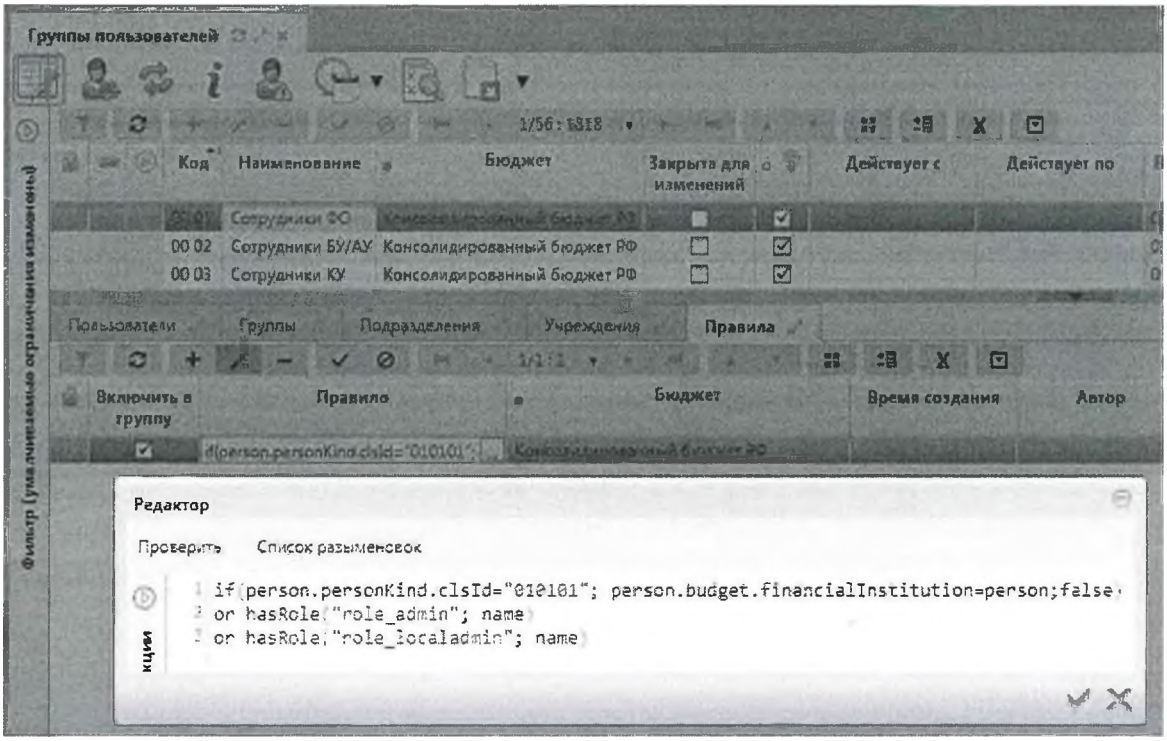


Рисунок 16 – Пример правила для группы «Сотрудники ФО»

В справочнике «Пользователи» есть специальная детализация «Функциональные роли», предназначенная для централизованного администрирования. Если в регионе установлена «НСИ» с функционалом единой точки входа, то можно не только централизованно вести перечень сотрудников, перечень учреждений, но и выполнять элементы централизованного администрирования. Каждому пользователю в ПК «НСИ» могут назначаться функциональные роли, и предметная подсистема может обрабатывать эти функциональные роли.

Пример. Роль администратора подсистемы исполнения бюджета (краткое обозначение ИСП.АДМ). Пользователю назначается эта роль, но возникает вопрос: «Как обработать эту роль? Как система узнает о том, что этого пользователя нужно считать администратором?» В правилах есть специальная функция hasRole («есть роль») –функция проверки наличия переданной роли. С помощью функции hasRole можно определить наличие указанной функциональной роли, как показано на рисунке 16.

Администратор может делать собственные функции на java-скрипт или декларативном языке. Система помечает такие функции, они могут задаваться «налету».

В целом, декларативные правила достаточно простые и, как правило, не больше одной строчки.

11. Настройка объектов прав

11.1. Простые способы задания прав на объекты

Субъектов права (пользователей) может быть много, тысячи. Для того, чтобы упростить администратору работу, используются группы пользователей. Благодаря использованию групп пользователей число субъектов права сокращается существенно, примерно на 2-3 порядка. То есть администратор работает с десятками групп пользователей, вместо того, чтобы работать с тысячами пользователей системы.

Объектов права в системе очень много. Если взять первичные документы, то их может быть несколько миллионов. Соответственно, каждый из первичных документов является объектом права.

Проблема – очень много объектов права. Рассмотрим способы решения этой проблемы.

Если администратор будет работать не с первичными документами, а со справочниками, то в справочниках число объектов права ограничено. Поэтому, если надо задавать права на справочники, то такие случаи обработать гораздо проще.

Рассмотрим задания объекта права в справочниках. Для примера возьмем справочник «Права на формы ввода». Этот справочник задает иерархию дерева форм ввода, как показано на рисунке 17. Другое предназначение справочника – это задание прав на работу с этими справочниками.

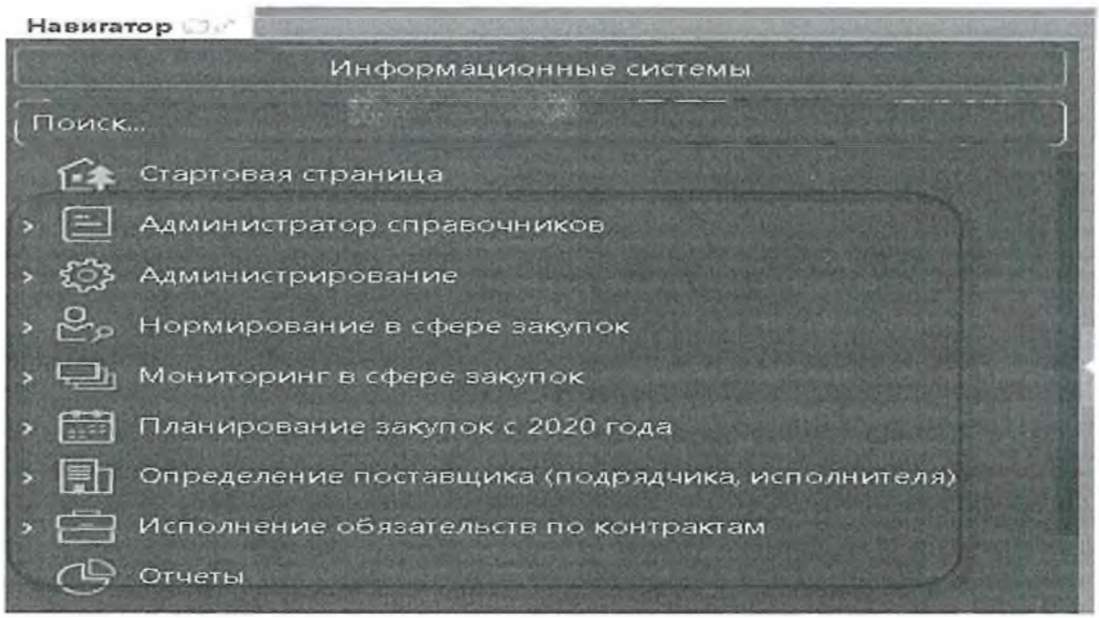


Рисунок 17 – Дерево форм ввода

Типичная задача: ГРБС нужны одни формы ввода, сотрудникам финансовых органов –другие формы ввода, а ПБС третьи формы ввода. Все это можно настроить в справочнике «Права на формы ввода».

В детализациях интерфейса «Права на формы ввода» есть колонка «Уровень доступа, как показано на рисунке 18. Она выделена синим цветом шрифта. Синий шрифт означает, что колонка может изменяться региональным администратором и при обновлении данные сохранятся.

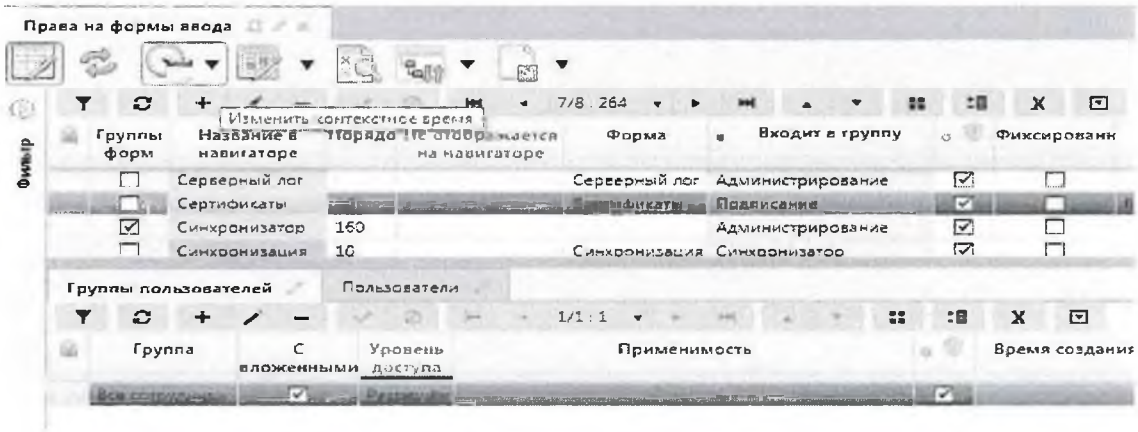


Рисунок 18 – Колонка «Уровень доступа»

Значения атрибута «Уровень доступа»:

— «Отсутствует» – значит, что строка не будет учтена подсистемой прав;

— «Разрешен» – строка дает разрешение на объект права указанному субъекту права;

— «Запрещен» –перекрывает разрешение, права не будет;

— «Эксклюзивный» - перекрывает запрет, он снова дает право («Эксклюзивный» уровень сильнее, чем «Запрещен»).

Региональный администратор может менять уровень доступа. Например, права на работу с формой «Сертификаты» выданы всем сотрудникам, несмотря на то, что форма сертификатов находится в разделе администрирования, а для раздела администрирования права выданы только администраторам. Для формы сертификатов сделаны исключения, потому что удобно, когда сотрудники сами по возможности занимаются администрированием своих сертификатов, если это не противоречит политике безопасности.

Допустим, что политика безопасности клиента такова, что пользователям нельзя разрешать регистрировать свои сертификаты, это должен за них делать только администратор безопасности. В этом случае, достаточно пометить уровень доступа как отсутствующий и все сотрудники, кроме администраторов системы, перестанут видеть форму «Сертификаты».

Можно добавить какую-то конкретную группу (например, «Сотрудники КУ») и запретить доступ к сертификатам только этой группе и в рамках конкретного бюджета, на который у нас есть права. Рисунок 19 показывает пример такой настройки: сотрудники КУ бюджета района не имеют доступ к форме «Сертификаты», сотрудники остальных бюджетов и сотрудники, не являющиеся сотрудниками КУ бюджета района имеют права на форму. Она у них будет появляться в дереве рабочих мест, и они с ней смогут работать.

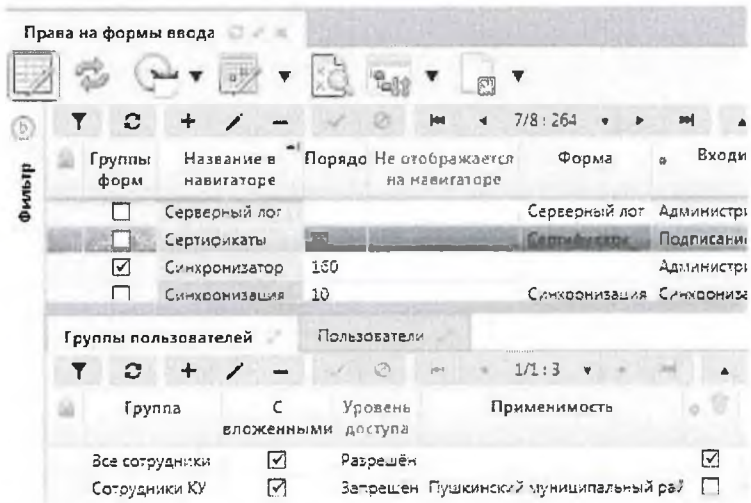


Рисунок 19 – Пример настройки уровней доступа групп пользователей на интерфейс «Сертификаты»

Если потребовалось части сотрудников КУ («Сотрудники РБС»), несмотря ни на что дать права, то для этого надо добавить вложенную группу с уровнем доступа «эксклюзивный» с бюджетом район, как показано на рисунке 20. В этом случае даже несмотря на то, что сотрудники РБС тоже являются сотрудниками КУ района, для них форма сертификатов была бы все равно видна.

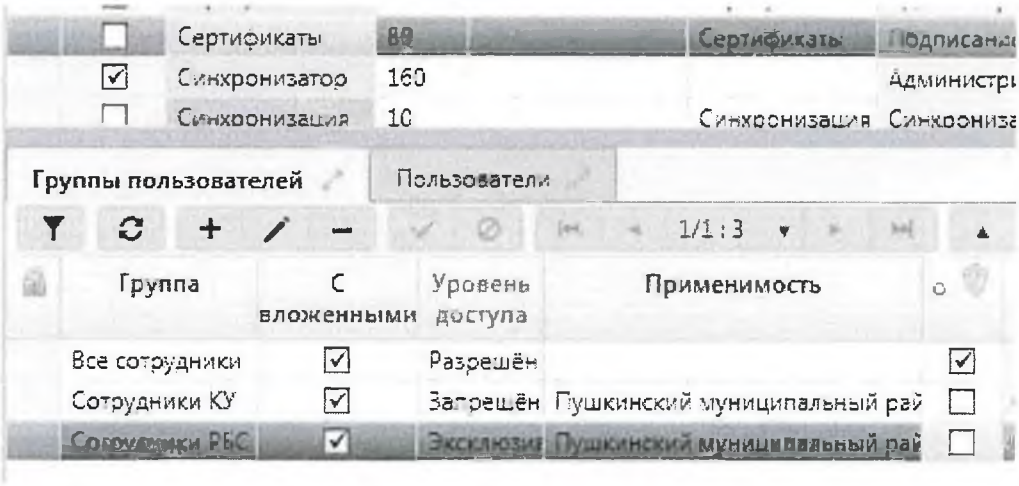


Рисунок 20– Пример настройки эксклюзивного доступа групп пользователей на интерфейс «Сертификаты»

Права на форму ввода характерны тем, что форм ввода не много и мы можем в качестве объекта права использовать указание конкретной формы ввода. Но даже с таким простым случаем возникают сложности. Для удобства администрирования прав на форму ввода добавляется понятие групп форм ввода (например, группа «Администрирование»). Можно назначать права на группы, и они будут распространяться на все вложенные объекты. Это один из приемов, который активно используется для иерархических объектов, т. е. если у объекта есть вложенные объекты, то удобно при задании права использовать эту иерархию и распространять права родителя на вложенные объекты.

Рассмотрим другие редакторы прав, где тоже используется простое назначение объекта права.

Для настройки прав на декларативные правила используется интерфейс «Декларативные правила». Часто требуется отключить какое-то правило для конкретного бюджета или для конкретной группы сотрудников. Региональный администратор находит нужное правило, заходит в детализацию «Права», выбирает группу и указывает бюджет. Базовые атрибуты, которые есть практически всегда – «Группа», задающая субъекта «Права», «Уровень доступа», «Применимость». Но в ряде случаев могут быть дополнительные атрибуты. Например, у декларативных правил– «Уровень проверки», как показано на рисунке21. Объектом права здесь является не само декларативное правило, а пара: декларативное правило и уровень проверки.

В «Уровне проверки» можно указать, что жесткое срабатывание для указанного правила запрещено всем сотрудникам бюджета. В результате все сотрудники бюджета при срабатывании этого правила будут вместо ошибки получать предупреждение, потому что на уровень проверки «Предупреждение» у них право не отняли, как показано на рисунке 21. Если надо правило отключить совсем, то уровень проверки надо задать пустым (в этом случае отключатся правила как с уровнем «Ошибка», так и с уровнем «Предупреждение»).

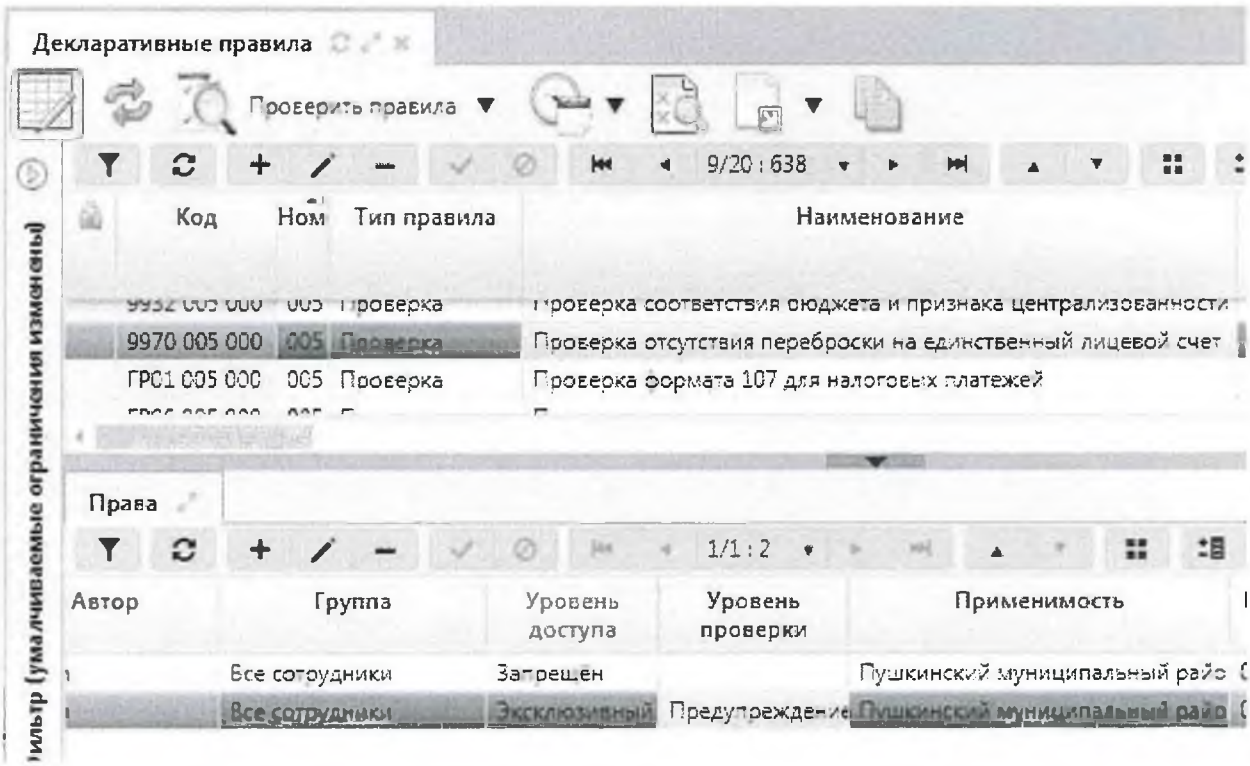


Рисунок 21 – Пример настройки прав на декларативные правила

Такие же простые редакторы, которые работают с конкретными объектами права используются для задания прав на сценарии обработки, генерации, печатные формы. Они однотипные. Администратор определяет генерацию (печатный документ, сценарий), заходит в детализацию, определяет группу, которой надо запретить эту генерацию (печатный документ, сценарий и т.д.), и указывает уровень доступа.

На примере печатных документов рассмотрим особенность. В детализации печатных форм у уровня доступа список значений меньше: отсутствует, запрещен, эксклюзивный. Нет уровня доступа «разрешен». Это сделано для удобства администрирования и для того, чтобы сохранить совместимость с теми версиями, когда не было возможности назначать права на такие объекты права. Предполагается, что по умолчанию всегда для всех групп есть право «Разрешен». То есть система за администраторов прав добавляет строчку. При управлении можно этот запрет убрать либо установить эксклюзивный уровень. Для справочников, где нет значения уровня доступа «разрешен», действует правило назначения права «по умолчанию», то есть такие объекты разрешены всем сотрудникам.

Особенности учета прав для глобальных администраторов

Особенностью системы прав является то, что глобальные администраторы фактически имеют гораздо большие права, но эти глобальные права нигде явно не заданы. С одной стороны, это минус, потому что отсутствие явного задания– это не очень хорошо. С другой стороны, плюс. Например, глобальный администратор не может случайно убрать у себя права, приведя систему в неконсистентное (некорректное) состояние, при котором система некорректно выполняет (или перестает выполнять) функции. Сейчас такой возможности у глобального администратора нет.

Он не сможет удалить права настолько, чтобы потом самому не зайти и не исправить это.

Особенности учета прав для пользователей, не привязанных к организациям. Могут быть пользователи, которые не привязаны ни к сотруднику, ни к организации. Вот с такими пользователями возникают некоторые проблемы при учете прав, потому что этого пользователя нельзя отнести ни к одному из бюджетов. А права привязываются к конкретным бюджетам. Это администраторы, которые вынуждены по тем или иным причинам администрировать несколько бюджетов. Это сотрудники сопровождения, филиалов, информационных служб субъектов РФ, которые администрируют муниципальные образования и т.д. Для пользователей, которые не привязаны к бюджету, следует использовать следующее правило: обрабатываются только права, которые привязаны к «Консолидированному бюджету РФ». В перечне это корневой элемент и называется «Консолидированный бюджет РФ». В том случае, если пользователь не привязан к конкретному бюджету, то для него учитываются только те права, которые назначены на консолидированный бюджет РФ.

11.2. Задание сложных прав на объекты

11.2.1. Настройка прав на видимость документов

Права на видимость требуется поддерживать в первую очередь для первичных документов, т.к. число первичных документов очень велико. Если число пользователей тысячи, то число первичных документов – миллионы и возможных комбинаций с правами десятки либо сотни. Перемножив эти величины, получим число комбинаций этих троек, необходимых для настроек права, примерно 10^{12}, это очень большое число. Этот огромный объем прав надо уметь настраивать, а также необходимо уметь настраивать права на видимость для тех документов, которые пользователь еще не сохранил. Как это можно сделать? Решение заключается в том, что у таких документов выделяют ключевые метрики.

Часто пользователи описывают правила видимости как достаточно неформальные правила, которые можно сформулировать примерно следующим образом: пользователь одного бюджета не должен видеть документы остальных бюджетов; пользователь одного учреждения не должен видеть документы остальных учреждений. Таких правил достаточно много, у правил есть исключения. Выделяются какие-то ключевые метрики, например, бюджет, учреждение, лицевой счет, и т.д., и права на первичные документы назначаются через значения прав на эти метрики. Выделяются ключевые метрики, характерные для предметного проекта, и реализуется назначения прав на эти ключевые метрики и потом опосредованно просчитывается право на первичные документы. Основным справочником, который используется для конфигурирования прав на видимость является справочник с аналогичным названием «Права на видимость», как показано
на рисунке 22. В заголовке этого справочника перечень групп, а в детализации – метрики. В качестве основных метрик выбраны:

— перечень бюджетов (детализация «По бюджетам»);

— справочник организаций (детализация «По организациям»);

— справочник лицевых счетов (детализация «По л/с»);

— справочник кодов глав (детализация «По кодам глав»);

— справочник состояний (детализация «По состояниям»).

— Дополнительно есть еще закладка «Правила».

Закладки «По категориям документов», «По счетам обслуживаемых бюджетов» – это уникальные метрики, которые используются только в «WEB-Исполнении».

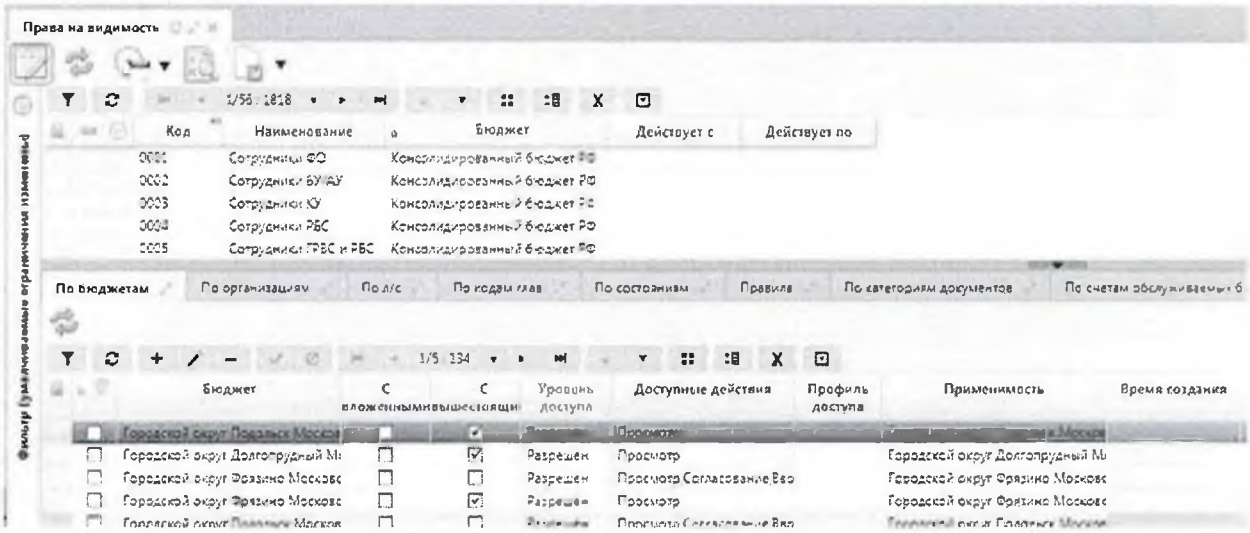


Рисунок 22 – Интерфейс «Права на видимость»

Базовая метрика – это перечень бюджетов. В детализации «Бюджет», как показано на рисунке 22есть колонка «Уровень доступа». Субъект права в заголовке определен в качестве конкретной группы. В качестве объекта права выступает указание бюджета.

Бюджет является иерархическим объектом права, поэтому есть колонки для более удобной работы с иерархическими объектами права:

— «С вложенными» — не только на указанный бюджет, но и все его дочерние бюджеты;

— «С вышестоящими» - указанный бюджет и все его предки.

В справочнике «Права на видимость» есть колонка «Доступные действия» со списком из трех значений: «просмотр», «согласование», «ввод». Понятно, что указанный справочник задает права не только на видимость, но и на операцию ввода. Операции просмотра и ввода сильно связаны. Если мы имеем право на ввод, значит имеем право и на просмотр. Если мы имеем право на просмотр, то необязательно имеем право на ввод. Поэтому эти операции с правом – это отдельные операции и конфигурируются они отдельно.

Зачем нужна операция согласования. Если просмотр документа дает право только на чтение, ввод на операцию добавления, то согласование дает право ГРБС согласовывать документы подведомственных учреждение, после того как ввод документа был завершен. Согласование не дает право на редактирование документа, а позволяет обрабатывать документ по бизнес-процессу. С точки зрения системы это нечто среднее между просмотром и правом на внесение изменений.

Задача администраторов – сконфигурировать права на видимость. Первая цель – это определить права пользователей на ключевые метрики.

Рассмотрим разные способы назначения прав на метрику «Перечень бюджетов». Самый простой способ – это явное назначение прав на группы бюджетов пользователям соответствующего бюджета. На рисунке 23 приведен пример конфигурирования права на перечень бюджетов следующим образом: для всех пользователей бюджета мы даем права на бюджет и его вышестоящие бюджеты, но только на просмотр. А на ввод мы даем права только на этот бюджет. Если бы еще были обслуживаемые бюджеты, то мы бы могли еще использовать галочку «С вложенными». Так настроено, потому что родительские бюджеты — это консолидированные бюджеты (консолидированный бюджет РФ, консолидированный бюджет области), которые не должны быть доступны для редактирования сотрудникам конкретного бюджета. Но право на просмотр документов по этим бюджетам дать необходимо, иначе пользователи не увидят много общих вещей. Например, они не смогут работать с бюджетной классификацией федерального уровня.

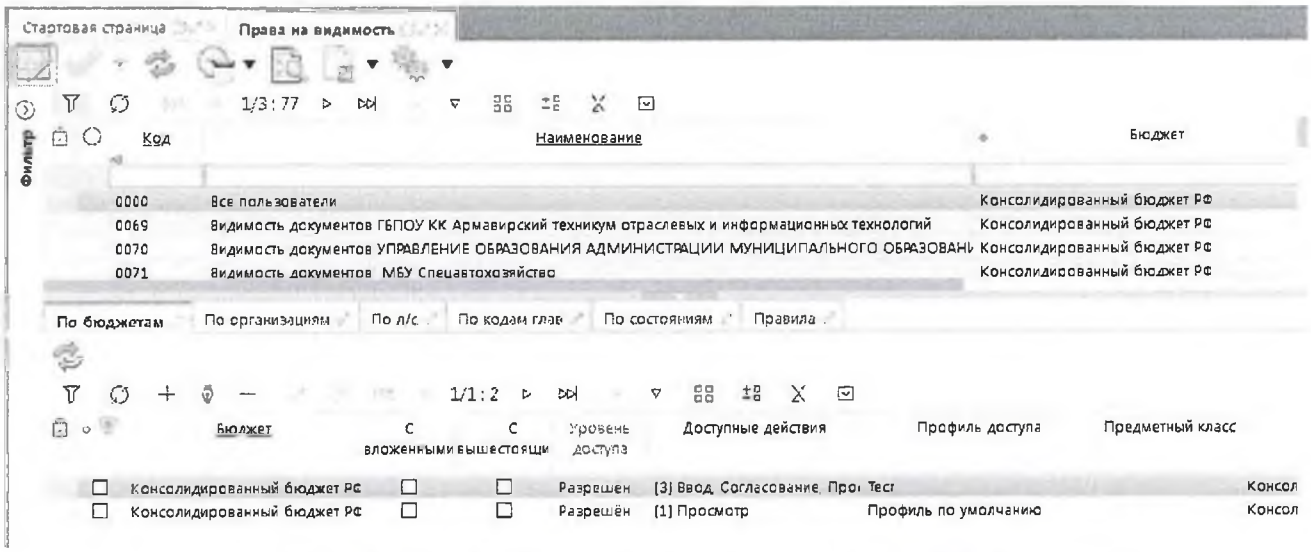


Рисунок 23 – Пример конфигурирования права на перечень бюджетов

При назначении прав на метрику организаций справочник «Учреждения (ОВ)» можно рассматривать как иерархический, но здесь иерархия немного другая – по принципу подведомственности. У каждой организации есть распорядитель, либо учредитель и у него тоже в принципе может быть свой распорядитель, если это РБС. Для упрощения задания прав эту иерархию тоже удобно использовать. Права на метрику организаций можно указывать как явно, перечисляя конкретные учреждения, так и опосредованно, указывая только организацию-распорядителя или указывая только организацию ЦБ. Если указывается организация ЦБ, то задаются права на все учреждения, обслуживающиеся в этой ЦБ.

На других метриках сделаны аналогичные атрибуты, облегчающие задание прав.

В облегчении администрирования прав на видимость сделано много, но все равно этого недостаточно. Надо для большого числа групп сотрудников создавать права на метрики. Это достаточно трудоемко. Приходится дополнительно добавлять много групп сотрудников, чтобы точно назначить права на метрики. Например, для того, чтобы дать права сотрудникам учреждения на все лицевые счета этого учреждения, надо на сотрудников этого учреждения завести группу, включить сотрудников в эту группу и дать этой группе права на соответствующие лицевые счета. Все равно получается очень долго и трудоемко.

Проще сделать можно, потому что неформальное правило, которое описывает заказчик, часто звучит, например, так: «сотрудники любого учреждения имеют право на лицевые счета этого учреждения». И хотелось бы иметь способ описать, чтобы права на метрики формировались автоматически, чтобы это не делать администратору вручную.

Такой способ был найден – задание прав на видимость с использованием правил. До того, как появились правила, были различные средства автоматизации, но они заключались в том, что права на метрики генерировались автоматически. При этом их не надо было заносить администратору руками, они появлялись в правах на видимость, администратор их видел, но это было все равно неудобно. Появлялось много дополнительных групп пользователей, которые генерировались автоматически, у этих групп пользователей делалось наполнение. В случае, если требовались исключения, возникали определенные неудобства.

На рисунке24представлены примеры правил. Основа правила – это java-скрипт. Правила пишутся системным администратором и, как правило, существующие централизованные правила подходят всем. Один раз разработали и на всех серверах используются.

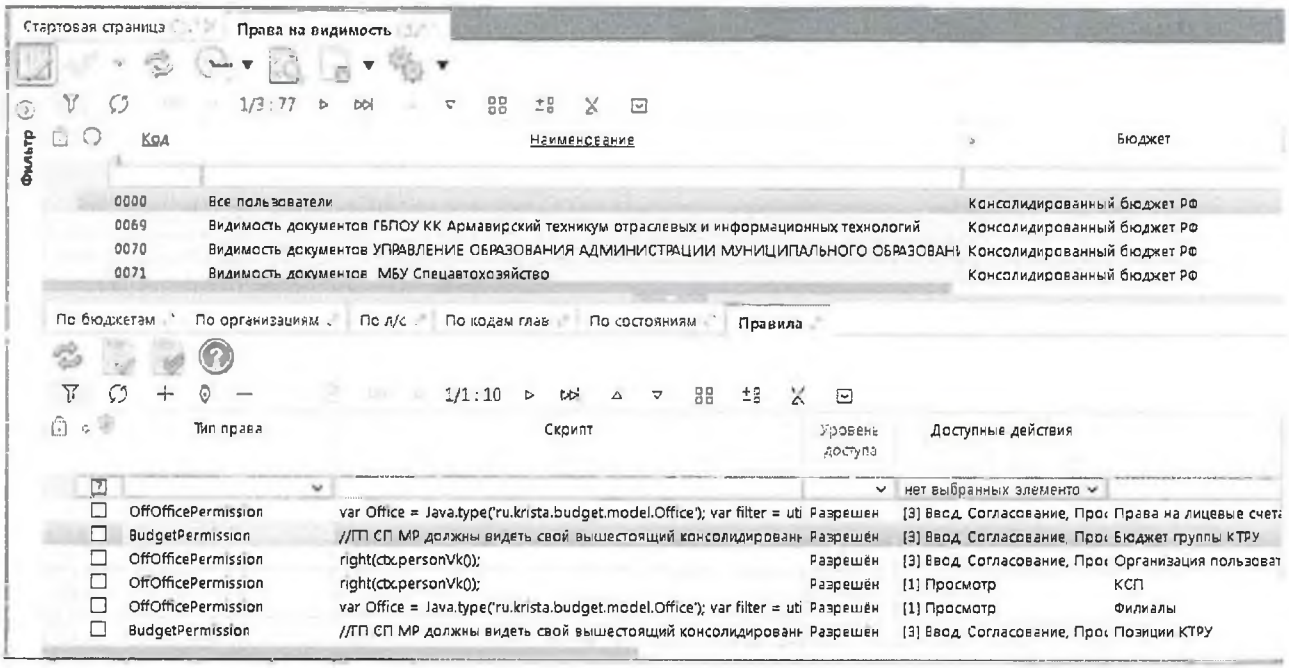


Рисунок 24 – Пример правила в интерфейсе «Права на видимость»

Одна строка правила заменяет много строк групп пользователей с доступным действием просмотра.

Причем правило универсально, оно подходит для всех регионов. Если задавать тоже самое руками через группы пользователей, то пришлось бы делать это на каждом сервере, потому что для каждого объекта права требуется указание конкретного бюджета.

Преимущества правил: настраиваются унифицировано один раз и согласно этим настройкам делается генерация объектов права по соответствующей указанной метрике на любом сервере.

Можно настраивать региональные правила (используя признак централизованности), которые будут действовать в рамках конкретного сервера для конкретного региона. Централизованное правило имеет включенное значение «признака централизованности», региональное - выключенное.

Однако, возникает проблема с исключениями. К сожалению, в тех неформальных правилах, которые описывает заказчик, что пользователи конкретного учреждения должны иметь права на все лицевые счета, всегда есть исключения. Например, подведомственные учреждения не должны иметь права на лицевые счета ГРБС. Если подведомственное учреждение работает с документом бюджетной росписи, у которой в заголовке указан его ГРБС, то такой документ тоже должны видеть в части, касающейся бюджетного учреждения. Другой пример: есть внутренний платеж учреждения А учреждению Б, такой платеж должны видеть оба учреждения, хотя там присутствует лицевой счет, на который у учреждения нет прав. Таких исключений много, система прав в части организации прав на видимость должна иметь механизмы, позволяющие задавать эти исключения.

Рассмотрим механизм, позволяющий задавать исключения.

Специальный интерфейс «Профили доступа» доступен только глобальному администратору, как показано на рисунке 25.

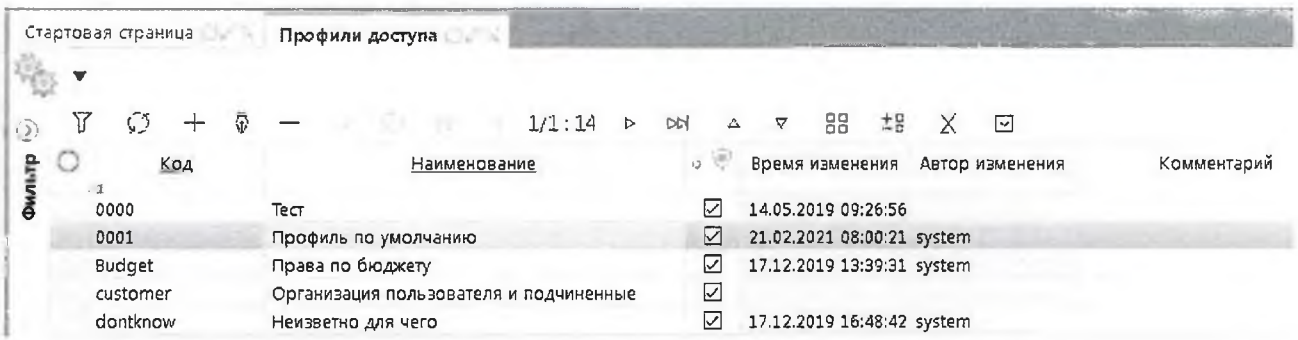


Рисунок 25 – Интерфейс «Профили доступа»

Те исключения, которые рассматривали выше, привязываются к конкретному первичному документу. В целом, правило о том, что сотрудники учреждения имеют права на лицевые счета этого учреждения, действует для большинства интерфейсов, но есть интерфейсы, где это правило надо расширить или переформулировать. То есть в целом метрики действуют в рамках конкретных предметных классов, конкретных форм ввода, конкретных первичных документов. Можно пойти по простому пути и указывать вместе с метрикой первичный документ, для которого это правило бы действовало. Но первичных документов в системе много и не желательно каждый раз в правах на видимость, которых и так много, еще вводить первичный документ как предметный класс. Для большинства предметных классов эти правила одинаковы. Поэтому хотелось перейти к варианту, когда бы задавались только исключения или выделялись бы конкретные группы. Цель –максимально упростить администрирование, для этого и предназначены профили доступа. Бывают правила, которые формируются как правила по умолчанию.

В этом случае базовое правило о том, что сотрудники учреждения имеют права на лицевые счета этого учреждения, действует по умолчанию, и его помечают специальной отметкой через
профили доступа. Дальше есть еще правила, которые являются исключениями. Учреждения могут иметь права на документы своего ГРБС, в том случае, если это документы доведения до подведомственных. Такие правила помечаются дополнительным профилем доступа, отделяя их от предыдущих правил по умолчанию. Профиль доступа является просто отметкой о том, что это правило надо будет обработать по-другому.

В одной из конфигураций прав на видимость, которая использовалась до начала запуска правил, определяли группу для учреждения и сотрудникам этого учреждения давали права. Т.е. права на организацию давали следующим образом: по умолчанию сотрудники получали права на организацию (неформальное правило о том, что сотрудники учреждения имеют права на документы этого учреждения), дальше для документов распределения давали права на документы ГРБС. Основная суть использования профилей доступа в том, что фактически разные наборы прав помечаем профилем доступа.

Могут встречаться случаи, когда профиль доступа оставлен пустым, т. е. указан объект метрики с незаполненным профилем доступа. В этом случае система интерпретирует это как право на любой профиль доступа (правило будет распространяться и на профиль по умолчанию и на все остальные профили).

11.2.2. Описание правил фильтрации

Рассмотрим задачу построения фильтра, которая решает проблему видимости. Надо отфильтровать документы, которые пользователи не должны видеть. Для решения этой задачи предназначен интерфейс «Доступ к предметным классам», как показано на рисунке 26, который решает задачу разметки. Указывается, что в определенном предметном классе есть метрика. Например, есть метрика «Бюджет».

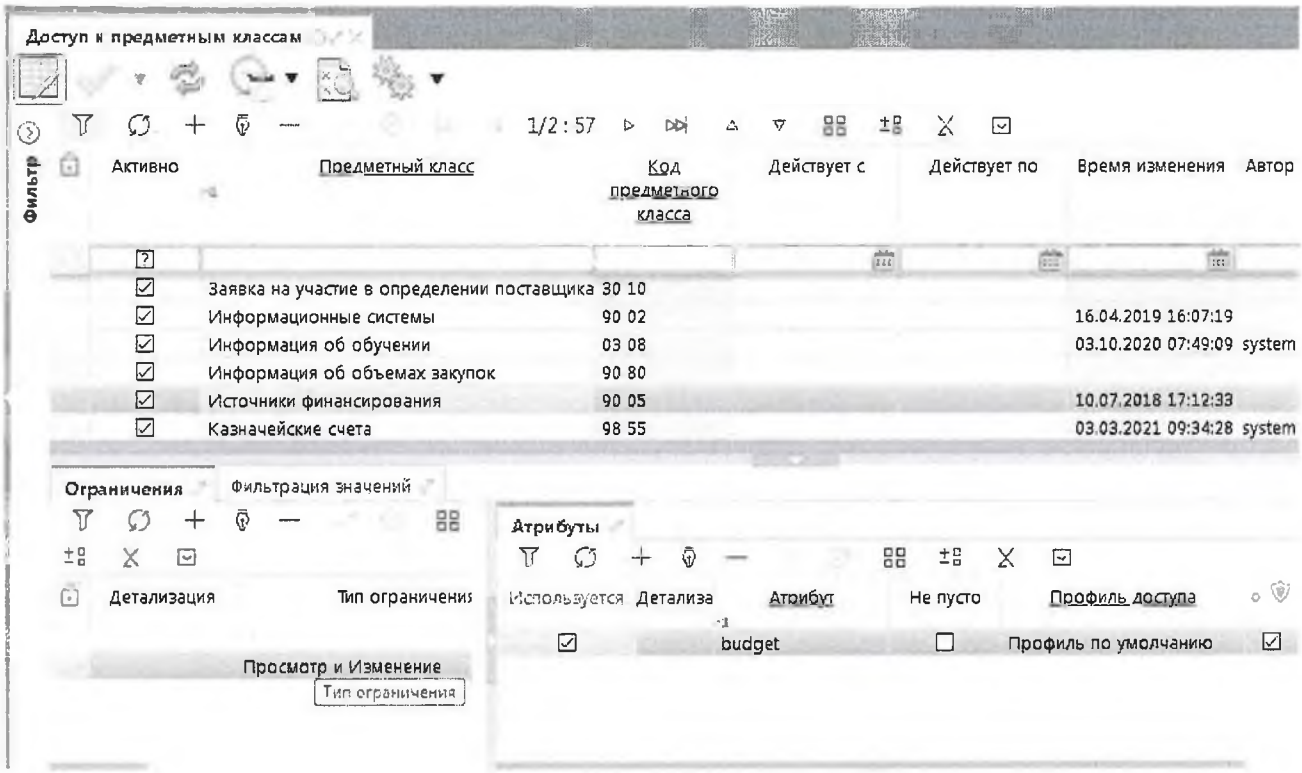


Рисунок 26 – Интерфейс «Доступ к предметным классам»

В типах ограничений есть три возможных значения:

— «просмотр»,

— «изменение»,

— «просмотр и изменение».

Чаще всего при конфигурировании используется тип ограничения «просмотр и изменение».

11.2.3. Настройка прав на видимость для модальных справочников и автокомплитов

Рассмотренные настройки касались в первую очередь прав на видимость документа полностью. Пользователь либо видит документ, либо не видит. На практике требуется, кроме организации прав на видимость документов, ещё настраивать права на видимость для модальных справочников, права на видимость автокомплитов.

Например, указывается в документе «Учреждение» – учреждение является метрикой, это учреждение задано в доступе к предметному классу на соответствующую метрику. И хотелось бы, чтобы при выборе этого учреждения те права на метрики, которые определены, использовались для фильтрации справочника, связанного с этой метрикой. Т.е. чтобы при выборе учреждения пользователь мог видеть только те учреждения, на которые в его метрике даны права. Хотелось бы делать так, чтобы система всё это определяла автоматически и не надо было бы конфигурировать дополнительно.

Поэтому в том случае, если права на модальные справочники и автокомплиты совпадают с правами на метрики, то не надо ничего дополнительно указывать. Система сама автоматически строит фильтры на основании ранее заданной информации. В том случае, если требуется настраивать права на фильтрацию справочников отличающуюся от прав на метрики, то должна использоваться вторая закладка «Фильтрация значений», которая может изменить правило построения фильтра справочника.

11.2.4. Настройка прав на видимость данных в отчетах

На основании первичных документов строятся отчеты, и в отчетах возникает такая же задача – сделать, чтобы пользователь, который не имеет права на другие учреждения, при построении отчета не видел данные по другим учреждениям.

Это можно сделать на интерфейсе «Администратор отчетов».

Могут быть случаи, когда отчет должен формироваться независимо от прав на видимость данных. У таких отчетов на интерфейсе «Администратор отчетов» в колонке «Фильтрация по правам» не должно быть галки. Если фильтрация по правам нужна, то в колонке «Фильтрация по правам» ставится галка.

Отчеты могут строиться:

— по первичным документам (по сущностям). В этом случае вся необходимая разметка уже есть, берется информация из доступа к предметным классам, т.е. используются те же правила построения фильтров, что и для ограничения прав на видимость первичных документов;

— по регистрам (особые структуры, представляющие собой кэш информации из первичной документов, служащие для упрощения разработки отчетов и для ускорения их формирования). В этом случае нет правил для построения фильтра, поэтому надо системе давать дополнительную информацию. Для задания дополнительной информации используется интерфейс «Доступ к регистрам» как показано на рисунке 27, предназначенный для настройки под учетной записью «system», для региональных администраторов конфигурирование не потребуется.

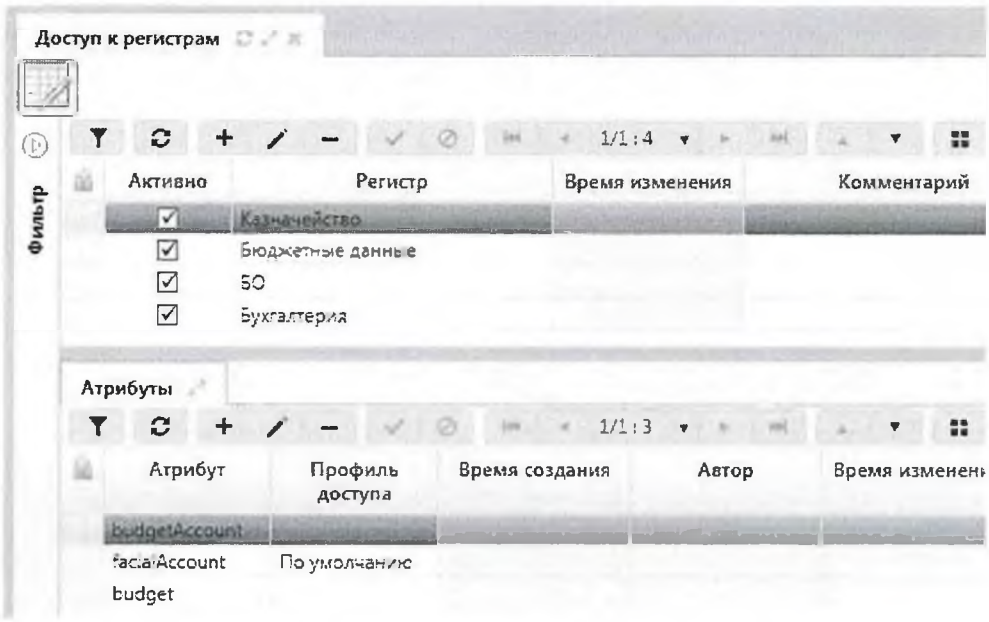


Рисунок 27 – Интерфейс «Доступ к регистрам»

Для регистров в детализации «Атрибуты» задается соответствующая разметка. Указывается, какой атрибут является перечнем бюджетов, какой является счетом бюджета, а какой - лицевым счетом. Этой информации для системы достаточно, чтобы построить фильтр при обращении за данными к регистрам.

Вот так решается проблема настройки прав на видимость данных в отчетах. Используются те же механизмы, которые использовались при построении фильтрации в первичных документах, а для регистров сделана дополнительная разметка.

11.2.5. Настройка прав на видимость для справочников, вызываемых с панели ограничений

Когда на панели ограничений есть элементы, связанные с метриками, то нужно, чтобы пользователь при выборе значений из справочника видел отфильтрованные значения в соответствии с правами на метрики.

Как это конфигурируется:

— для форм ввода – дополнительного конфигурирования не требуется. За наполнение панели ограничений для форм ввода отвечает интерфейс «Правила применимости параметров», который сопоставляет параметр со свойством ограничения. Этой информации системе достаточно для того чтобы определить связь параметра с соответствующей метрикой и построить нужный фильтр.

— для отчетов – используется интерфейс «Правила применимости параметров источников». В отчете задается из каких источников он берет данные. Для отчета можно использовать те ограничения, которые допустимы для источников данных, используемых отчетом. Например, если отчет использует источники плана и источники факта, то в отчете допустимы ограничения, которые могут использоваться для плана, или ограничения, которые могут использоваться для факта.

В интерфейсе «Правила применимости параметров источников» определяются ограничения для источников плана, источников факта и т.д. Здесь уже меньше информации – нет возможности сопоставить параметр с конкретным атрибутом сущности, поэтому в данном интерфейсе присутствуют атрибуты, необходимые для поддержки построения фильтра по правам:

— атрибут «Использовать фильтрацию по правам» – необязательно у параметра, по которому строится ограничение, ставится галочка «Использовать фильтрацию по правам». Например, ограничение по бюджету трансферта для которого использование фильтрации по правам не требуется, т.к. бюджет трансферта — это не бюджет документа. В этом случае галочки «Использовать фильтрацию по правам» не будет;

— атрибут «Профиль доступа» (смотри п.п. 11.2.1);

— дополнительная информация берется из колонки «Свойство ограничения». Если источник берет данные из регистров, то строится фильтрация по регистрам.

Таким образом, параметр связан с источником и свойством ограничения, а у регистра есть необходимая информация (на интерфейсе «Доступ к регистрам»). Можно построить фильтр.

12. Настройка операций

12.1. Настройка прав на операции в бизнес-процессах

Множество прав очень большое – это перемножение субъектов права (пользователи) на объекты права (документы) и на операции с этими правами. Мы рассмотрели, как уменьшить множество субъектов права (за счет использования групп), рассмотрели, как уменьшить множество объектов права (за счет использования метрик и за счет назначения прав на родительские элементы в иерархических сущностях). Теперь посмотрим операции с правами. Их тоже может быть достаточно много и фактически бизнес-процессы позволяют решить эту проблему упорядочивания задания прав на операции с документами.

В интерфейсе «Редактор бизнес-процессов» есть два редактора табличный и графический. Графический редактор удобен для визуального восприятия, вызывается по ссылке «Перейти» в поле «Редактор», как показано на рисунке 28. Табличный редактор удобно использовать для задания прав на переходы.

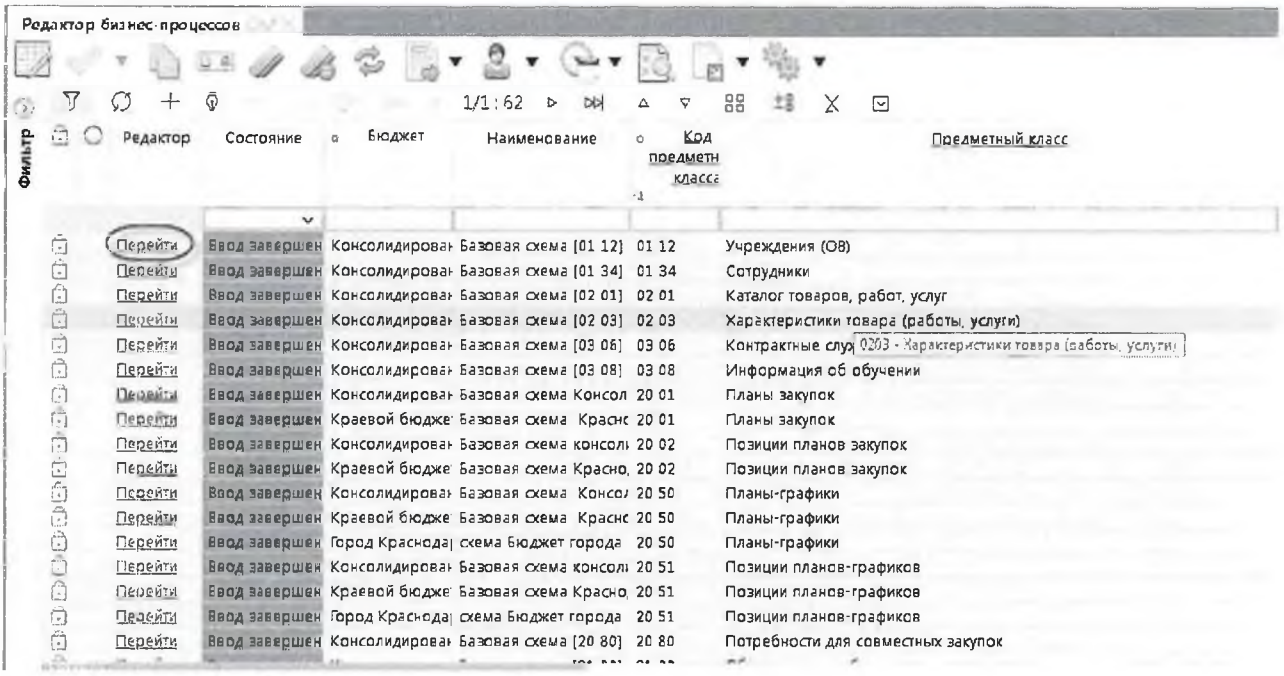


Рисунок 28 – Интерфейс «Редактор бизнес-процессов»

С первичными документами пользователь может совершать достаточно много действий. На каждое из этих действий администратор должен иметь возможность назначать права. Бизнес-процесс является удачным решением, чтобы решить эту проблему. Бизнес-процесс описывает, какие операции над документом может делать пользователь. Есть сложный анализ контекста: над каждым документом конкретный пользователь может делать разные операции.

Не будем рассматривать все детали бизнес-процессов, а рассмотрим только часть, связанную с администрированием прав.

Аналогом операций в бизнес-процессах являются действия и переходы. Действия – это более приближенное для пользователя, а переходы – это низкоуровневая сущность. Администратору удобно назначать права не на действия, а на переходы, потому что одно действие может в себе содержать несколько переходов. И система сама автоматически в зависимости от документа и дополнительного контекста может принимать решение, какой переход возможен, а какой нет. Когда пользователь инициирует действие, система может пойти либо по одному переходу, либо по другому переходу. И вот в связи с этим удобнее назначать права именно на переходы, а дальше уже на основании прав на переходы просчитываются права на действия.

Бизнес-процесс – это граф состояний документа и переходов. Вершины графа – это состояния, а дуги являются переходами. Документ в процессе обработки перемещается по этому графу состояний из начального в конечное состояние.

Операций с документом достаточно много. Число операций права фиксировано. Т.е. в более простых случаях администратор работает всегда с одной операцией права – выполнить,

видеть, редактировать. Иногда администратор работает с двумя операциями права, т.е. видимость и редактирование задаются вместе. Но динамически определять операции права крайне неудобно. Возникает задача обработки динамического числа операций права. Здесь выполнен хитрый ход: в реальности рассматриваются операции права как объекты права, над которыми есть всего лишь одна операция «выполнение». Переходы являются операциями, мы рассматриваем переходы как объекты права с операцией «право выполнения». В результате получается всего одна операция.

Чтобы задать права на переход, в детализации «Переходы» есть специальная детализация «Права», как показано на рисунке 29. В детализации «Права» все те же самые атрибуты, что и в других детализациях прав:

— группа пользователей, которая имеет право на переход (субъект права);
— уровень доступа (отсутствует, разрешен, запрещен, эксклюзивный);
— применимость, которая задает область видимости строки; признак централизованности.

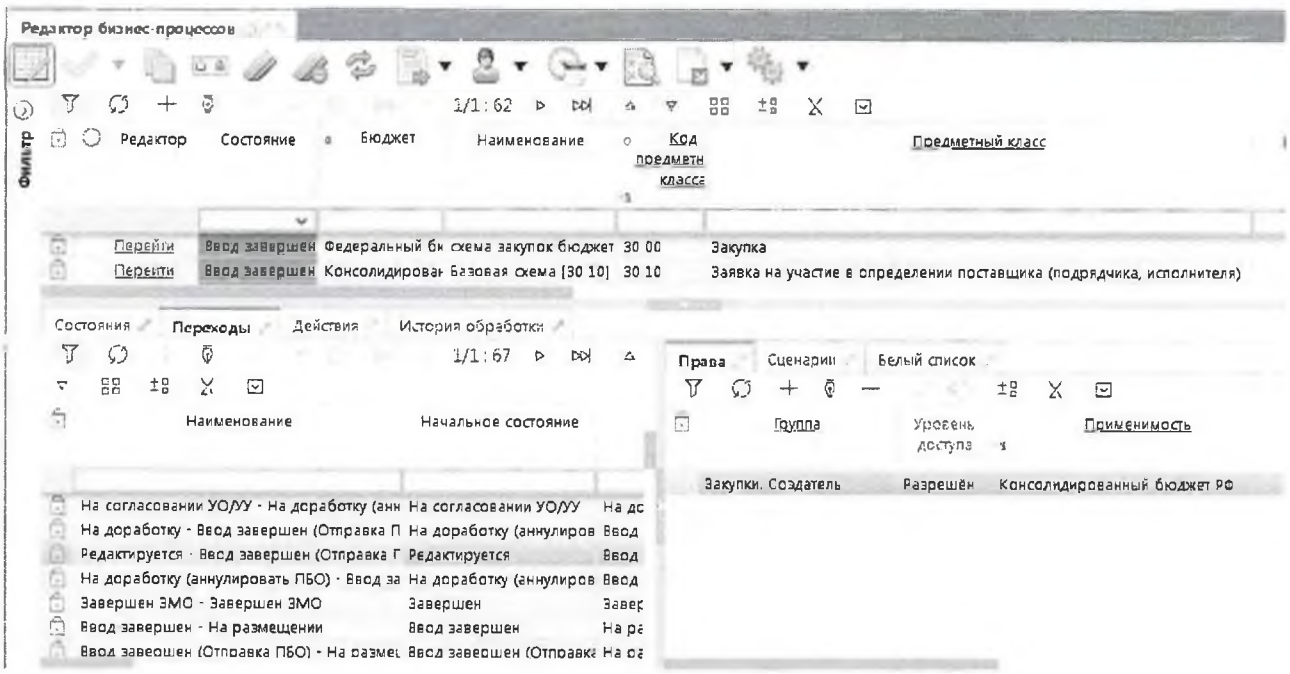


Рисунок 29 – Интерфейс «Редактор бизнес-процессов» детализация «Переходы»

Региональный администратор может добавить собственную строку прав: без галочки признака централизованности, указать свой бюджет и доназначить/исключить группу, как показано на рисунке 30. Это общий принцип назначения прав.

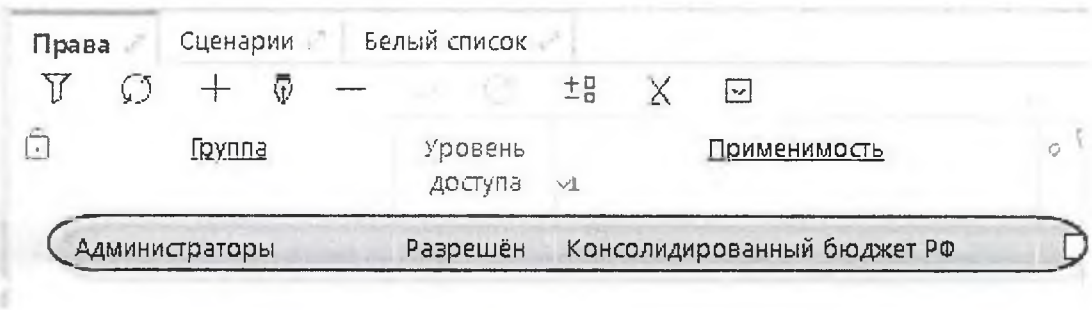


Рисунок 30 – Пример доназначения группы на переход

Для блокировки прав группам можно не только добавлять новую строку, но и менять атрибут «Уровень доступа» у существующих централизованных строк. Часто используется значение «Отсутствует», оно эквивалентно удалению строки.

Но так как централизованные строки региональный администратор удалять не может, то вместо этого используется такой прием: в «Уровень доступа» ставится «Отсутствует»

и данная строка права перестает использоваться при расчете прав.

На основании заданных прав на переходы система вычисляет права на действия. Упрощенно вычисления следующие: если действие содержит хотя бы один переход, на который у пользователя есть права, то это действие пользователь может выполнять. Система в соответствии с этим алгоритмом просчитывает для документа доступные действия и показывает в списке разрешенных действий.

12.2. Поатрибутное блокирование

Мы уже рассмотрели, как дать пользователям права на операции с документом – это функция регионального администратора. Часто приходится не только перекраивать группы на региональном уровне, но и изменять права на переходы, добавлять права новым группам, блокировать права существующим группам. Еще задача, которую должен решать администратор – определить атрибутный состав документа. Часто нужно открыть для редактирования (или закрыть) конкретные атрибуты документа. Если документ обрабатывается по бизнес-процессу, то это решается достаточно просто. Для настройки поатрибутного блокирования существуют две закладки.

Первая закладка – в детализации «Состояния» специальная детализация «Черный список». В основном, редактирование документа производится в начальном состоянии, в так называемом состоянии черновика. Черновик вводится, его редактирование завершается, потом документ подписывается, и последующее его редактирование уже ограничено и редактируется узкий ряд атрибутов (дата принятия, причина отклонения).

А в черновике, наоборот, редактируются практически все атрибуты, кроме некоторых, которые надо закрывать от редактирования в черновике.

Поэтому закладка называется «Черный список», т.к. для состояний запрещается редактирование. Администратору проще указать множество, которое надо запретить, чем множество, которое надо разрешить.

Как правило, «Черный список» используется для черновиков. В нем указываются колонки, которые редактируются на более поздних этапах. Например, дата принятия, код и текст причины отклонения, как показано на рисунке 31.

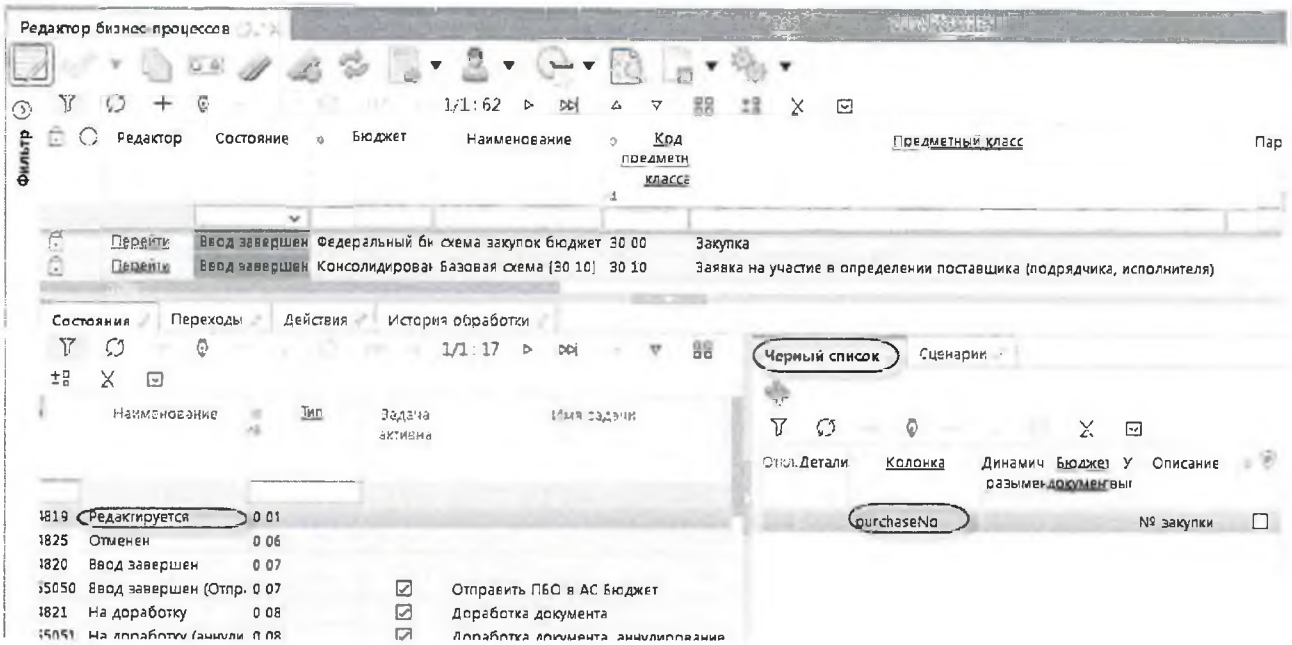


Рисунок 31 – «Черный список» для состояния «Вводится»

После задания в «черном списке» колонок необходимо нажать кнопку «Обновить кэш системы состояний». Пользователь при открытии формы увидит эти колонки заблокированными.

При необходимости администратор может расширить черный список и включить в него дополнительные колонки.

Есть особенность – так называемое право на ввод документа. Право на ввод документа в бизнес-процессах вычисляемое. Оно вычисляется на основании прав на переходы. Логика такая: если у пользователя есть право хотя бы на один переход из начального состояния, то пользователь имеет право на добавление документа.

В черновиках все атрибуты по умолчанию разрешены, во всех остальных состояниях все атрибуты по умолчанию запрещены (автоматически блокируются). Поэтому на последующих этапах обработки возникает обратная задача – открытие заблокированных атрибутов для редактирования. Это выполняется на второй закладке, расположенной в детализации «Переходы» специальная детализация «Белый список».

«Белый список» привязывается не к состояниям, а к переходам. Так сделано для повышения универсальности. Например, из состояния, в котором находится документ, можно документ принять или отклонить. Права могут быть настроены так, что у пользователя может не быть прав на действие «отклонение», могут быть права на действие «принятие». В этом случае, если бы белый список привязывался к состояниям, система не знала можно ли пользователю проставлять дату принятия или нет.

И для любого документа, вне зависимости от прав, дата принятия и код причины отклонения были бы открыты. А надо чтобы они были открыты для пользователей, которые имеют соответствующие права на принятия и отклонение. Поэтому удобнее белый список привязывать не к состояниям, а к переходам. Добавление в белый список производится как в черном списке.

Бывают случаи, когда недостаточно условия связанного с переходом. Пользователь для двух документов может иметь права на выполнение перехода, но в одном случае он должен менять атрибут, а в другом нет. Вот в таком случае можно воспользоваться дополнительным условием (поле «Условие выполнения» в белом списке).

«Условие выполнения» это декларативное правило. В редакторе декларативных правил есть аналог мастера функций, проверка синтаксиса.

Планируется доработать редактор декларативных правил и редактор java-скриптов – добавить предоставление информации о модели. Часто надо ссылаться на значение атрибутов. Например, чтобы получить ИНН учреждения надо взять документ, по документу получить учреждение, а у учреждения взять ИНН. Получается цепочка атрибутов, которые транзитивно следуют друг за другом. Чтобы задавать такие цепочки администратор должен знать модель. И чтобы облегчить жизнь администраторам, будет добавлен новый функционал, который будет поддерживать перечень атрибутов и иерархическое проваливание.

Примечание: В черном и белом списках кнопки добавления атрибутов по умолчанию не активны потому, что требуется перевести бизнес-процесс в состояние «На доработке» (нажать кнопку «Действия над документом» действие «Корректировать». Кнопки добавления + «Добавление по одному атрибуту», «Множественное добавление атрибутов» разблокируются. После завершения настройки бизнес-процесса надо не забыть перевести его в состояние «Ввод завершен» (по кнопке «Действия над документом» действие «Опубликовать»), после этого все изменения вступят в действие. При действии «Опубликовать» производится автоматический пересчет кэша, поэтому нажимать на зеленую кнопку «Обновить кэш системы состояний» не требуется.

Для закладки «Права» перевод в состояние корректировки не требуется.

12.3. Задачи обработки документов

Задачи обработки документов –это отдельная большая тема. Рассмотрим задачи обработки документов только в той части, которая касается прав.

Задачи обработки документов могут влиять на права. Например, если пользователь не является исполнителем по задаче, то документ для него будет заблокирован.

Задачи являются частью бизнес-процессов, конфигурируются в «Редакторе бизнес-процессов» на закладке «Состояния». Поля, отвечающие за конфигурацию задач: «Правило назначения исполнителя», «Модераторы задач», «Разрешение персонификации», «Неблокирующая задача».

Поля синего цвета, значит, они при установке обновлений системы не изменяются и можно делать региональные настройки, а бизнес-процесс при этом будет оставаться централизованным.

Для настройки этих полей требуется перевести бизнес-процесс в состояние «На доработке» (по кнопке «Действия над документом» действие «Корректировать») и выбрать режим редактирования пользовательских значений по кнопке «Режим редактирования пользовательских значений».

Рассмотрим, какие есть готовые способы назначения исполнителя у атрибута «Правило назначения исполнителя». Наиболее часто используемые правила назначения исполнителя:

- «Инициатор задачи» – пользователь, который перевел документ в определенное состояние и должен будет его обработать;
- «Сотрудники организации инициатора задачи». Исполнителями по задаче будет не только пользователь-инициатор задачи, но и все сотрудники организации. Удобно для документов, относящихся к области ответственности учреждений. Например, когда кто-то заболел, уехал в командировку, чтобы документы могли обработать другие сотрудники этого учреждения;
- «Сотрудники организации-распорядителя инициатора задачи». Документ может переходить из одной зоны ответственности в другую. Например, из зоны ответственности учреждения документ после подписания переходит в зону ответственности ГРБС для согласования. Тут можно определить исполнителя задачи по лицевому счету документа, а по нему определить ГРБС и назначить в качестве инициаторов задачи всех сотрудников этого ГРБС.

Если требуемого правила нет в централизованной поставке, то справочник может динамически дополняться на интерфейсе «Настраиваемые правила» администраторами без привлечения разработчика (правила настраиваются на java-скрипте).

После определения исполнителя задачи система имеет данные о правах на переходы и данные об исполнителе задачи. Система должна вычислить по этой информации кто может обрабатывать документ в текущем состоянии. Для администратора получается достаточно удобно. Исполнитель задачи назначается по общим правилам. Можно в качестве исполнителя задачи назначить конкретного пользователя, коллективно всех пользователей учреждения или всех пользователей отдела учреждения.

Задачи обработки не назначаются на группы, т.е. субъект права в отличие от остальной подсистемы прав здесь назначается немного по-другому: либо пользователям, либо через отдел, либо через учреждение. И когда надо указать больше одного пользователя, приходится указывать в целом учреждение. А потребность, например, в том, что документ должен обрабатывать руководитель конкретного учреждения или руководитель и главный бухгалтер этого учреждения. Получается, что по-отдельности ни права на переходы, ни права с использованием указания исполнителя задачи не могут решить проблему. При назначении прав на переходы указывается группа «Руководитель и главный бухгалтер», но в группу «Руководитель и главный бухгалтер» обычно входят руководители и главные бухгалтеры всех учреждений. И получается, что любой руководитель и любой главный бухгалтер любого учреждения сможет обработать документ. А делать отдельные группы для каждого учреждения – это достаточно трудоемко. С такими общими группами, которые включают в себя всех руководителей или всех бухгалтеров, задачу через права на переходы не решить. Указание исполнителя задач тоже не решает проблему из-за того, что учреждение можно указать, а вот выделить руководителя и бухгалтера нельзя. Но как только администратор начинает совмещать эти два подхода, получается простое решение проблемы – через права на переходы задаются права на группы «Руководитель», «Бухгалтер», через исполнителей задачи указывается организация, права совмещаются и получается то, что требуется – руководитель или бухгалтер учреждения имеют права на нужный документ.

Таким образом, с помощью совмещения этих двух механизмов значительно упрощается администрирование прав. Рассмотрим следующий атрибут «Модерирование задач». Мы назначили исполнителя задач, но на практике исполнитель заболел/в отпуске/в командировке/уволился, а задача назначена, документ должен кто-то обработать. Чтобы выйти из этого тупика необходимо привлекать администратора. В части задач такой администратор называется модератором задач. Это локальный администратор, которым может быть руководитель подразделения, назначенный ответственный сотрудник для таких ситуаций для каждого конкретного документа (для росписи может быть один человек, для платежных поручений по выплатам – другой и т.д.).

В централизованной поставке для простоты сделана одна группа «Модераторы задач». Администратор может включить в нее пользователя и этот пользователь будет модератором для всех документов. Если требуется назначить модератора задач отдельно для какой-то группы документов, то администратор должен сам создать соответствующую группу (модератор задач документов планирования, модератор задач кассовых документов и т.д.) и в соответствующем режиме бизнес-процесса администратор может изменить централизованную группу «Модераторы задач» на другую группу.

Пользователи, имеющие права модераторов задач, будут работать с кнопкой «Модерирование задач». Она есть на всех формах ввода первичных документов. Для модераторов разрешены следующие операции, как показано на рисунке 32:

— назначить задаче другого исполнителя (если исполнитель заболел, то может назначить обработку документа на другого исполнителя);
— удалить исполнителя (задача будет доступна всем пользователям, имеющим право на переход);
— восстановить исполнителя (первоначального исполнителя);
— закрепить задачу за собой.

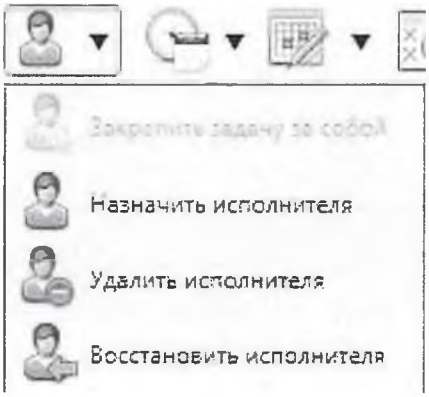


Рисунок 32– Действия, доступные по кнопке «Модерирование задач»

Кроме модератора, эта функция доступна также всем пользователям, обрабатывающим данный тип документа. Например, на обработку в отраслевой отдел пришли документы, требующие проверки. Т.к. документ пришел от учреждений в ФО, он пришел из другой зоны ответственности. В этом случае, нельзя автоматически определить исполнителя задач, и задача ставится в целом на отдел (все сотрудники отраслевого отдела будут иметь право на его обработку).

Когда один человек начал проверять документ, то другой пользователь, который ничего об этом не знает, тоже начнет проверять этот же документ. Для таких случаев предусмотрена функция «закрепить задачу за собой». Любой пользователь, который может обрабатывать документ, может нажать этот пункт, и для остальных пользователей, которые могли обработать документ, документ станет закрыт (появится замок). В «Редакторе бизнес-процессов» эта функция настраивается в атрибуте «Разрешение персонификации», как показано на рисунке 33. Как правило, разрешается исполнителям закреплять за собой практически все задачи.

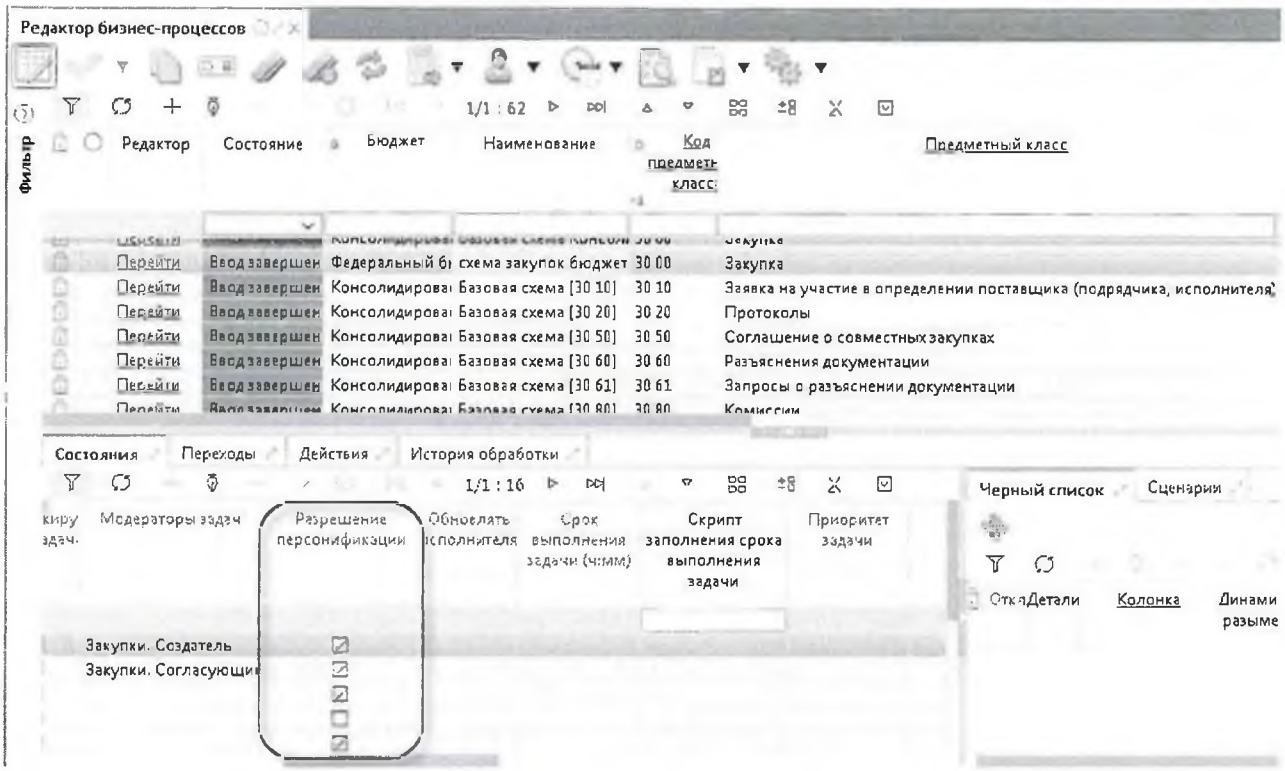


Рисунок 33 – Атрибут «Разрешение персонификации» в интерфейсе «Редактор бизнес-процессов»

Атрибут «Неблокирующая задача» используется, когда возникает необходимость делать задачи, но они не должны быть блокирующими. Есть задача, у неё есть исполнитель, но такая задача не должна учитываться при расчете прав на обработку документа.

В таком случае, ставится галка «Неблокирующая задача» у задачи, и исполнитель задачи перестает учитываться при расчете прав на обработку документа.

12.4. Специальные случаи задания прав

Основное назначение интерфейса «Права на классы», как показано на рисунке 34, – это запрет на редактирование экземпляров определенного класса на формах ввода. Указывается группа пользователей, предметный класс и/или имя класса модели.

В поле «Имя класса модели» можно явно задать имя или можно в конце написать звездочку «*» (это будет означать, что будут права на любой класс, который относится к данному пространству имен (имя которого начинается с этого префикса). Это сделано для того, чтобы можно было задавать права сразу на большую группу классов.

Поле «Уровни доступа» – помогает более гибко настраивать права. Например, если всем сотрудникам запретить права на большую группу классов, а потом подгруппе администраторов контрагентов выдать эксклюзивный доступ на класс банковских карт.

Поле «Применимость» используется для назначения прав на определенных бюджетах. Можно выдать запрет на все бюджеты, а потом в конкретных бюджетах начать раздавать права отдельным группам пользователей, чтобы получились разные права для разных бюджетов.

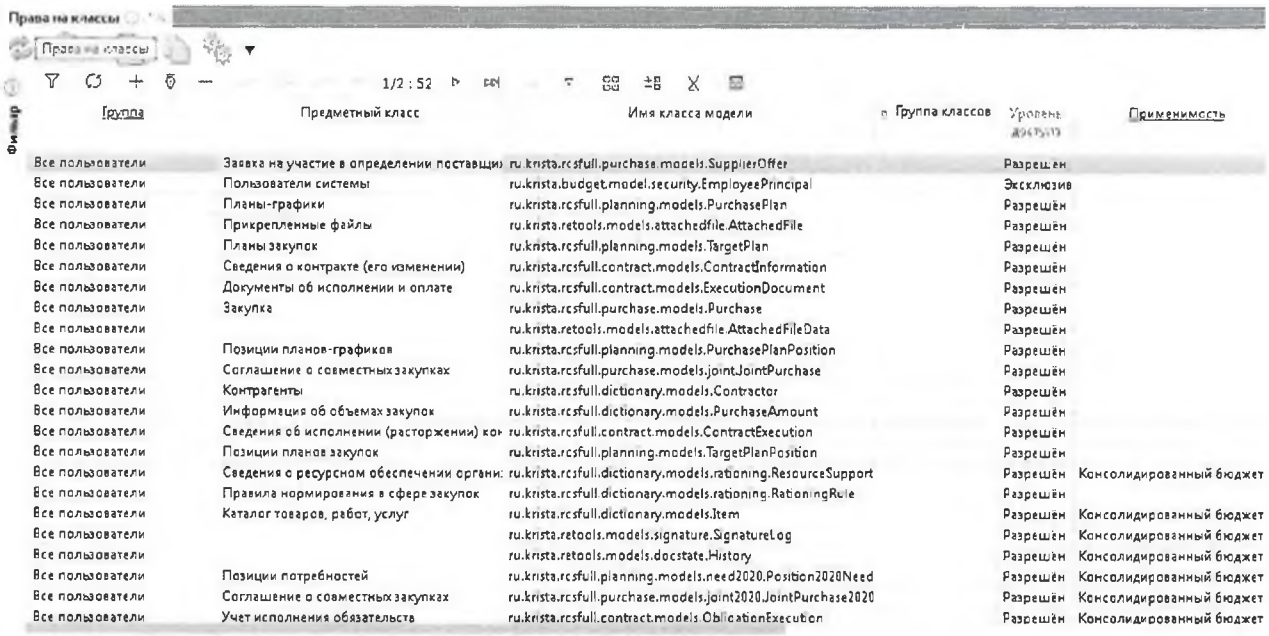


Рисунок 34 – Интерфейс «Права на классы»

13. Средства диагностики и рекомендации по решению проблем

Рассмотрим средства диагностики, которые предоставляет система.

Если администратор произвел настройку прав, но по каким-то причинам настройка не заработала, то требуется понять, что сконфигурировано неправильно.

Очень часто проблемы возникают из-за того, что администратор после внесения изменений забыл нажать «зеленую кнопку» кэшей прав (кэши прав не обновились и все осталось по-старому).

Рекомендации:

1. Сбросить кэш. Заходим на форму «Группы пользователей» и нажимаем на большую зеленую кнопку «Обновить права и группы». Эта кнопка сбрасывает все кэши (у подсистемы прав не один кэш).

2. Выйти и войти в систему заново.

Если проблема осталась, то:

3. Проверить текущие группы пользователя – в интерфейсе «Пользователи системы» в детализации «Группы пользователя» надо посмотреть все группы, в которые входит пользователь.

Примечание: пользователь тоже может самостоятельно посмотреть, в какие группы он входит, в интерфейсе «Сертификаты» по кнопке «Показать роли и группы текущего пользователя».

4. Проверить права пользователя в интерфейсе «Пользователи системы» в детализации «Права пользователя». Это мощный инструмент диагностики, который в удобном виде предоставляет администратору всю информацию, которая есть в кэше системы. Это та информация, по которой просчитываются права и которую видит подсистема прав из кэша прав.

По информации в детализации «Права пользователя» администратор видит, что состояние кэша старое (тогда просто обновляет кэш), либо видит, что на эту организацию нет прав (тогда в «Правах на видимость» смотрит, почему нет прав на организацию). Видит флаги, которые определяют профиль доступа, видит идентификаторы тех операций, которые задавали в формах прав на видимость. Если идентификаторы не соответствуют ожидаемым, то значит в «Правах на видимость» сделаны неверные настройки.

В детализации «Права пользователя» есть встроенный фильтр, который удобно использовать для поиска прав, как показано на рисунке 35.

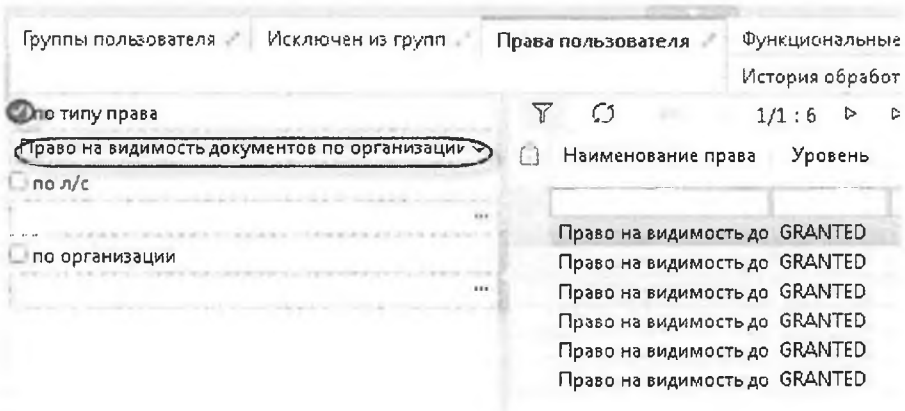


Рисунок 35 – Пример использования фильтра в детализации «Права пользователя» интерфейса «Пользователи системы»

5. Из-за того, что поддерживается вхождение групп пользователей в другие группы, могут получаться рекурсивные задания. Если администратор неверно сконфигурировал вхождение групп в группы и допустил рекурсию, то система может найти такие ошибки.

В интерфейсе «Группы пользователей» надо нажать специальную кнопку «Проверить корректность групп». Система строит граф групп и пытается найти петли в этом графе.

6. В «Правах на видимость» есть возможность задания правил, автоматизирующих конфигурирование прав на видимость. И этот этап можно продиагностировать и посмотреть, какой набор экземпляров метрики вернет правило.

Правила можно проверять по специальным кнопкам:  «Проверить правило»,  «Проверить все правила для данной группы пользователей», указав конкретного пользователя (контекст, который нам нужен). В результате, как показано на рисунке 36: видно, что указанный пользователь в рамках его бюджета в рамках его контекста (организации и т.д.) получит право на 1лицевой счет.

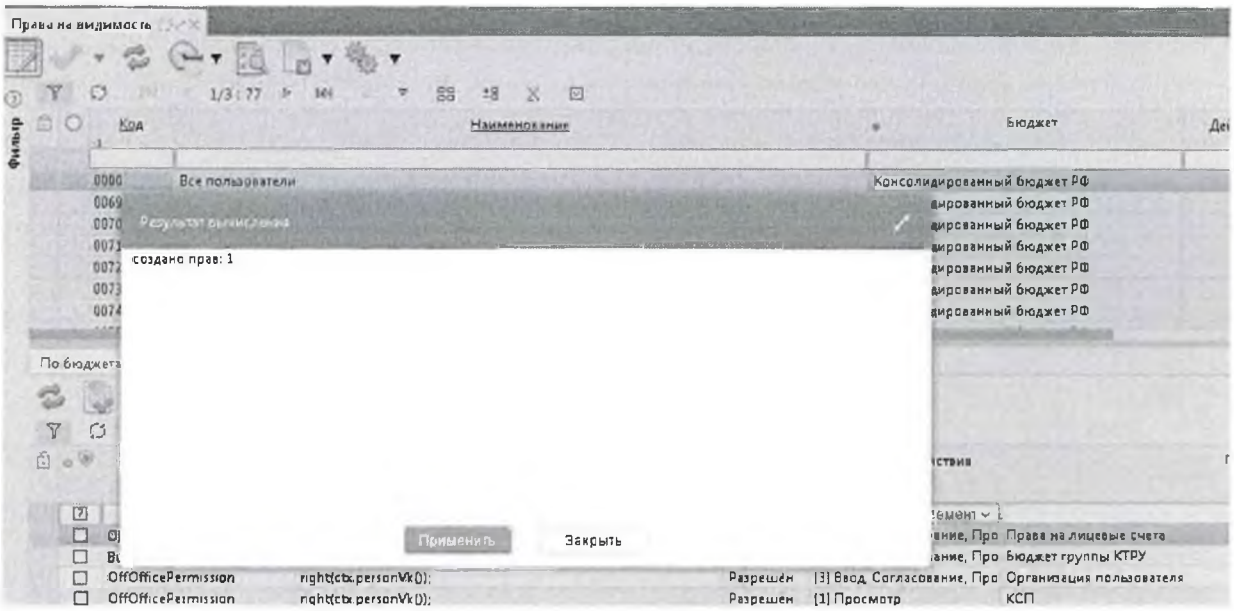


Рисунок 36 – Результат проверки правила

На практике часто получается, что в результате вычислений выводится 0 прав. Это значит, что пользователь, который обратился с проблемой, не получит прав ни на один счет бюджета, значит, наше правило настроено неверно и его надо исправить.

14. Менеджер блокировок

В интерфейсах есть поле «Индикатор блокировки», показано на рисунке 37– это менеджер блокировок.

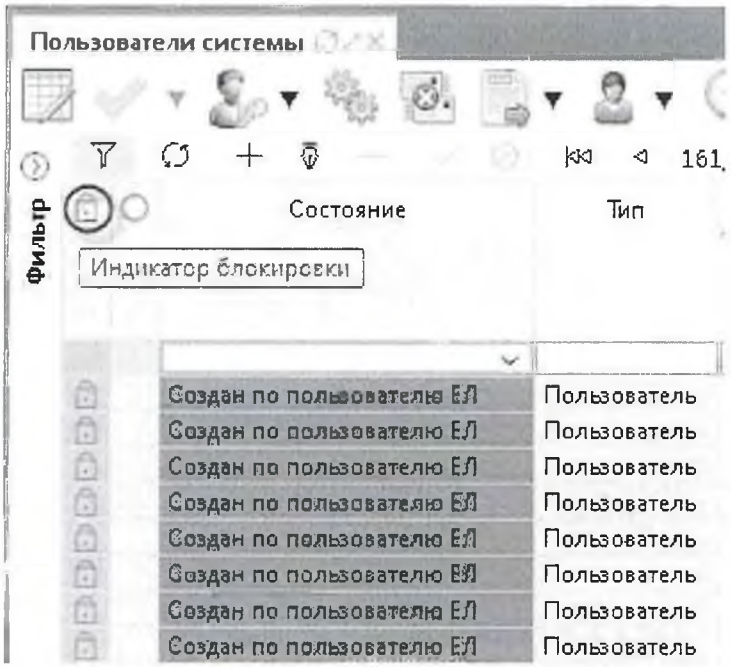


Рисунок 37 – Колонка «Индикатор блокировки»

Была проблема, что в разных местах проверялась возможность редактирования записи по-разному. Т.е. запись может быть заблокирована от редактирования по системе бизнес-процессов, по признаку централизованности, по праву на класс, с помощью поатрибутной блокировки и т.д. Т.е. много подсистем, которые могут запрещать нам что-либо делать. И возникает ситуация, когда у нас строчка заблокирована, а почему непонятно. С точки зрения программистов тоже плохо. Когда, например, необходимо показать кнопку, которая позволяет сделать вставку или позволяет автоматизированно отредактировать запись, то возникает проблема, как проверить, можно ли эту кнопку показывать, можно разрешать действие или нет.

Появилась потребность в менеджере блокировок, который бы мог централизованно дать ответ на вопрос: данная запись (данный объект) заблокирован? Если заблокирован, то что конкретно у него заблокировано (вставка, удаление, отняты права на редактирование или заблокированы конкретные атрибуты). Поэтому появился менеджер блокировок. Т.е. он работает не только с системой прав, но к нему подключаются провайдеры, которые обсчитывают блокировки из других подсистем.

Лог-менеджер –это объект, который позволяет себя расширять. У него есть ряд провайдеров, каждый провайдер отвечает за блокировки своего типа. Есть несколько подсистем, выполняющих блокировки и каждый провайдер отвечает за свою блокировку. Если нужно их расширять, то возможно написать свой провайдер, который будет добавлять новые блокировки. Менеджер их вместе объединит и в удобном виде отобразит в колонке «Индикатор блокировки». Пользователь, программист может узнать, почему заблокирована от изменений данная конкретная строка, как показано на рисунке 38.

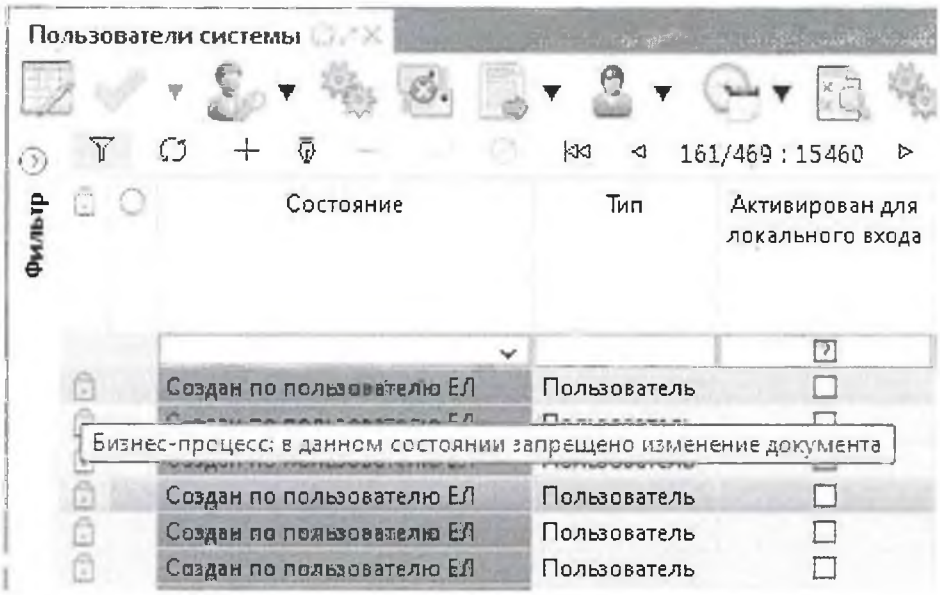


Рисунок 38 – Результат работы менеджера блокировок

Рассмотрим сообщение: «Бизнес-процесс: в данном состоянии запрещено изменение документа» – до двоеточия выводится наименование провайдера или подсистемы, которая заблокировала строку, а далее идет причина, почему конкретно эта подсистема заблокировала. Так можно однозначно понять, откуда взялась блокировка.

В списке может быть несколько строк – это значит, что документ попадает под несколько блокировок.

В тексте выводятся блокировки всей строки, блокировки на отдельные атрибуты в тексте не указываются.

Замок – визуальное отображение того, что есть блокировка. Серый замок – запрет на редактирование, желтый замок – запрет на переходы.

Перечень подсистем, которые могут блокировать:

— признак централизованности;

— система бизнес-процессов;

— подсистема прав на класс, на видимость;

— подсистема динамических связей (междокументная связь);

— поатрибутная блокировка.

Подсистема прав может сообщить:

— собственная блокировка –значит заблокировал текущий пользователь;

— блокировка по заголовку – пользователь находится в детали или в связанном документе, у которого заблокирован заголовок, и он каскадно получил эту блокировку;

— нет прав на изменение данного класса – заблокировано правами на класс;

— документ заблокирован по правам на ввод – заблокировано правами на ввод.

15. Подключение новых типов прав

Часто возникают задачи использовать подсистему прав для дополнительных классов объектов права (проектные классы), которых нет еще в системе.

Чтобы добавить новый тип права, надо работать с 5 сущностями.

Первая сущность – это сам новый тип права. Право – это объект, который описывает объект права и контекст обработки (что нужно делать с этим правом). Например, есть право на бюджет, и есть право на бюджет счета бюджета. И там, и там задается бюджет в качестве объекта права. Но в одном случае бюджет используется, как собственно право на бюджет, а в другом случае используется для выдачи права сразу на несколько счетов бюджета, которые принадлежат этому указанному бюджету. То есть объект один и тот же, но благодаря типу права понятно, что с этим объектом делать.

Кроме того, в праве присутствуют действия, которые можно с этим объектом сделать. Ранее были приведены примеры прав, они были, как правило, без действий, потому что там есть только одно действие (например, право на форму– форму можно только открыть), и такого
атрибута просто не требуется добавлять.

В самом праве нет указания на то, кто этим правом владеет. Права выдаются группам пользователей. Выдача прав конкретным субъектам производится с помощью форм, которые были рассмотрены ранее.

Чтобы добавить новый тип права надо создать класс с новым типом права, который мы унаследуем от java.security.Permission, или от некоторого шаблона. Например, очень многие права – это права на отдельно взятые объекты. Идентификатором этих объектов является первичный ключ ID, то есть, прямо может наследоваться от IdPermission.Фактически весь код класса сводится к тому, что этот класс наследуется от IdPermission и записывается конструктор.

Все остальное делается на уровне базовых классов. Фактически, класс права - это класс хранилища информации о том объекте, на которое выдано право. Плюс, возможно, действие, связанное с правом.

Единственный тонкий момент – это метод implies. Можно сказать, что метод implies очень похож на метод equals. Но у него есть некоторое отличие. Отличие заключается в том, что если взять право, у которого допустимо несколько действий, например, выдано право на видимость какого-то бюджета и указано действие, что можно видеть и редактировать, а потом спрашиваем, а можем ли мы это право видеть? Вот если включает, то implies, то true, мы можем сказать, что такое право есть. Таким образом, основной метод типа права это implies. В IdPermission он уже реализован.

Есть специальные предки и для прав на основе бюджетов, то есть те, которые оперируют не идентификатором ID, а те, которые оперируют иерархическими структурами. Таким образом, описать новый тип права не так сложно, если он укладывается в стандартные. Если он не стандартный, то писать придется немного побольше, но в общем тоже ничего сложного не будет.

Вторая сущность – это выдача прав. Описание того, как права распределяются по субъектам, кому какие права даются. Чаще всего в системе это делается с помощью «табличек». Есть целый ряд классов, описывающих эти «таблички». Если выбрать правильного предка в иерархии, то все будет унаследовано и описывать надо в соответствующем классе только ссылку на конкретный объект. Если это ссылка на бюджет, то надо её описать как ссылку на бюджет. Если бюджет с подчиненными, то тогда поставить галку, что с подчиненными.

Можно задавать эту связку не только в «табличках», но и любым другим способом. Некоторые права выдаются автоматически, то есть они могут генерироваться.

Третья сущность - источники политик. Это специальные классы, которые берут информацию из описаний, формируют политику с описанием кому какие права выданы во внутреннем формате системы. Таким образом, мы связываем способ задания прав для пользователя и механизмы, которые работают с этими правами внутри системы.

Механизмы, которые работают внутри системы, об этих «формочках» системы прав ничего не знают. Источник политик читает «табличку» и начинает формировать записи: этому пользователю мы даем такое-то право, этому такое-то и т.д. Политика возвращается и дальше она используется в системе. Когда появляется запрос: «Дай мне права для данного пользователя», система смотрит эти политики. В политике может указываться не конкретный пользователь, а группа пользователя, применимость (т.е. бюджет), и система смотрит, какие записи из этой политики могут быть применены к данному пользователю. Посмотрела, выбрала и теперь ей надо сформировать права. То есть объект RightInfoSourceформирует не права, а описания прав. Типы прав могут быть разными и иметь разные конструкторы. Система не знает, каким образом ей создать это право. Как работать с правом она знает, это объект, у которого есть метод implies, больше ей ничего знать в общем-то не надо.

Четвертая сущность – это фабрика. Фабрика умеет создавать права. Она берет описание права, которое вернул источник политик, и создает по нему право, которое помещается в список прав данного конкретного пользователя. Фабрика создает право, и, кроме того, она умеет создавать для конкретных прав коллекции прав. Зачем нам нужны коллекции прав? Ранее упоминалось, что практически на всех интерфейсах есть список уровней доступа. Коллекции прав как раз обрабатывают эти уровни доступа. То есть когда права помещаются в коллекцию прав, коллекция прав не сваливает все права в одну кучу, а в соответствии с правами доступа создает для себя несколько разделов. И когда требуется запросить право на самом деле не перебираются

все права подряд, потому что иначе никак не узнать, что, допустим, уровень запрета выше, чем уровень разрешения, или уровень эксклюзива еще выше. Решение подобных задач отдается коллекции. Когда запрашивается у коллекции: «а есть ли у пользователя такое право?», – коллекция начинает внутри себя перебирать права.

Перебирает она их в определенном порядке: сперва наиболее высокоприоритетные, потом менее приоритетные, и, наконец, самые низкоприоритетные. При этом коллекции могут перебирать эти права, используя ускорители. Например, если у нас идет право на объекты, которые описываются идентификатором ID, и кроме идентификатора у них вообще ничего нет (ни действий, ни дополнительных флажков), то можно все этиIDпросто сложить в один большой набор Set или Map и просто по ID дергать.

Проверить, имеется ли право на какой-то объект, получается очень быстро, даже если этих объектов миллионы. Ускоряется обработка, потому что для стандартных типов прав коллекции уже написаны (около 4 штук). Но если создавать уникальный тип права, то можно поддержать свою коллекцию, которая будет более быстро обрабатывать проверки на наличие права для данного конкретного типа прав. И указать это в фабрике, которая создает права. После этого право появится в системе.

Последняя сущность более информационная, она касается интерфейса «Пользователи системы» детализации «Права пользователя». В ней выводятся те права, которые есть у конкретного пользователя. Например, описание прав «по бюджету» содержит сам объект права «бюджет», HID и текстовое описание («городской округ»). Откуда берется эта информация? Для этого нужен последний объект, или последняя сущность - это потомок PermissionInfoProvider, точнее объект, реализующий этот интерфейс. Он описывает сами права, один PermissionInfoProvider зачастую описывает много типов прав (у нас всего их около 3 штук в системе), он возвращает описания для прав и умеет создавать резолверы для прав. Резолвер – это тот, кто преобразует идентификатор в строку описания для того, чтобы корректно показать в объекте права. Резолвер еще занимается тем, что выводит информацию о дополнительных флагах. Но флаги – разные для разных типов прав. А резолвер для конкретного типа права уже знает, он может посмотреть на право, сформировать строчку описания, вернуть и таким образом мы на интерфейсе увидим понятную человеку информацию (рисунок 39). А не просто object. object, т.к. система не знает, что это такое.

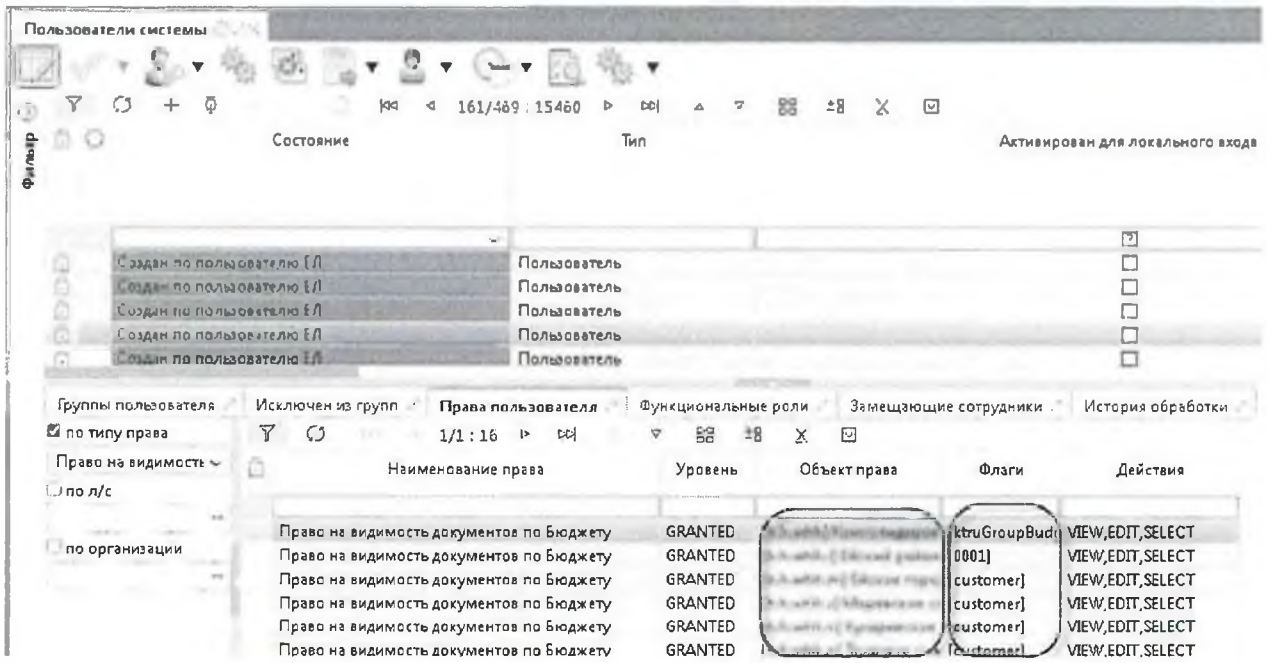


Рисунок 39 – Вывод текстового описания

Это 5 сущностей, которые надо создать, поддержать для того, чтобы появился новый тип права в системе.

16. Описание интерфейсов подсистемы прав

16.1. Интерфейс «Права на формы ввода»

Интерфейс предназначен для настройки рабочих мест/групп интерфейсов (объединение интерфейсов в группы, определение отображаемого названия и порядка следования в навигаторе и т.д.) и назначения прав доступа на эти интерфейсы пользователям или группам пользователей. Как показано на рисунке 40.

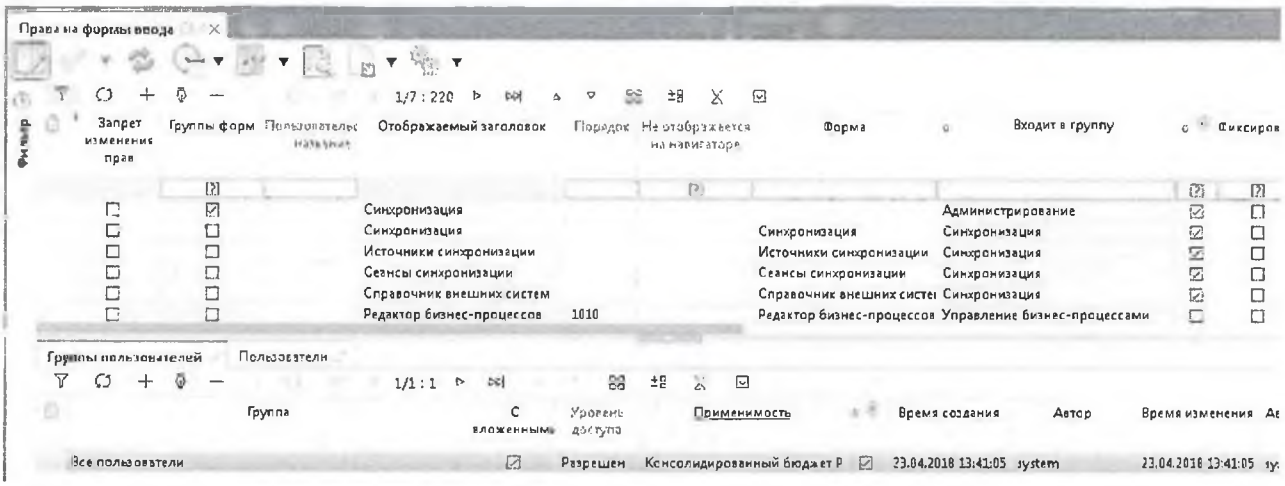


Рисунок 40 – Интерфейс «Права на формы ввода»

В детализации данного интерфейса можно назначать права, как на определенную группу пользователей, так и на конкретного пользователя системы.

Детализация «Группы пользователей» содержит следующий перечень колонок:

- «Группа». В данной колонке выбирается необходимая группа пользователей;
- «С вложенными». Данный признак означает, что права будут назначены не только для текущей группы, но и для всех групп, вложенных в нее;
- «Уровень доступа». Данная колонка может изменяться региональным администратором и после обновления системы изменения, внесенные администратором, не будут исправлены. Колонка принимает следующие значения:
  - отсутствует (выбранная группа пользователей не будет учтена подсистемой прав);
  - разрешен (выбранной группе дается право на форму ввода);

- запрещен (запрещает выбранной группе пользователей доступ);
- эксклюзивный (перекрывает запрет для группы, имеет приоритет выше, чем у значения «Запрещен»);

— «Применимость». Данная колонка позволяет вносить изменения локально, которые будут касаться пользователей указанного бюджета;

— «Признак централизованности». Если значение «true», то данная строка является централизованной (одинакова для предметной системы во всех регионах), если «false» – пользовательской (настраивается только для конкретного региона);

— «Время создания». Время создания записи;

— «Автор». Автор созданной записи;

— «Время изменения». Время последнего изменения записи;

— «Автор изменения». Автор последнего изменения записи.

Детализация «Пользователи» содержит следующий перечень колонок:

— «Пользователь». Выбор конкретного пользователя, для которого необходимо назначить права;

— «ФИО». Поле заполняется автоматически исходя из заданного в колонке «Пользователь»;

— «С вложенными». Данный признак означает, что права будут назначены не только для текущей группы, но и для всех групп, вложенных в нее;

— «Организация». Поле заполняется автоматически исходя из заданного в колонке «Пользователь»;

— «Уровень доступа». Данная колонка может изменяться региональным администратором и после обновления системы изменения, внесенные администратором, не будут исправлены. Колонка принимает следующие значения:

- отсутствует (выбранная группа пользователей не будет учтена подсистемой прав);
- разрешен (выбранной группе дается право на форму ввода);
- запрещен (запрещает выбранной группе пользователей доступ);
- эксклюзивный (перекрывает запрет для группы, имеет приоритет выше, чем у значения «Запрещен»);

— «Время изменения». Время последнего изменения записи;

— «Автор изменения». Автор последнего изменения записи.

16.2. Интерфейс «Декларативные правила»

Интерфейс предназначен для задания условий на формы ввода, которые будут проверяться при вводе новой записи на интерфейсе, а также для настройки ограничения набора значений в модальных справочниках, вызываемых на формах ввода (для записей, удовлетворяющих заданным условиям). На данном интерфейсе можно настраивать права для тех групп, на которых выбранное декларативное правило не должно распространяться, как показано на рисунке41«Декларативные правила».

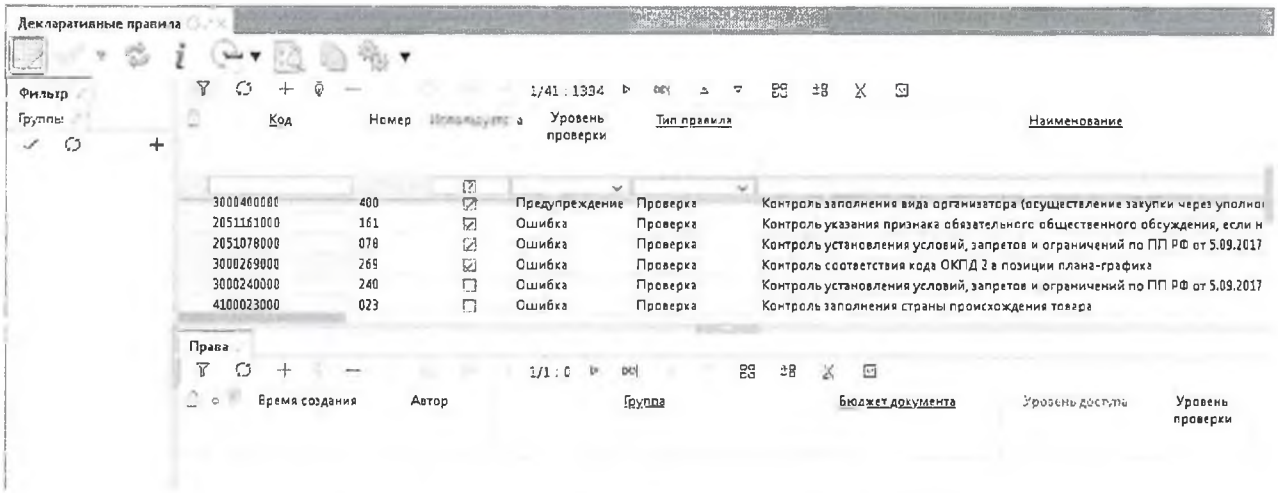


Рисунок 41 – Интерфейс «Декларативные правила»

В детализации данного интерфейса можно назначать права на определенную группу пользователей системы. Детализация «Права» содержит следующий перечень колонок:

— «Группа». В данной колонке выбирается необходимая группа пользователей;

— «Признак централизованности». Если значение «true», то данная строка является централизованной (одинакова для предметной системы во всех регионах), если «false» – пользовательской (настраивается только для конкретного региона);

— «Уровень доступа». Данная колонка может изменяться региональным администратором и после обновления системы изменения, внесенные администратором, не будут исправлены. Колонка принимает следующие значения:

- отсутствует (выбранная группа пользователей не будет учтена подсистемой прав);
- запрещен (запрещает выбранной группе пользователей доступ);
- эксклюзивный (перекрывает запрет для группы, имеет приоритет выше, чем у значения «Запрещен»);

— «Применимость». Данная колонка позволяет вносить изменения локально, которые будут касаться пользователей указанного бюджета;
— «Уровень проверки». Колонка принимает следующие значения:
  – пустое значение (полностью отключает проверку);
  – ошибка (будет срабатывать только предупреждение);
  – предупреждение (будет срабатывать только ошибка);
— «Время создания». Время создания записи;
— «Автор». Автор созданной записи;
— «Время изменения». Время последнего изменения записи;
— «Автор изменения». Автор последнего изменения записи.

16.3. Интерфейс «Администратор печатных форм»

Интерфейс содержит перечень печатных форм документов (формируемых непосредственно на интерфейсах Системы) и настройки для каждой из них (с использованием режима многобюджетности), как показано на рисунке 42 «Администратор печатных форм».

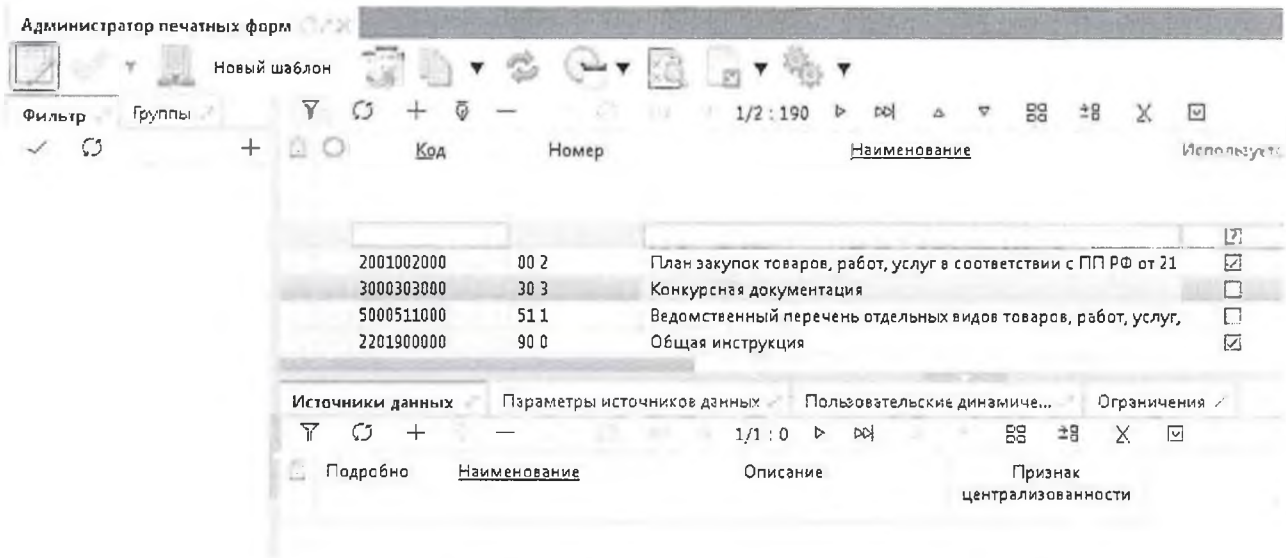


Рисунок 42 – Интерфейс «Администратор печатных форм»

В детализации «Права» данного интерфейса можно назначать права, как на определенную группу пользователей, так и на конкретного пользователя системы. Детализация «Декларативные правила» содержит следующий перечень колонок:

— «Группа». В данной колонке выбирается необходимая группа пользователей;

— «Признак централизованности». Если значение «true», то данная строка является централизованной (одинакова для предметной системы во всех регионах), если «false» – пользовательской (настраивается только для конкретного региона);
— «Уровень доступа». Данная колонка может изменяться региональным администратором и после обновления системы изменения, внесенные администратором, не будут исправлены. Колонка принимает следующие значения:
  - отсутствует (выбранная группа пользователей не будет учтена подсистемой прав);
  - запрещен (запрещает выбранной группе пользователей доступ);
  - эксклюзивный (перекрывает запрет для группы, имеет приоритет выше, чем у значения «Запрещен»);
— «Применимость». Данная колонка позволяет вносить изменения локально, которые будут касаться пользователей указанного бюджета;
— «Время создания». Время создания записи;
— «Автор». Автор созданной записи;
— «Время изменения». Время последнего изменения записи;
— «Автор изменения». Автор последнего изменения записи.

16.4. Интерфейс «Группы пользователей»

Интерфейс «Группы пользователей» является базовым интерфейсом субъектов права. В большинстве случаев права задаются на определенные группы, а не на конкретных пользователей. Все группы в справочнике делятся на централизованные (одинаковы для предметной системы во всех регионах) и нецентрализованные (специфичные группы, предназначенные для конкретного региона).

Наполнение групп возможно несколькими способами:

— на вкладке «Пользователи» задаются конкретные пользователи, входящие в группу (добавление пользователя на этой вкладке будет рассматриваться приоритетнее относительно других вкладок);
— на вкладке «Группы» добавляются вложенные группы. При добавлении вложенной группы для нее необходимо указать бюджет в поле «Применимость» (группа будет использоваться только для пользователей, входящих в указанный бюджет);
— на вкладке «Подразделения» происходит расширение группы всеми сотрудниками, входящими в подразделение;

— на вкладке «Учреждения» происходит расширение группы всеми сотрудниками, входящими в учреждение;

— на вкладке «Правила» задается правило для автоматического включения пользователя в группу. Само правило задается на декларативном языке в редакторе. В окне редактора существует возможность поиска конкретной функции по названию в строке поиска, либо по категории, как показано на рисунке 43.

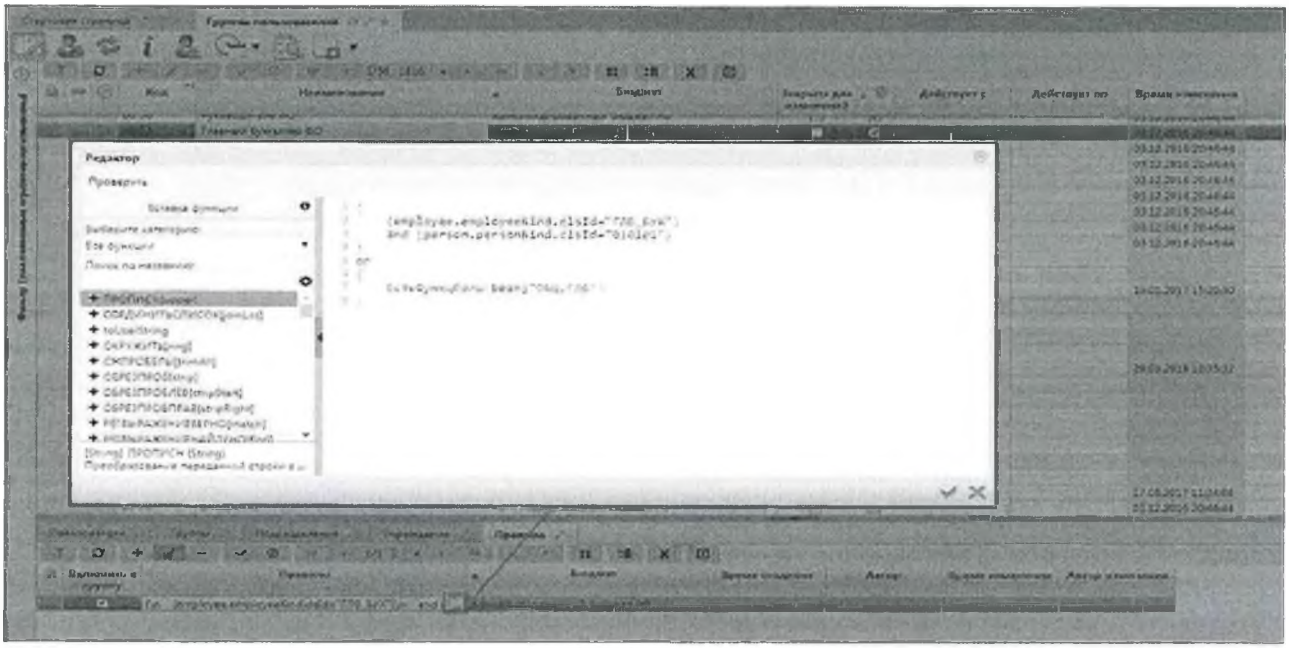


Рисунок 43 – Редактор правила

После наполнения группы пользователей для того, чтобы изменения вступили в силу необходимо на панели инструментов поочередно нажать кнопки  «Обновить группы пользователей»,  «Обновить права и группы», которые вызывают пересчет кэшей.

16.5. Интерфейс «Пользователи системы»

На интерфейсе «Пользователи системы» содержатся учетные записи пользователей (субъекты права), имеющих доступ к системе, как показано на рисунке 44. Справочник «Пользователи системы» позволяет управлять пользователями системы в части:

— активации/деактивации их учетных записей;

— отслеживать в каком состоянии на текущий момент времени находится учетная запись, каким образом она была активирована;

— управлять временем действия одноразовых паролей;

— менять тип учетной записи;

— просматривать группы, в которых пользователь состоит, его права и функциональные роли.

Если у пользователя системы нет привязки к организации и к бюджету, то у такого пользователя учитываются только те права, которые назначены на консолидированный бюджет РФ.

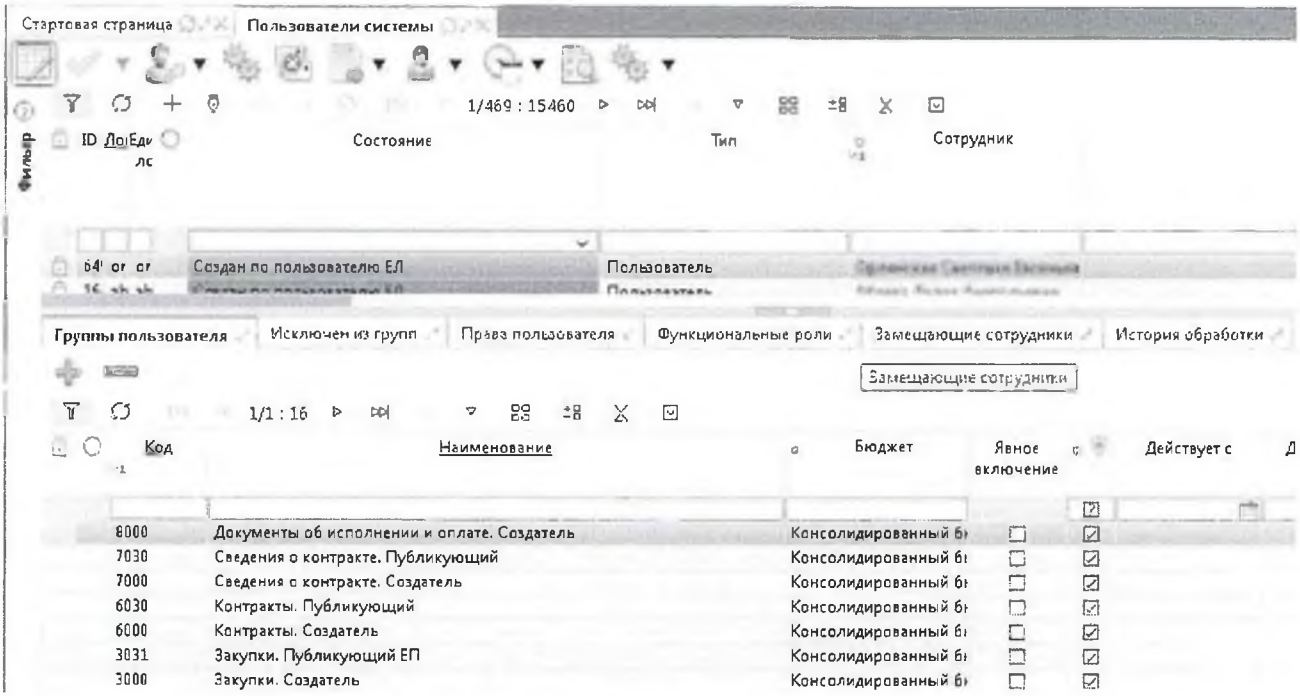


Рисунок 44 – Интерфейс «Пользователи системы»

В детализации «Группы пользователей» отображаются все группы, в которые включен пользователь без возможности добавления.

В детализации «Права пользователя» отображаются права для работы в системе, которые доступны пользователю.

В детализации «Функциональные роли» существует возможность добавления, удаления пользователю функциональных ролей для работы с системой. Эти роли представляют собой упрощенный способ назначения прав пользователю работы с системой.

В детализации «История обработки» показан список действия, которые производили с учетной записью пользователя.

16.6. Интерфейс «Права на видимость»

Интерфейс «Права на видимость» аналогичен интерфейсу «Группы пользователей». Права на видимость формируются вместе с созданием групп, при этом сразу же задаются права по умолчанию, как показано на рисунке 45.

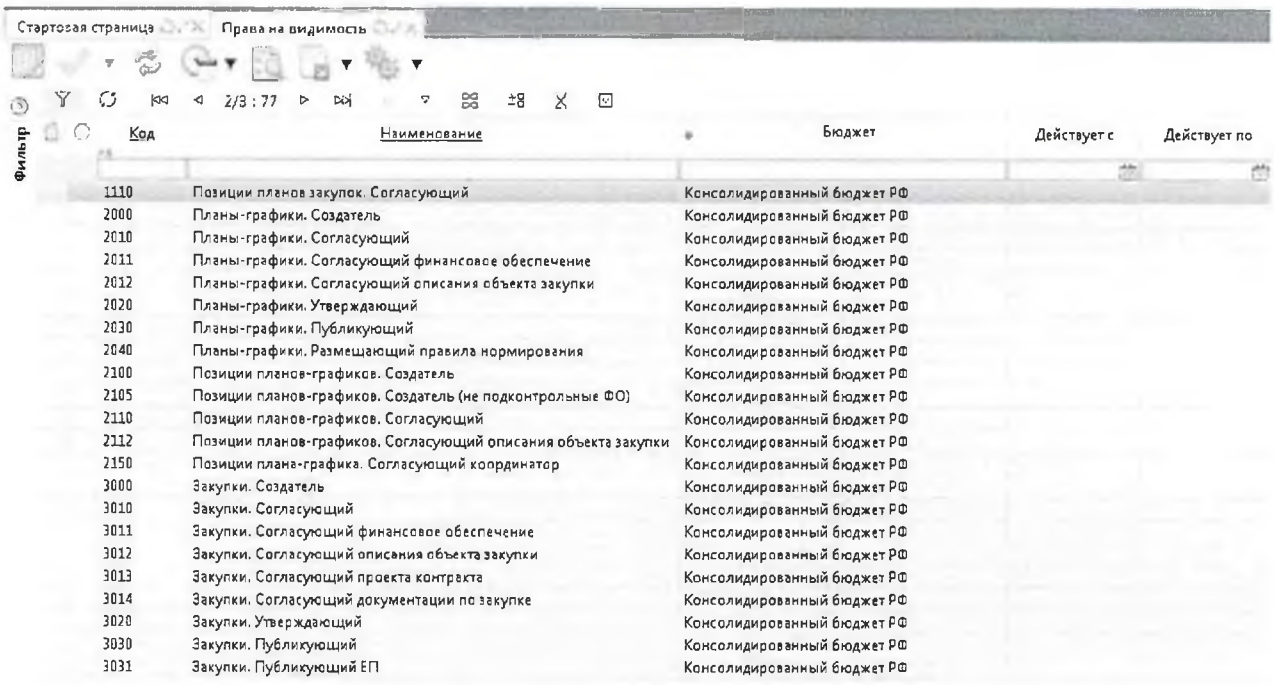


Рисунок 45 – Интерфейс «Права на видимость»

В детализации данного интерфейса можно назначать права на видимость в разрезе бюджетов, организаций, лицевых счетов, кодов глав, состояний, счетов обслуживаемых бюджетов, категорий документов.

16.6.1. Детализация «По бюджетам»

В детализации «По бюджетам», как показано на рисунке 46, в качестве объекта права выступает перечень бюджетов, на который настраиваются права на видимость.

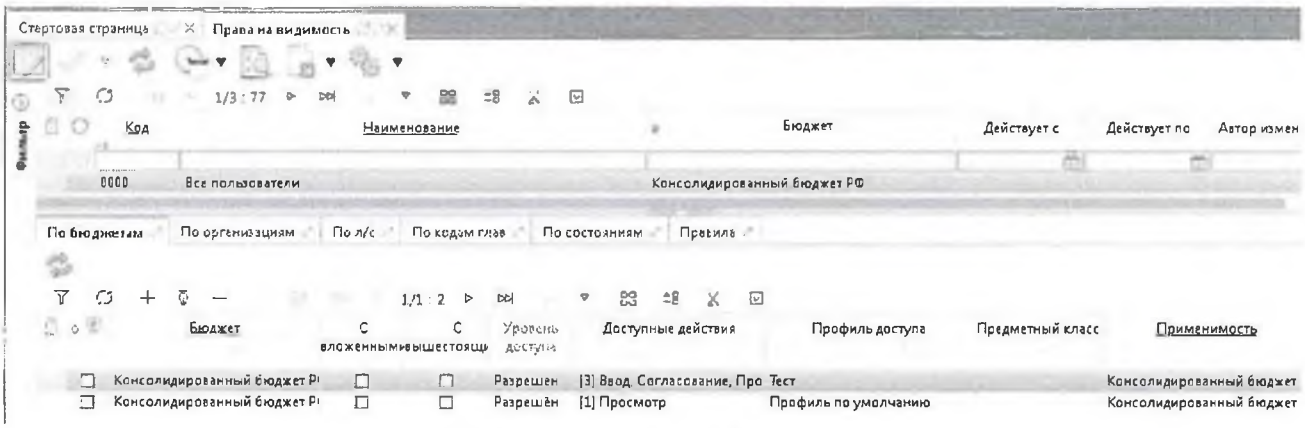


Рисунок 46 – Детализация «По бюджетам»

Детализация «По бюджетам» содержит следующий перечень колонок:

— «Признак централизованности». Если значение «true», то данная строка является централизованной (одинакова для предметной системы во всех регионах), если «false» – пользовательской (настраивается только для конкретного региона);

— «Бюджет». В данной колонке выбирается необходимая бюджет, в разрезе которых будут заданы права на видимость;
— «С вложенными». Установление флага-галки в колонке означает, что можно выполнять какие-либо действия не только для текущего бюджета, но и всех, вложенных в него. Как правило, такие права задаются, например, для группы «Сотрудники ФО», т.е. они могут выполнять действия, как в рамках своего бюджета, так и всех нижестоящих;
— «С вышестоящими». Установление флага-галки в колонке означает, что будут доступны действия в рамках указанного бюджета и всех вышестоящих. Зачастую, такие права назначаются для просмотра справочников, заведенных на уровне вышестоящего бюджета;
— «Уровень доступа». Данная колонка может изменяться региональным администратором и после обновления системы изменения, внесенные администратором, не будут исправлены. Колонка принимает следующие значения:
  - Отсутствует (выбранная группа пользователей не будет учтена подсистемой прав);
  - Запрещен (запрещает выбранной группе пользователей доступ);
  - Эксклюзивный (перекрывает запрет для группы, имеет приоритет выше, чем у значения «Запрещен»);
— «Доступные действия». Содержит перечень действий, которые предоставляются группе пользователей в разрезах, используемых для настройки прав на видимость. Как и уровни доступа, эти права расположены по возрастанию:
  - «Просмотр» – просмотр, без возможности изменения записей, самое минимальное право;
  - «Согласование» – возможность согласования документов;
  - «Ввод» – право на ввод данных;
— «Применимость». В данной колонке указывается наименование бюджета, на который данные настройки будут распространены;
— «Время создания». Время создания записи;
— «Автор». Автор созданной записи;
— «Время изменения». Время последнего изменения записи;
— «Автор изменения». Автор последнего изменения записи.

16.6.2. Детализация «По организациям»

Вкладка «По организациям», показана на рисунке 47, предназначена для задания прав непосредственно по организациям: организация-распорядитель, ЦБ и самаорганизация.

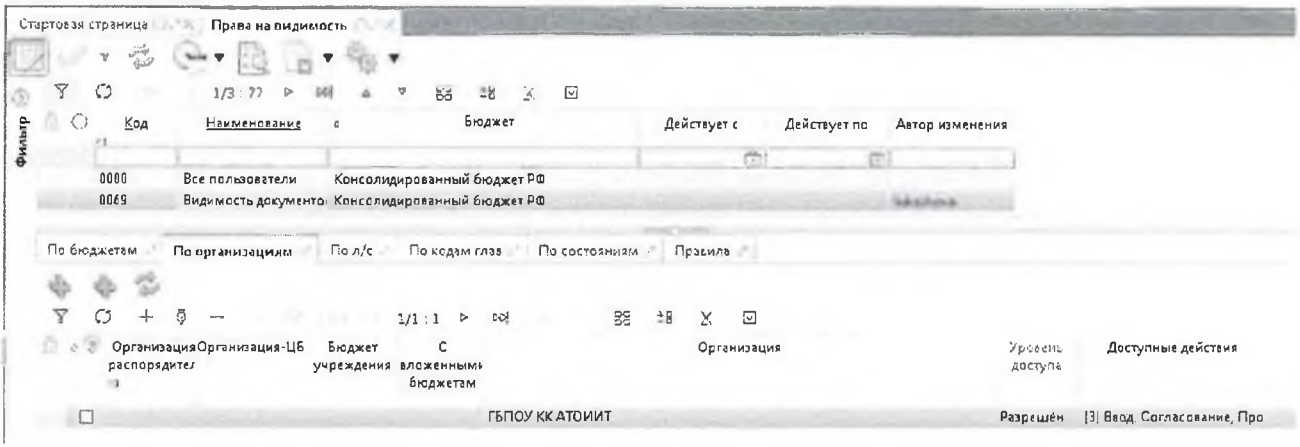


Рисунок 47 – Детализация «По организациям»

Детализация «По организациям» содержит следующий перечень колонок:

- «Признак централизованности». Если значение «true», то данная строка является централизованной (одинакова для предметной системы во всех регионах), если «false» – пользовательской (настраивается только для конкретного региона);
- «Организация-распорядитель». В этой колонке добавляется организация, которая является распорядителем. В этом случае права назначаются на все подведомственные учреждения;
- «Организация-ЦБ». Выбрав организацию в этой колонке, выдаются права на учреждения, которые обслуживаются в этой организации;
- «Бюджет учреждения». Установление флага-галки в колонке означает, что будут доступны действия в рамках указанного бюджета и всех вышестоящих. Зачастую, такие права назначаются для просмотра справочников, заведенных на уровне вышестоящего бюджета;
- «Организация». Выбор конкретной организации, которой необходимо назначить права;
- «Уровень доступа». Данная колонка может изменяться региональным администратором и после обновления системы изменения, внесенные администратором, не будут исправлены. Колонка принимает следующие значения:
  - Отсутствует (выбранная группа пользователей не будет учтена подсистемой прав);
  - Разрешен (выбранной группе дается право на форму ввода);

- Запрещен (запрещает выбранной группе пользователей доступ);
- Эксклюзивный (перекрывает запрет для группы, имеет приоритет выше, чем у значения «Запрещен»);

— «Доступные действия». Содержит перечень действий, которые предоставляются группе пользователей в разрезах, используемых для настройки прав на видимость. Как и уровни доступа, эти права расположены по возрастанию:

- «Просмотр» – просмотр, без возможности изменения записей, самое минимальное право;
- «Согласование» – возможность согласования документов;
- «Ввод» – право на ввод данных;

— «Применимость». В данной колонке указывается наименование бюджета, на который данные настройки будут распространены;

— «Профиль доступа». Управление профилями доступа в разрезе организаций предназначено для случаев, когда у одного учреждения в зависимости от выполняемых им функций (заведение платежных поручений, ведение сводной бюджетной росписи и др.) доступны разные списки организаций:

- «По умолчанию» – учреждению даны права только на себя;
- «Доведение до подведомственных (до РБС, ПБС)» – учреждению даны права на распределенные бюджетные данные, их дальнейшее доведение (при наличии);
- «Распределение с ГРБС и РБС» – учреждению дано права указывать организацию, как своего главного распорядителя;
- «Утверждение на ГРБС» – право дается группе пользователей, для утверждения бюджетных данных на ГРБС;

— «Время создания» – время создания записи;

— «Автор» – автор созданной записи;

— «Время изменения» – время последнего изменения записи;

— «Автор изменения» – автор последнего изменения записи.

16.6.3. Детализация «По лицевым счетам», «По кодам глав», «По состояниям»

Вкладка «По лицевым счетам» аналогична предыдущим, и предназначена для задания прав на лицевые счета. При неуказании значения в поле «Л/св ФО», организация-распорядитель, ЦБ и сама организация будут иметь права на все счета в соответствии с настройкой.

Вкладка «По кодам глав» предназначена для задания прав в соответствии с кодами глав.

Вкладка «По состояниям» предназначена для скрытия прав пользователей на видимость промежуточных стадий согласования документа при переходе по бизнес-процессу. Для предоставления Администратору права на видимость необходимо выбрать состояние, указать для всех групп пользователей уровень доступа «Запрещен», а для Администратора – «Эксклюзивный».

16.6.4. Детализация «Правила»

Вкладка «Правила» одна из ключевых закладок, которая используется на задание прав на видимость. Она предназначена для указания всех правил, которые задаются для пользователей, входящих в указанную группу. Написание правила является универсальными инструментом для всех баз, в отличие от явного назначения прав на конкретный бюджет либо конкретную организацию, дающие права только на той базе, в которой они были назначены. Все заполняемые на вкладке правила пишутся системным администратором, и являются общими для всех централизованных систем, как показано на рисунке 48.

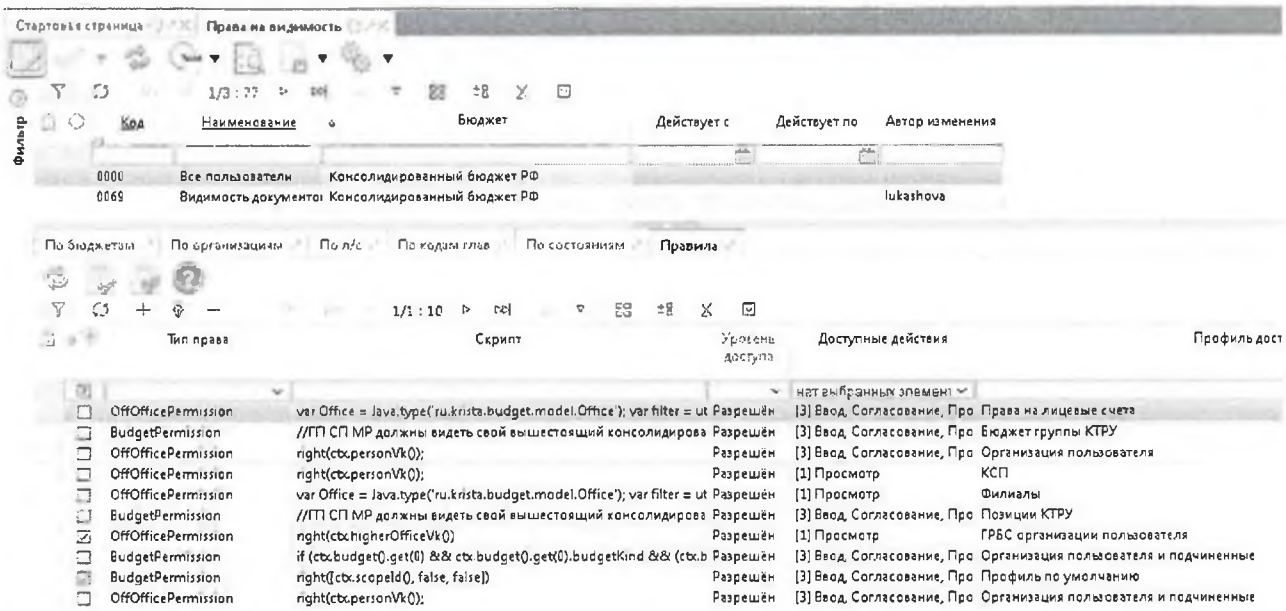


Рисунок 48 – Детализация «Правила»

Детализация «Правила» содержит следующий перечень колонок:

— «Признак централизованности». Если значение «true», то данная строка является централизованной (одинакова для предметной системы во всех регионах), если «false» – пользовательской (настраивается только для конкретного региона);

— «Тип права»;

— «Скрипт». Содержит java-скрипт и является основой любого правила. По нажатию на кнопку  «Описание правил» на панели инструментов детализации, администратор, заполняющий правило, получит краткую справку по основным функциям, используемым в java-скрипте;

— «Уровень доступа». Данная колонка может изменяться региональным администратором и после обновления системы изменения, внесенные администратором, не будут исправлены. Колонка принимает следующие значения:

- Отсутствует (выбранная группа пользователей не будет учтена подсистемой прав);
- Разрешен (выбранной группе дается право на форму ввода);
- Запрещен (запрещает выбранной группе пользователей доступ);
- Эксклюзивный (перекрывает запрет для группы, имеет приоритет выше, чем у значения «Запрещен»);

— «Доступные действия». Содержит перечень действий, которые предоставляются группе пользователей в разрезах, используемых для настройки прав на видимость. Как и уровни доступа, эти права расположены по возрастанию:

- «Просмотр» – просмотр, без возможности изменения записей, самое минимальное право;
- «Согласование» – возможность согласования документов;
- «Ввод» – право на ввод данных;

— «Примечание». Пояснение того, что означает тот или иной тип права;

— «Профиль доступа». Управление профилями доступа в разрезе организаций предназначено для случаев, когда у одного учреждения в зависимости от выполняемых им функций (заведение платежных поручений, ведение сводной бюджетной росписи и др.) доступны разные списки организаций:

- «По умолчанию» – учреждению даны права только на себя и свой лицевой счет;
- «Доведение до подведомственных (до РБС, ПБС)» – учреждению даны права на распределенные бюджетные данные, их дальнейшее доведение (при наличии);
- «Распределение с ГРБС и РБС» – учреждение дано права указывать организацию, как своего главного распорядителя;
- «Утверждение на ГРБС» – право дается группе пользователей, для утверждения бюджетных данных на ГРБС;

— «Применимость». В данной колонке указывается наименование бюджета, на который данные настройки будут распространены;

— «Время изменения». Время последнего изменения записи;

— «Логин автора изменения». Логин автора последнего изменения записи.

На данной вкладке предусмотрены специальные кнопки, позволяющие выполнять проверку правил. Проверка правил заключается в открытии модального окна справочника «Пользователи», с отфильтрованным списком пользователей, которым доступны права, в соответствии с правилами – «Проверить правило» и «Проверить все правила для данной группы пользователей».

16.7. Интерфейс «Доступ к предметным классам»

Интерфейс, показан на рисунке 49, предназначен для конфигурирования ограничений доступа и фильтрации значений предметных классов по назначенным правам.

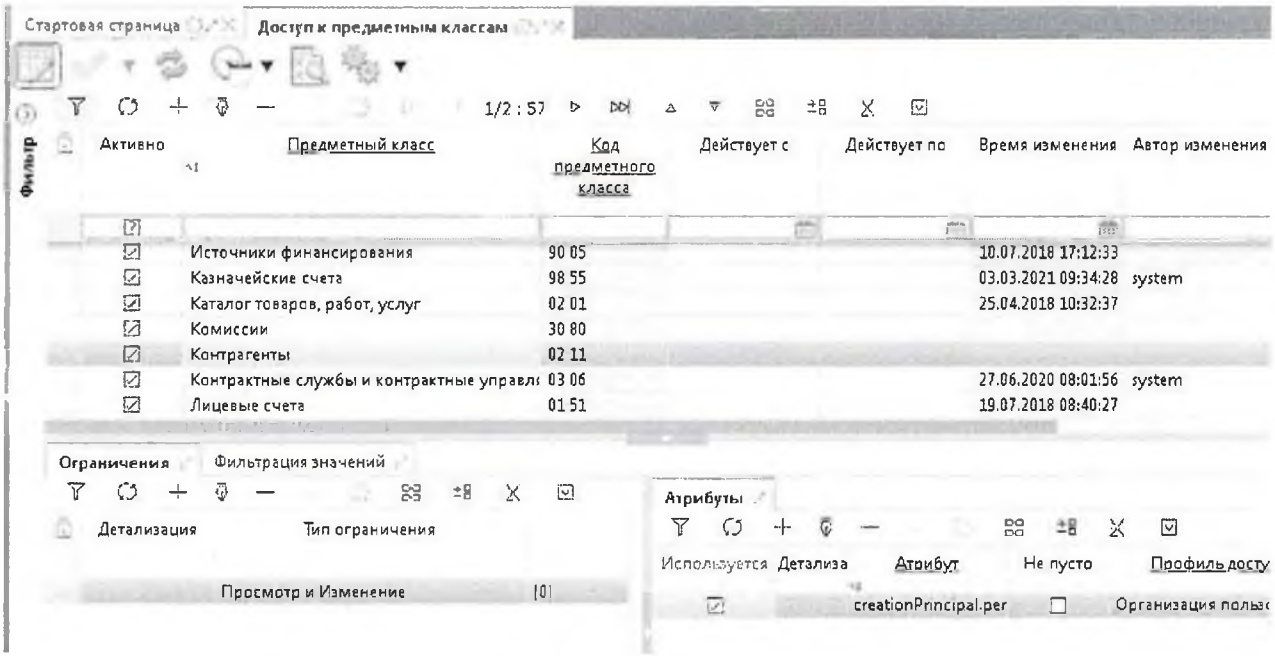


Рисунок 49 – Интерфейс «Доступ к предметным классам»

В детализации «Ограничения» происходит настройка ограничений в выбранном предметном классе по следующим атрибутам:

— «Детализация». Выбор области на интерфейсе, в которой будет происходит конфигурация изменений (рабочая область, детализация);

— «Тип ограничений». Выбор типа ограничения, по которому будет происходить конфигурация доступа (просмотр, изменение, просмотр и изменение);

— «Типы состояний». Типы состояний настраивают ограничения для документов по различным видам состояний документов (для черновиков).

16.8. Интерфейс «Редактор бизнес-процессов»

Интерфейс «Редактор бизнес-процессов» предназначен для управления бизнес-процессами документов (т.е. порядком их обработки). В базовой поставке системы уже существуют централизованные настройки (с признаком централизованности) схем бизнес-процессов, как показано на рисунке50.

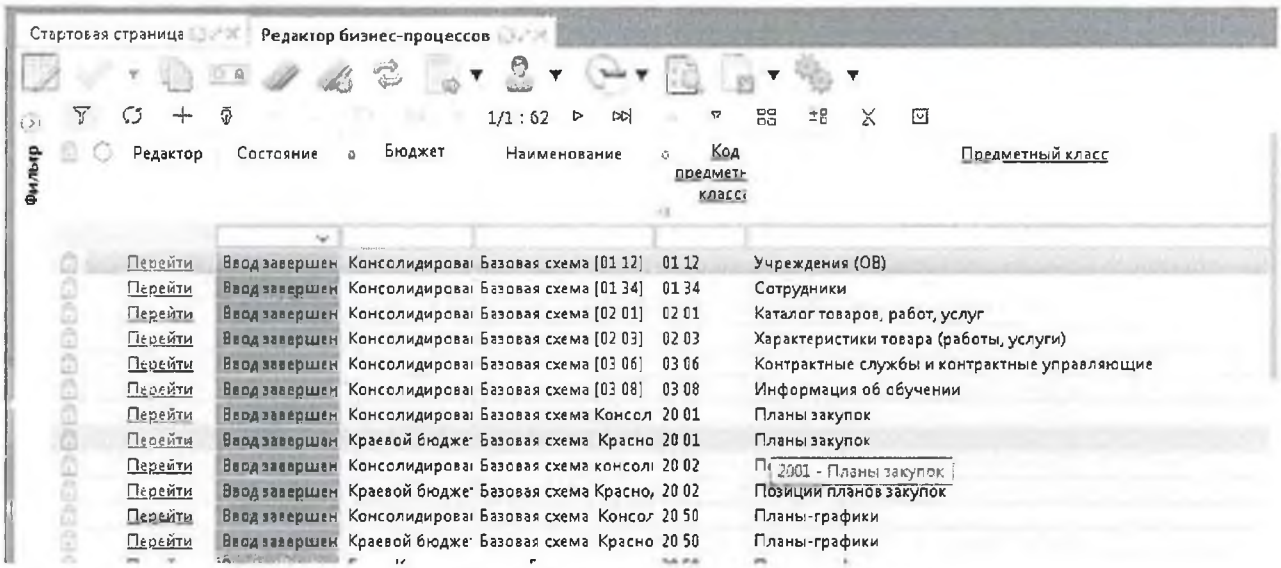


Рисунок 50 – Интерфейс «Редактор бизнес-процессов»

При задании прав на переходы можно использовать как табличный редактор в детализации «Переходы» интерфейса, как показано на рисунке 51, так и графический редактор, открывающийся по кнопке «Перейти» в колонке «Редактор» у записи, как показано на рисунке 52.

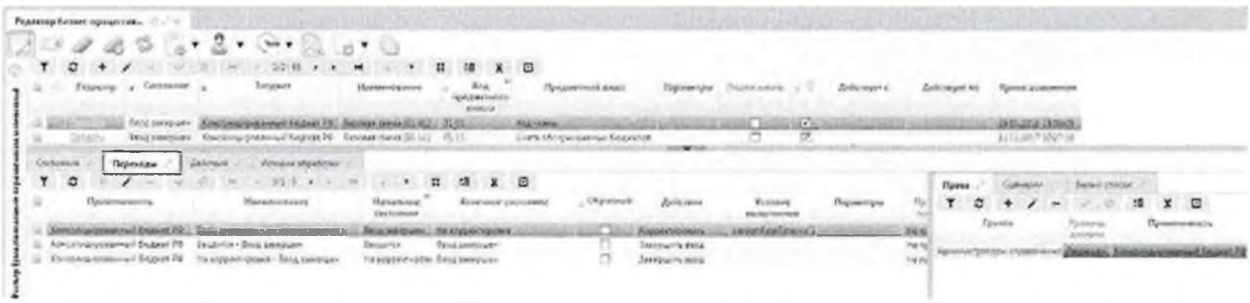


Рисунок 51 – Детализация «Переходы» интерфейса «Редактор бизнес-процессов»

Рисунок 52 – Графический редактор бизнес-процессов

16.8.1. Детализация «Переходы»

Детализация «Переходы» содержит перечень и вариативность переходов документа по схеме бизнес-процесса, представляет собой взаимосвязь начального и конченого состояния. Совокупность состояний, переходов и действий представляют собой маршрут обработки документа. Каждый переход должен быть отмечен, каковым он является в схеме: обратный (т.е. происходит откат документа в предыдущее состояние), или прямой – переход, передвигающий документ вперед по схеме состояний. Задание прав на переходы осуществляется на вкладке «Права», как показано на рисунке 53.

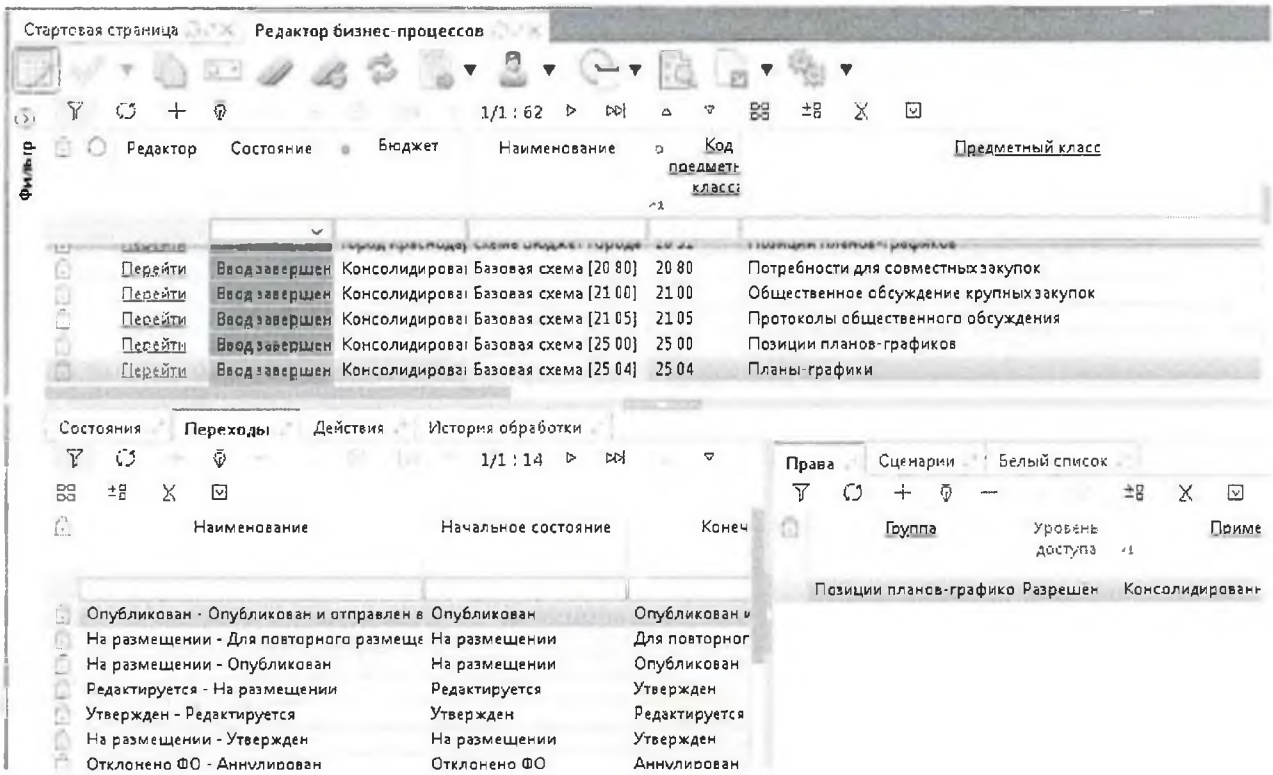


Рисунок 53 – Вкладка «Права» детализации «Переходы»

Вкладка «Права» содержит следующий перечень колонок:

— «Группа». Субъект права – группа пользователей, которой задаются права;
— «Уровень доступа». Данная колонка может изменяться региональным администратором и после обновления системы изменения, внесенные администратором, не будут исправлены. Колонка принимает следующие значения:
  - отсутствует (выбранная группа пользователей не будет учтена подсистемой прав);
  - разрешен (выбранной группе дается право на форму ввода);
  - запрещен (запрещает выбранной группе пользователей доступ);
  - эксклюзивный (перекрывает запрет для группы, имеет приоритет выше, чем у значения «Запрещен»);
— «Применимость». В данной колонке указывается наименование бюджета, на который данные настройки будут распространены;
— «Признак централизованности». Если значение «true», то данная строка является централизованной (одинакова для предметной системы во всех регионах), если «false» – пользовательской (настраивается только для конкретного региона);
— «Время создания». Время создания записи;
— «Автор». Автор созданной записи;
— «Время изменения». Время последнего изменения записи;
— «Автор изменения». Автор последнего изменения записи.

На вкладке «Белый список» настраиваются доступности полей для заполнения (заполняются для переходов). В черновиках все атрибуты по умолчанию разрешены, во всех остальных состояниях все атрибуты по умолчанию запрещены (блокируются автоматически). Редактирование белых списков осуществляется только над документами в состоянии «На доработке». Вкладка «Белый список» содержит следующий перечень полей:

— «Детализация». Выбор области на интерфейсе, в которой будет происходит конфигурация изменений (рабочая область, детализация);
— «Колонка». Выбор колонки сущностей, для которых необходимо настроить доступ;
— «Применимость». В данной колонке указывается наименование бюджета, на который данные настройки будут распространены.

16.8.2. Детализация «Состояния»

В детализации «Состояния» содержится список возможных состояний документа для текущего бизнес-процесса. Для каждого состояния может быть определена схема подписания, активность задачи (т.е. при установлении флага-галки напротив какого-либо состояния, будет возникать задача на дальнейшую обработку для документа, находящегося в указанном состоянии), правила назначения исполнителя и др. В детализации действуют «Черные списки». Их суть заключается в запрете на редактирование полей (заполняются для состояний «Черновик»). Как правило, в начальном состоянии документа запрещено указание даты принятия, причины отклонения, поэтому целесообразнее не перечислять все доступные поля, а указать лишь те, которые запрещены.

В детализации «Состояния» существует возможность конфигурирования задач обработки, которые могут влиять на права. Основные атрибуты, конфигурирующие задачи:

- «Правило назначения исполнителя». Выбирается способ назначений исполнителя;
- «Модераторы задач». Назначается группа пользователей (с включенными в нее ранее пользователями), которая в случае отсутствия исполнителя, может редактировать задачу. Для модератора задач разрешены следующие операции: назначение другого исполнителя задаче, удаление исполнителя по задаче, восстановить исполнителя по задаче, закрепление задачи за собой;
- «Разрешение персонификации». Колонка разрешает всем исполнителям закреплять задачи за собой, даже если они не являются модераторами;
- «Неблокирующая задача». Если задано значение «true» в колонке, исполнитель по задаче перестает учитываться при просчете прав на обработку документа.

Для того чтобы региональный администратор смог их отредактировать, изменяемый документ необходимо перевести в режим редактирования пользовательских значений по кнопке редактирования режимов  на панели инструментов, как показано на рисунке 54.

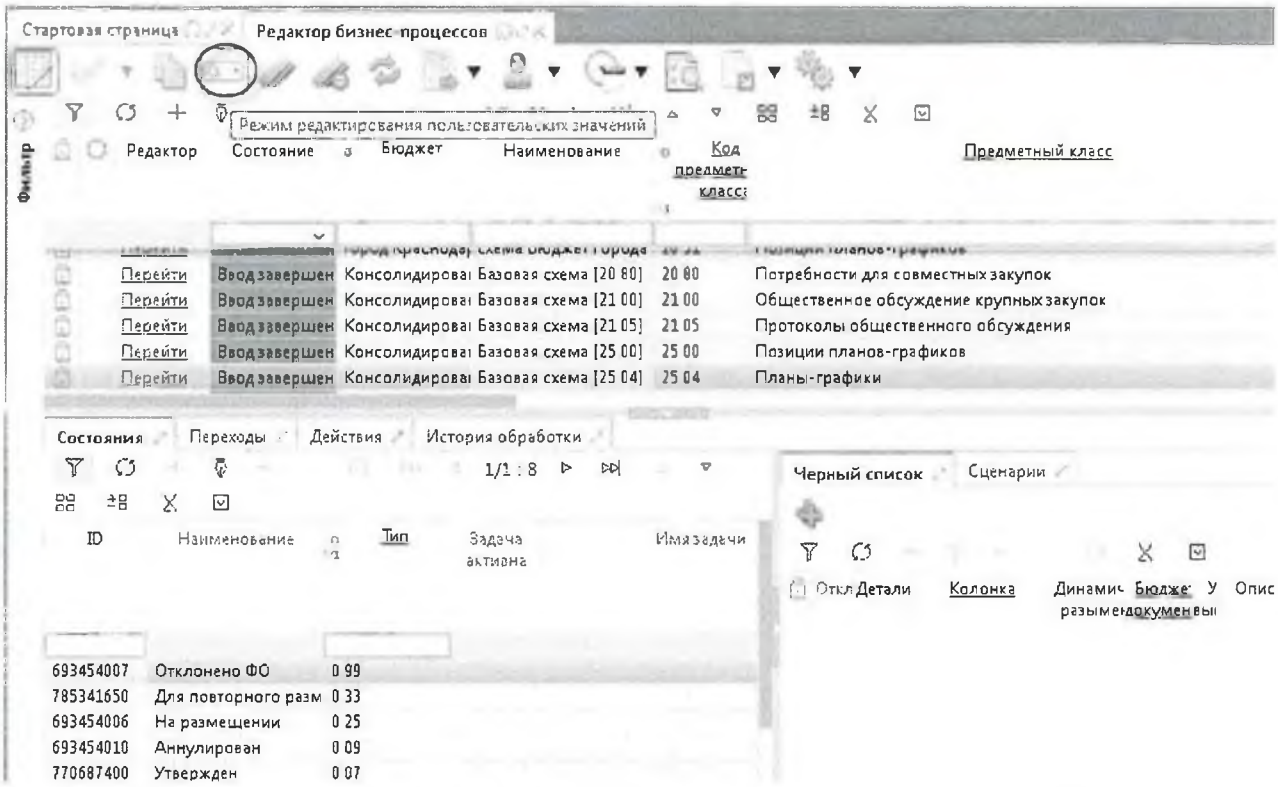


Рисунок 54 – Режим редактирования пользовательских значений

16.9. Интерфейсы «Правила применимости параметров», «Правила применимости параметров источника»

Интерфейс «Правила применимости параметров» служит для настройки правил применимости параметров на панели фильтрации для любого интерфейса системы. В этом справочнике для конкретного предметного класса параметр сопоставляется со свойством ограничения, как показано на рисунке 55.

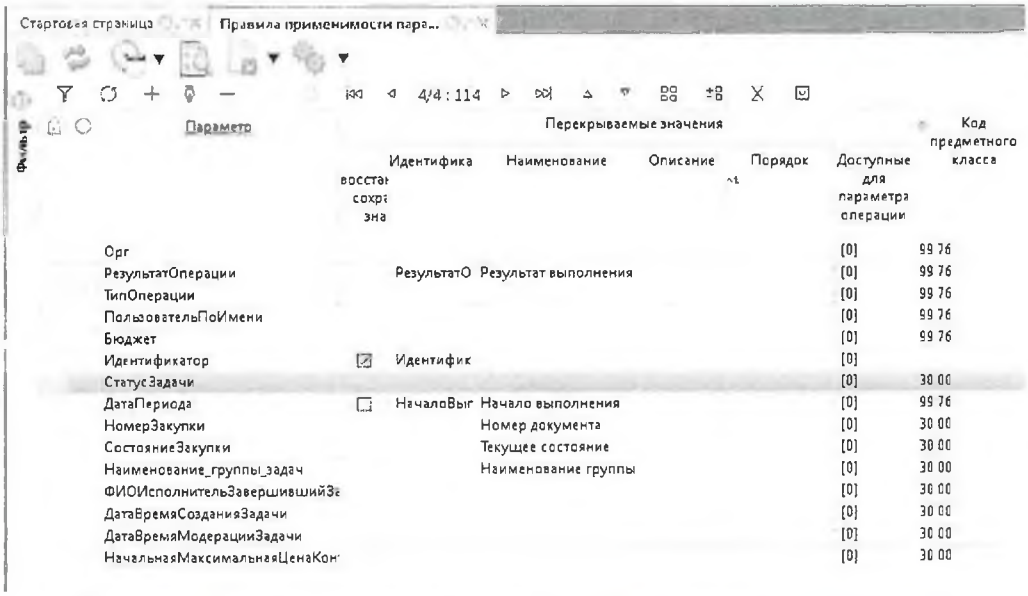


Рисунок 55 – Интерфейс «Правила применимости параметров»

Для настройки правил применимости параметров для отчетов используется интерфейс «Правила применимости параметров источников». Отчет выбирает, из каких источников необходимо брать данные. Для каждого отчета используются те ограничения, которые допустимы их источником данных, как показано на рисунке 56.

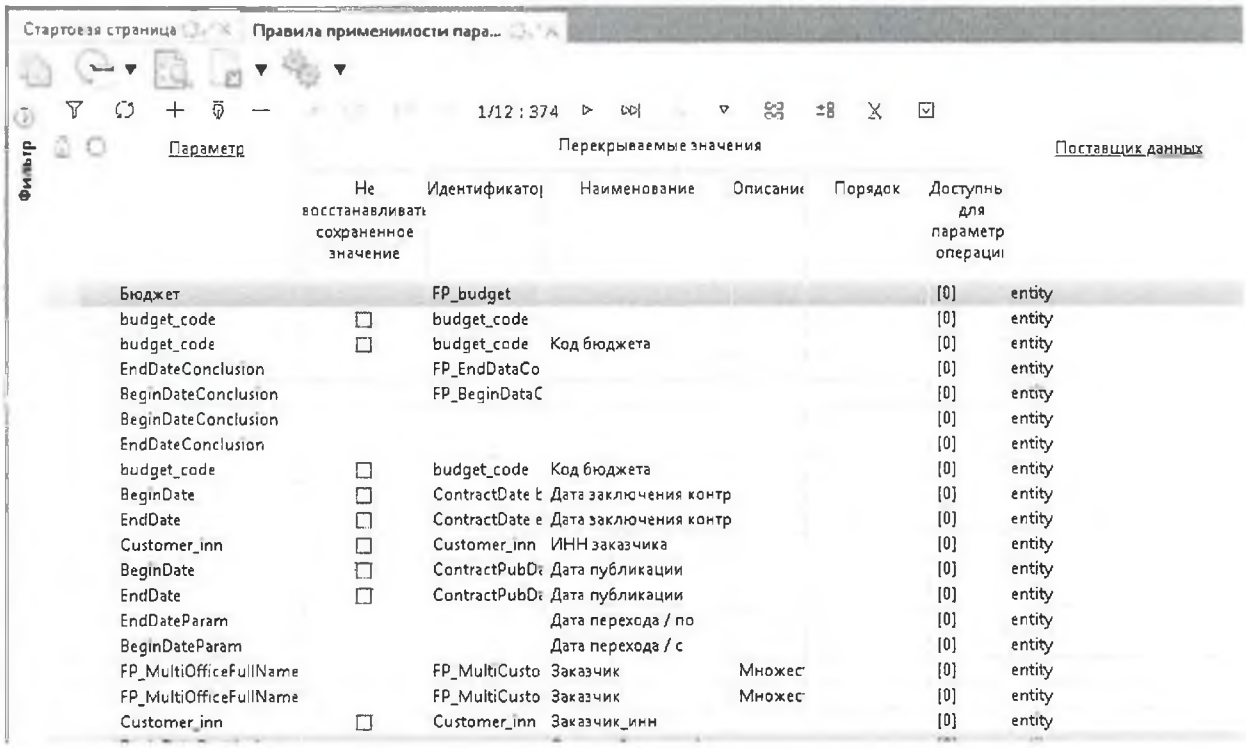


Рисунок 56 – Интерфейс «Правила применимости параметров источников»

16.10.Интерфейс «Справочник внешних систем»

На данном интерфейсе содержится перечень подсистем, с которыми происходит синхронизация системы. В детализации «Перечень доступных справочников» выполняется настройка возможности редактирования справочников пользователями системы, как показано на рисунке 57.

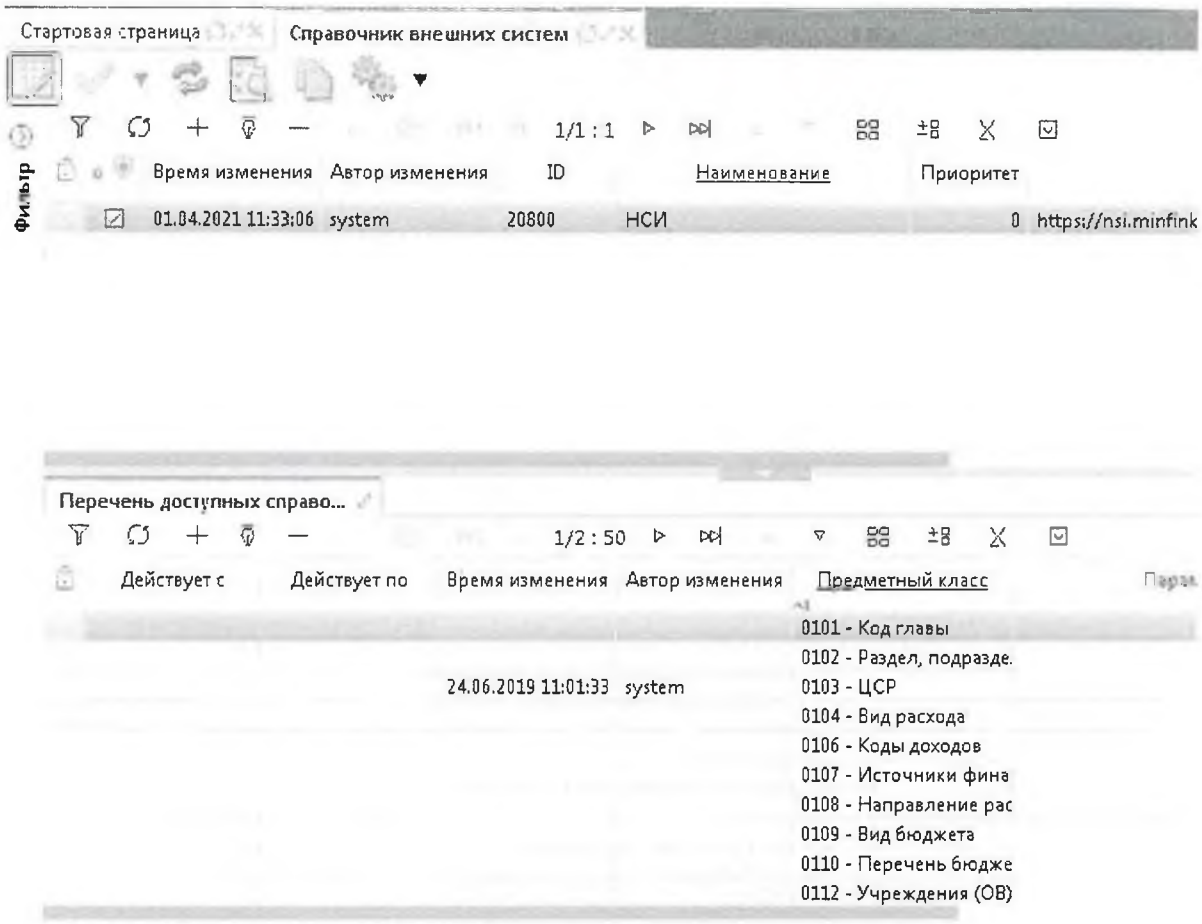


Рисунок 57 – Интерфейс «Справочник внешних систем»

Детализация содержит следующий перечень колонок:

— «Предметный класс». Выбирается конкретный предметный класс из справочника «Предметные классы»;

— «Скрипт получения данных». Редактор, в котором содержится java-скрипт;

— «Запрет ввода». Позволяет настроить запрет на редактирование справочников пользователем.

В детализации «Перечень доступных справочников» колонке «Запрет ввода» существует возможность запретить редактирование определенного справочника в системе для пользователя, если данные справочника загружаются из других систем, например, из ПК «НСИ».

17. Права глобальных администраторов

Права глобальных администраторов: добавление, изменение, удаление, активация и деактивация учетных записей, определение прав работы для сотрудников всех уровней своего бюджета.

У глобального администратора, настроена полная видимость всех организации справочника «Учреждения (ОВ)».

17.1. Активация учетной записи глобального администратора пользователей

После регистрации глобальных администраторов пользователей на указанный в заявке адрес электронной почты направляется письмо с дальнейшими инструкциями по активации учетной записи пользователей, как представлено на рисунке 58.

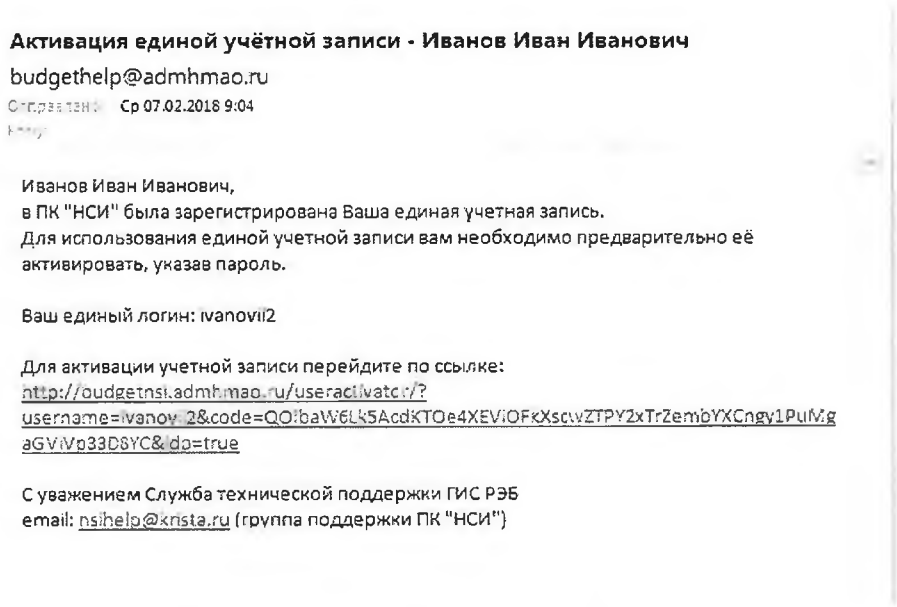


Рисунок 58 - Активационное письмо

После перехода по ссылке из письма для активации появится окно «Активация учетной записи пользователя», в котором необходимо указать два раза пароль для единой учётной записи и нажать кнопку «Активировать», как представлено на рисунке 59.

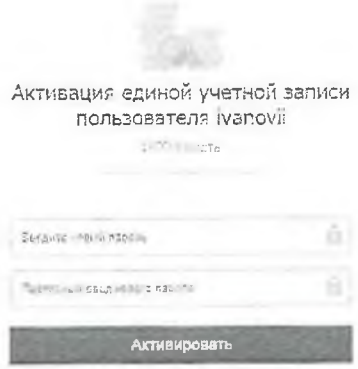


Рисунок 59 - Активация единой учетной записи

Существуют требования к сложности пароля: Пароль должен быть не короче 8 символов, содержать не менее 4-х латинских букв в верхнем и нижнем регистре и, хотя бы 1 цифру. Если эти требования соблюдены, то появится сообщение об успешной активации единой учетной записи, в противном случае будет выдано соответствующее сообщение об ошибке.

После успешной активации будет выдано соответствующее информационное сообщение.

17.2. Администрирование пользователей

Глобальные администраторы пользователей имеют возможность осуществить следующие операции по администрированию всех пользователей в рамках своего бюджета:

— добавления и удаления, активации и деактивации единых учетных записей пользователей;

— назначения функциональных ролей единым учетным записям пользователей.

Администрирование пользователей осуществляется с использование рабочего места «Управление пользователями» доступного в левом вертикальном меню системы, как представлено на рисунке60.

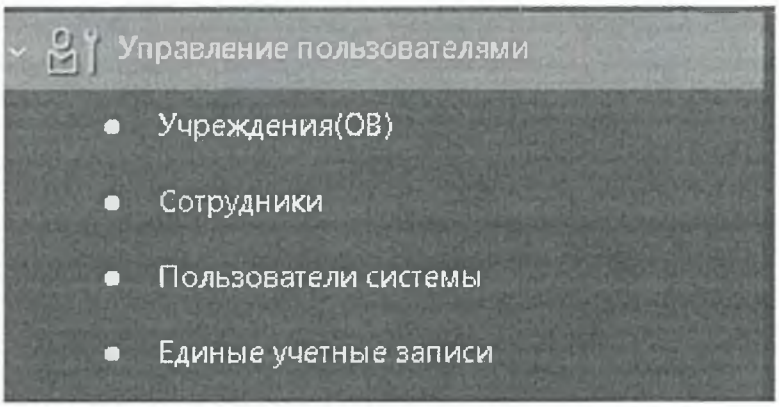


Рисунок 60 – Рабочее место «Управление пользователями»

17.2.1. Состав рабочего места(РМ) «Управление пользователями»

РМ «Управление пользователями» состоит из следующих групп:

— «Учреждения (ОВ)»;

— «Сотрудники»;

— «Пользователи системы»;

— «Единые учетные записи»;

Регистрация пользователей производится в несколько этапов:

1. Добавление нового сотрудника в справочник «Сотрудники» РМ «Управление пользователями» и автоматическая генерация единой учетной записи при утверждении сотрудника на интерфейсе «Единые учетные записи» РМ «Управление пользователями».

2. Назначение прав пользователю через указание функциональных ролей в справочнике «Сотрудники» РМ «Управление пользователями».

3. Отправка ссылки активации на адрес электронной почты, указанный у учетной записи, на интерфейсе «Единые учетные записи» РМ «Управление пользователями».

17.2.2. Добавление нового сотрудника и создание единой учетной записи

Добавление единой учетной записи для нового сотрудника выполняется в справочнике «Сотрудники» РМ «Управление пользователями», как представлено на рисунке 61.

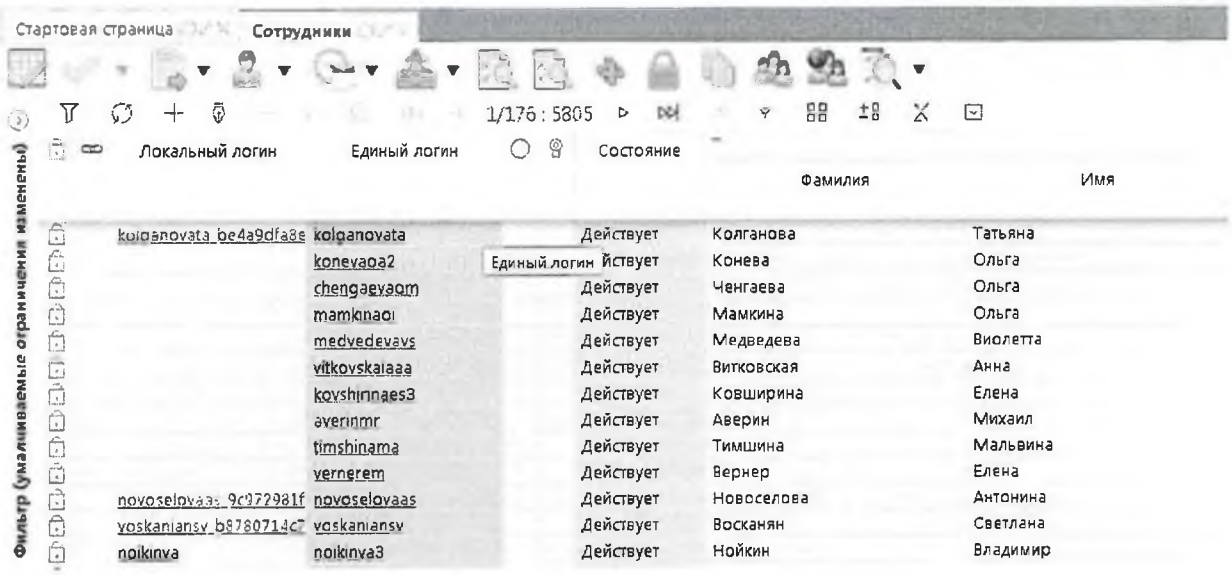


Рисунок 61 – Справочники «Сотрудники»

Для добавления нового сотрудника необходимо нажать на панели команд таблицы кнопку «Добавить запись», как представлено на рисунке 62.

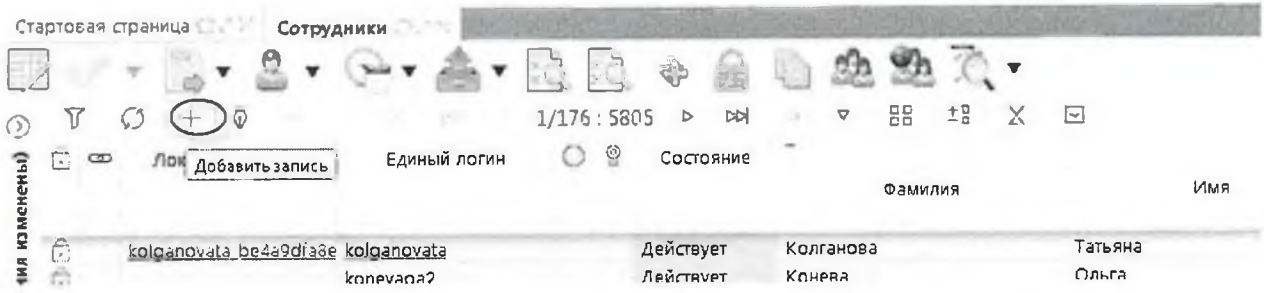


Рисунок 62 – Добавление нового сотрудника в справочник «Сотрудники»

В появившейся пустой строке заполнить все обязательные поля: «Фамилия», «Имя», «Отчество», «Должность», «Организация», «Адрес электронной почты» и нажать на панели команд таблицы кнопку «Принять изменения».

Кроме того, следует заметить, что поле «Организация» автоматически заполняется по пользователю, который вошел в систему.

При создании сотрудника следует выбрать требуемую организацию, для этого необходимо раскрыть модальный справочник с организациями и найти в нем с помощью быстрого фильтра
(например, по ИНН) требуемую организацию, как представлено на рисунке 61.

Если какое-то из обязательных полей будет не заполнено, то при сохранении записи появится сообщение об ошибке, как представлено на рисунке 63.

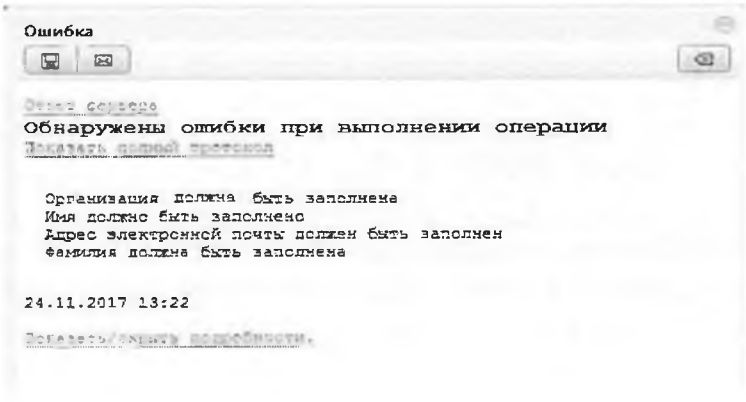


Рисунок 63 – Сообщение об ошибке

Далее созданную запись сотрудника следует утвердить, для этого необходимо выбрать запись и нажать на панели команд кнопку «Действия над документом» - «Утвердить», как представлено на рисунках 64,65.

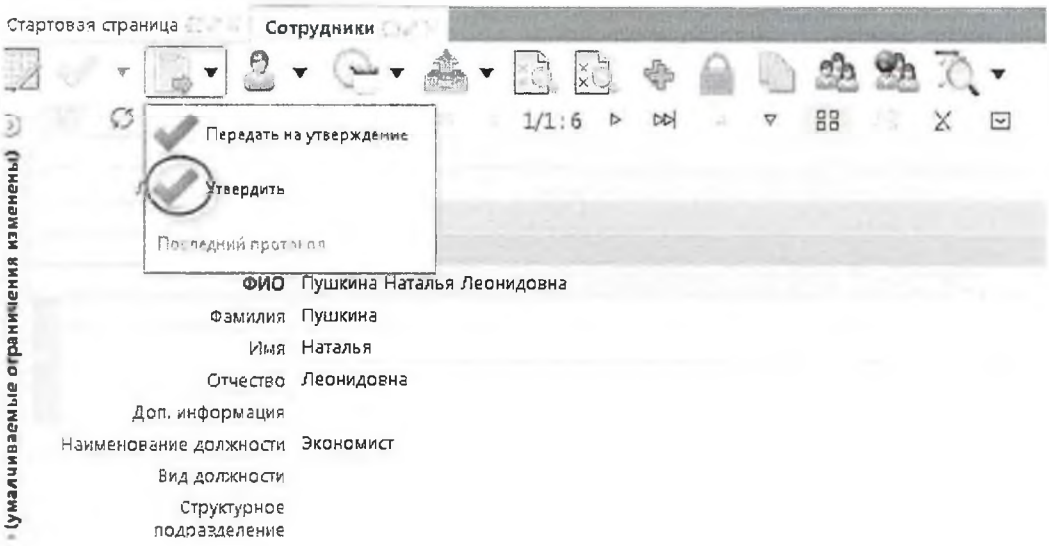


Рисунок 64 – Утверждение сотрудника из формы ввода

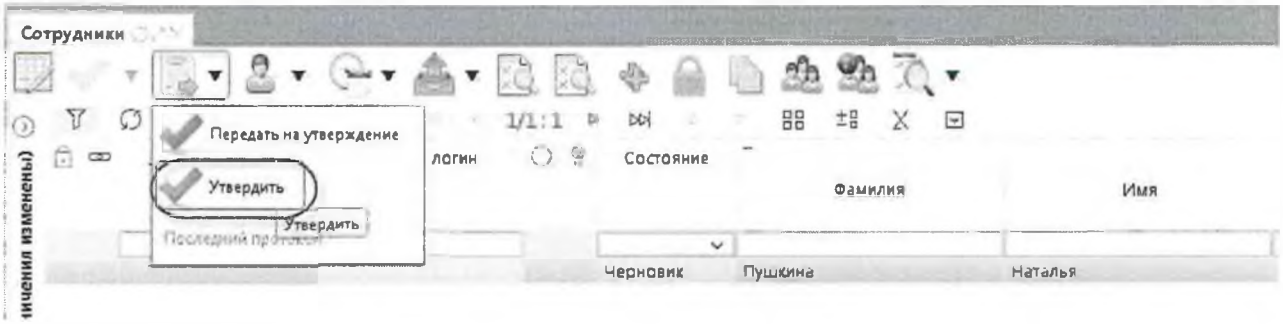


Рисунок 65 – Утверждение сотрудника путем выбора из списка сотрудников

После успешного завершения операции утверждения в колонке «Единый логин» должен отобразиться сформированный логин для сотрудника, а запись изменит свое состояние на «Действует».

Операцию утверждения можно выполнять и над группой сотрудников, для этого необходимо нажать на клавиатуре клавишу «Shift», выделить мышкой несколько сотрудников в состоянии «Черновик» и нажать на панели команд кнопку «Действия над документом» - «Утвердить».

17.2.3. Добавление единой учетной записи для существующего пользователя

В случае если пользователь уже существует в справочнике «Сотрудники» необходимо проверить наличие у него логина единой учетной записи.

Для этого необходимо посмотреть заполнено ли поле «Единый логин». В том случае, если поле пустое, то генерировать единую учетную запись нужно. Если поле «Единый логин» заполнено, это означает, что у данного сотрудника уже существует единая учетная запись.

Для генерации логина единой учетной записи необходимо выбрать запись справочника «Сотрудники» в состоянии «Действует» и сгенерировать единую учетную запись.

Существует 3 способа генерации единых учетных записей:

— способ 1 - генерация логина одиночной единой учетной записи без отправки сообщения активации на электронную почту. Для этого необходимо выделить запись в справочнике «Сотрудники» и на панели команд нажать на кнопку  «Действия над документом» - 

«Добавить единую учетную запись. Далее в открывшемся диалоговом окне «Параметры активации пользователей» нажать кнопку «Применить.

При успешном завершении операции в колонке «Единый логин» появится сгенерированный логин. Если логин единой учетной записи не сгенерировался, то следует обновить справочник, нажав на панели инструментов кнопку  «Обновить данные», проверить наполненность полей и повторить операцию генерацию повторно. Если при повторной операции проблема осталась, необходимо обращаться в Службу поддержки ПК «НСИ»;

— способ 2 - генерация логина одиночной единой учетной записи с возможностью указания функциональных ролей от уже имеющейся единой учетной записи с автоматической отправкой сообщения активации на электронную почту.

Для этого необходимо выделить запись в справочнике «Сотрудники» и на панели команд нажать на кнопку  «Сгенерировать единые логины и отправить активацию по почте».

Далее, если необходимо, назначить функциональные роли от какого-либо сотрудника, то следует щелкнуть в поле «Назначить функциональные роли аналогично сотруднику» диалогового окна «Параметры генерации единых учетных записей» кнопку открытия модального справочника и в открывшемся модальном справочнике «Сотрудники» с помощью кнопки  «Быстрый фильтр» выбрать сотрудника, у которого уже назначены роли, как представлено на рисунке 66.

В том случае, если требуется сгенерировать только логин единой учетной записи и отправить письмо активации на электронную почту (без назначения ролей от другого сотрудника), в диалоговом окне «Параметры генерации единых учетных записей» следует нажать кнопку «Применить».

При успешном завершении операции в колонке «Единый логин» появится сгенерированный логин, в детализации «Функциональные роли» добавятся функциональные роли от выбранного сотрудника, а также будет отправлено письмо с активацией на электронную почту;

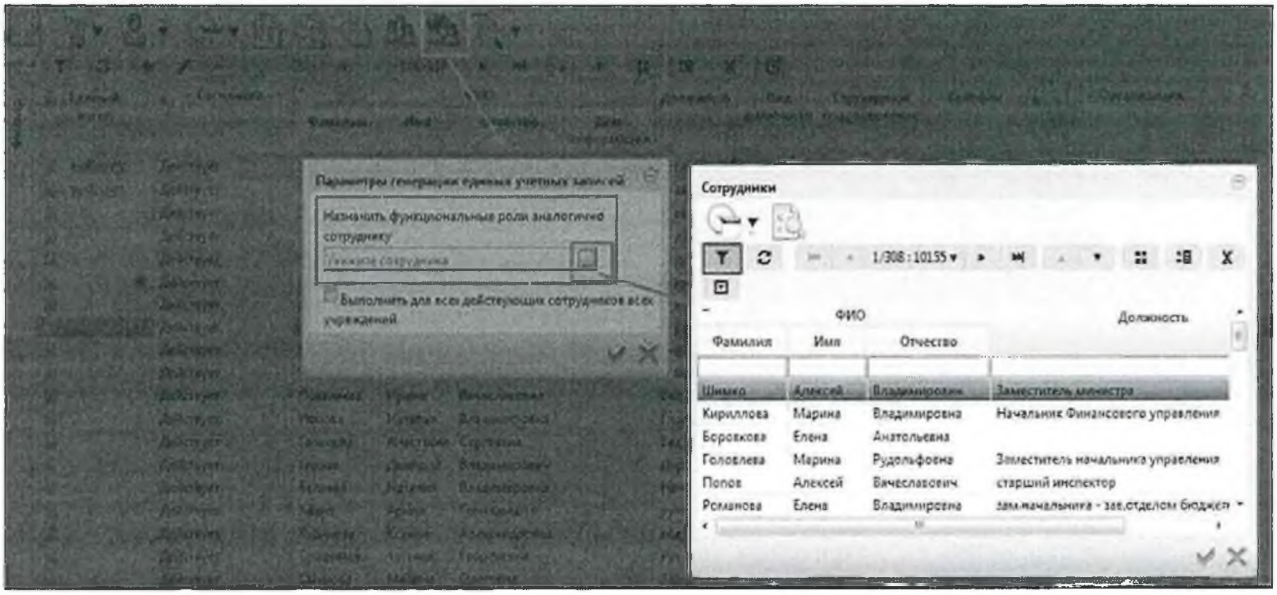


Рисунок 66 – Генерация логина единой учетной записи с отправкой письма активации для действующего сотрудника

— способ 3 - множественная генерация единых учетных записей с возможностью указания функциональных ролей от уже имеющейся единой учетной записи с автоматической отправкой сообщений активации на электронную почту.

Данная операция аналогична предыдущему способу генерации единых учетных записей, но выполняется уже над группой записей справочника «Сотрудники», для этого необходимо нажать на клавиатуре клавишу «Shift» и выделить мышкой несколько записей сотрудников в состоянии «Действует», далее работа пользователя полностью повторяет действия из предыдущего способа генерации единых учетных записей, как представлено на рисунке 67.

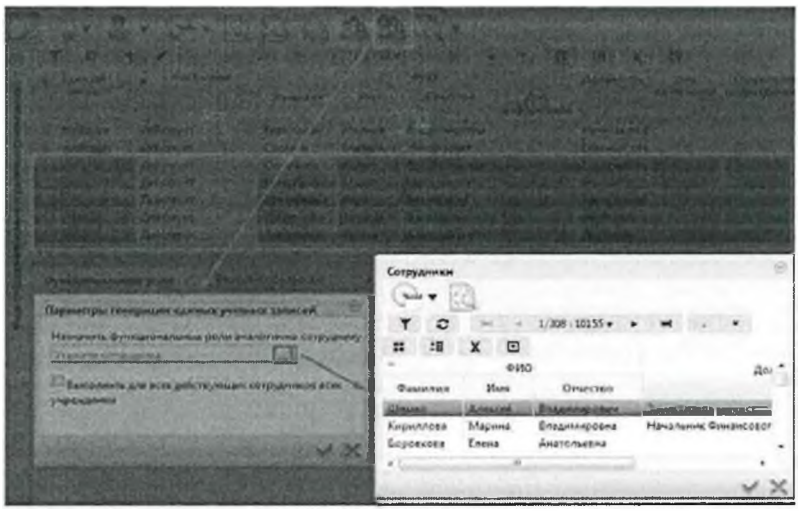


Рисунок 67 – Множественная генерация логинов единой учетной записи с отправкой писем активации для действующих сотрудников

17.2.4. Добавление / удаление функциональных ролей единой учетной записи

Для работы в подсистемах для пользователей должны быть добавлены функциональные роли.

Для добавления функциональных ролей единой учетной записи необходимо перейти в детализацию «Функциональные роли» справочника «Сотрудники» РМ «Управление пользователями». В указанной детализации нажать кнопку  «Добавить функциональные роли» и в открывшемся модальном окне «Функциональные роли» указать для выбранного сотрудника функциональные роли, как представлено на рисунке 68.

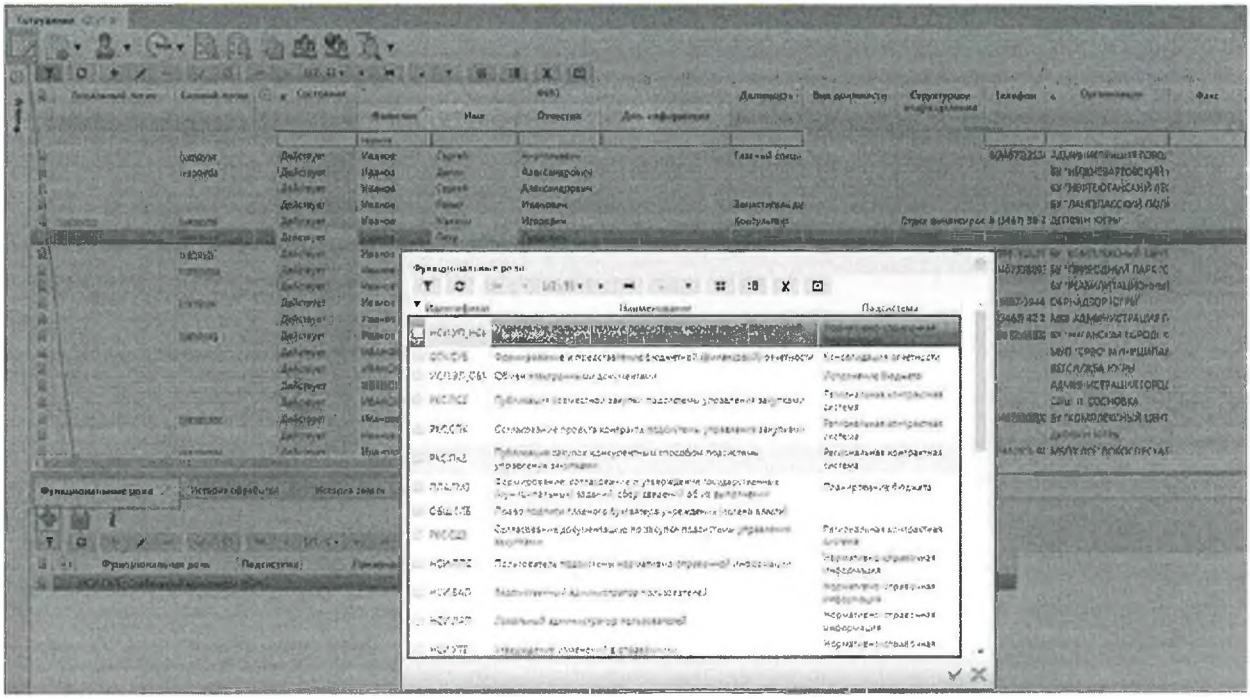


Рисунок 68 – Добавление функциональных ролей единой учетной записи

Для удаления функциональных ролей единой учетной записи необходимо перейти в детализацию «Функциональные роли» справочника «Сотрудники» РМ «Управление пользователями». В указанной детализации выбрать функциональную роль и нажать кнопку «Закрыть функциональные роли», как представлено на рисунке 69.

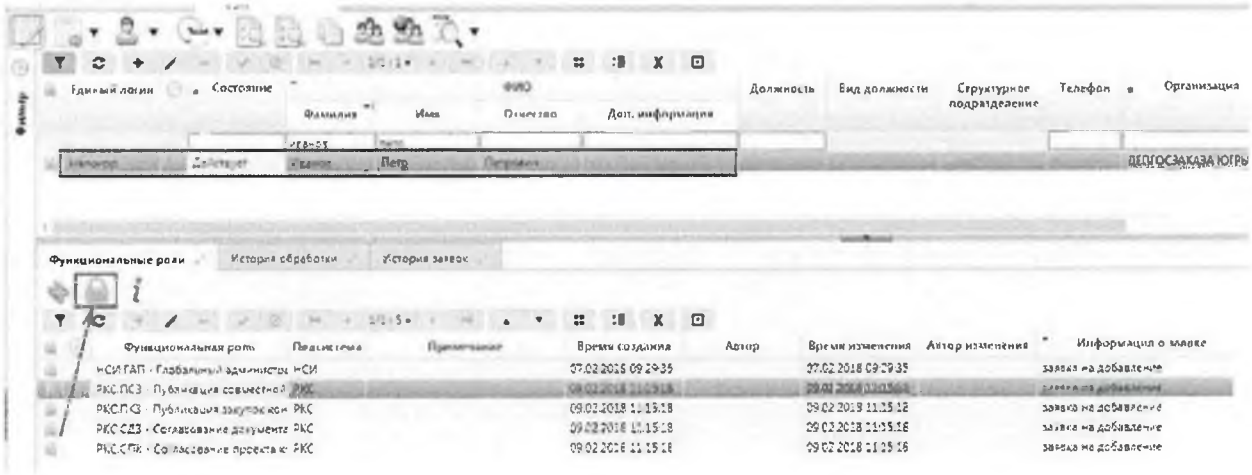


Рисунок 69 – Множественная генерация логинов единой учетной записи с отправкой писем активации для действующих сотрудников

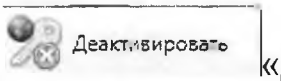
17.2.5. Активация / деактивация / удаление / восстановление единой учетной записи

Для активации единой учетной записи необходимо перейти на интерфейс «Единые учетные записи» РМ «Управление пользователями», найти там с помощью быстрого фильтра сгенерированный логин в состоянии «Вводится» и, если у данной единой учетной записи указан адрес электронной почты, то нажать на панели команд кнопку  «Действия над документом» - 

«Активировать по почте».. Данную операцию можно выполнять и над группой единых учетных записей, нажав на клавиатуре клавишу «Shift» и выделить мышкой несколько единых учетных записей в состоянии «Вводится».

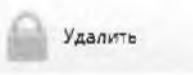
При успешном завершении операции пользователю будет направлено письмо со ссылкой для активации пароля, а единая учетная запись изменит свое состояние на «Отправлено приглашение».

После успешной активации единой учетной записи ее состояние изменится на «Активирован пользователем».

Для деактивации единой учетной записи необходимо перейти на интерфейс «Единые учетные записи» РМ «Управление пользователями», найти там с помощью быстрого фильтра требуемую единую учетную запись, которая должна находиться в состоянии «Активирован администратором» или «Активирован пользователем», и нажать на панели команд кнопку  «Действия над документом» - 

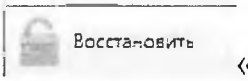
«Деактивировать. Данную операцию можно выполнять и над группой единых учетных записей, нажав на клавиатуре клавишу «Shift» и выделить мышкой несколько активированных единых учетных записей.

При успешном завершении операции пользователю будет направлено письмо, содержащее сообщение о деактивации единой учетной записи, а единая учетная запись изменит свое состояние на «Деактивирован». В данном состоянии для редактирования доступно поле «Адрес электронной почты».

Для удаления единой учетной записи необходимо перейти на интерфейс «Единые учетные записи» РМ «Управление пользователями», найти там с помощью быстрого фильтра требуемую единую учетную запись, которая должна находиться в состоянии «Активирован администратором» или «Активирован пользователем», и нажать на панели команд кнопку  «Действия над документом» - 

«Удалить. Данную операцию можно выполнять и над группой единых учетных записей, нажав на клавиатуре клавишу «Shift» и выделить мышкой несколько активированных единых учетных записей.

При успешном завершении операции пользователю будет направлено письмо, содержащее сообщение о блокировке единой учетной записи, а единая учетная запись изменит свое состояние на «Заблокирован администратором» и будет видна на интерфейсе только при нажатой на панели команд кнопке  «Показать скрытые/закрытые».

Для восстановления единой учетной записи необходимо перейти на интерфейс «Единые учетные записи» РМ «Управление пользователями», найти там среди скрытых записей с помощью быстрого фильтра требуемую единую учетную запись, которая будет находиться в состоянии «Заблокирован администратором», и нажать на панели команд кнопку  «Действия над документом» - 

«Восстановить. Данную операцию можно выполнять и над группой единых учетных записей, нажав на клавиатуре клавишу «Shift» и выделить мышкой несколько активированных единых учетных записей.

При успешном завершении операции пользователю будет направлено письмо, содержащее сообщение о разблокировке единой учетной записи, а единая учетная запись изменит свое состояние на то, которое было перед блокировкой, при этом пароль останется прежним и не потребует замены.

17.2.6. Добавление подразделений организации в справочнике «Учреждения (ОВ)» РМ «Управление пользователями»

Для некоторых организаций требуется добавление структурных подразделений в детализации «Подразделения» справочника «Учреждения (ОВ)».

Для того, чтобы добавить подразделение у организации необходимо открыть справочник «Учреждения (ОВ)» РМ «Управление пользователями».

Далее в данном справочнике выбрать организацию, для которой необходимо добавить подразделение, и перейти в детализацию «Подразделения», как представлено на рисунке 70.

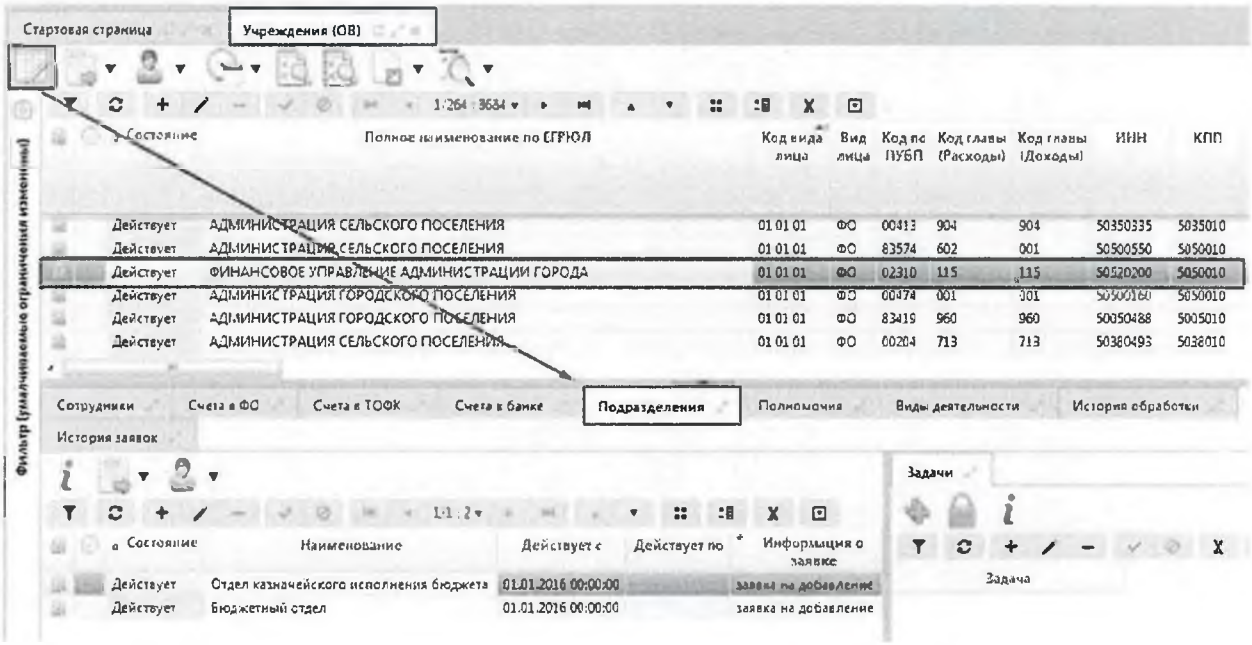


Рисунок 70 – Детализация «Подразделения» в справочнике «Учреждения (ОВ)»

Добавление подразделения выполняется нажатием на кнопку «Добавить запись» на панели команд таблицы. В появившейся пустой строке заполнить поле: «Наименование» и нажать на панели команд таблицы кнопку «Принять изменения», как представлено на рисунке 71.

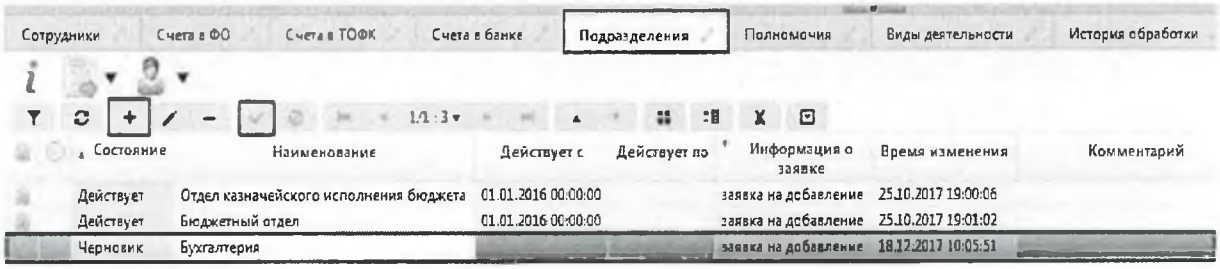


Рисунок 71 – Добавление подразделения в детализацию «Подразделения» справочника «Учреждения (ОВ)»

Далее созданную запись с подразделением следует передать на утверждение и утвердить, для этого необходимо выбрать запись и нажать на панели команд кнопку «Действия над документом» - «Передать на утверждение» и «Действия над документом» - «Утвердить», как представлено на рисунке 72.

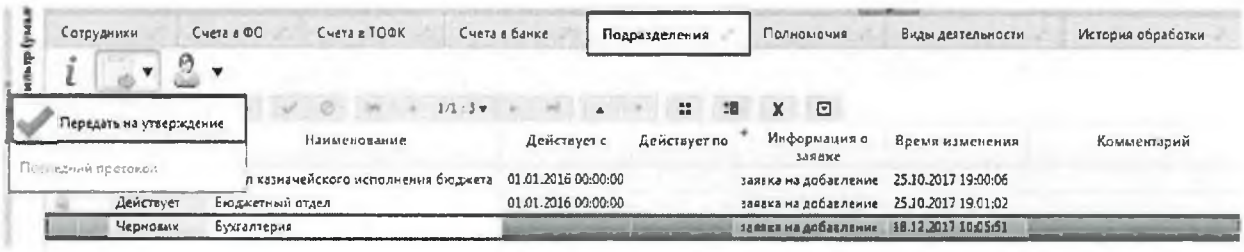


Рисунок 72 –Передача на утверждение подразделения в детализации «Подразделения» справочника «Учреждения (ОВ)»

17.2.7. Изменение информации о сотруднике в справочнике «Сотрудники»

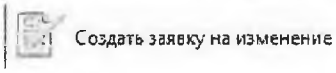
При добавлении единой учетной записи для сотрудника может возникнуть ситуация, что представленные в системе данные могут быть неактуальными.

Существует 2 способа изменения атрибутов сотрудника:

— заявка на изменение;

— заявка на уточнение.

Заявка на изменение применяется в случаях, когда у сотрудника присутствуют пустые поля, по которым требуется заполнение. К таким полям относятся должность, адрес, структурное подразделение, электронной почты.

Для формирования заявки на изменение необходимо выбрать запись сотрудника и на панели команд нажать кнопку  «Действия над документом» - «Создать заявку на изменение» 

Далее у появившейся записи в состоянии «Черновик изменения» следует заполнить недостающие поля, сохранить изменения нажатием на кнопку «Принять изменения» и утвердить, нажав на кнопку «Утвердить», как представлено на рисунке 73.

После успешного завершения операции утверждения запись изменит свое состояние на «Действует».

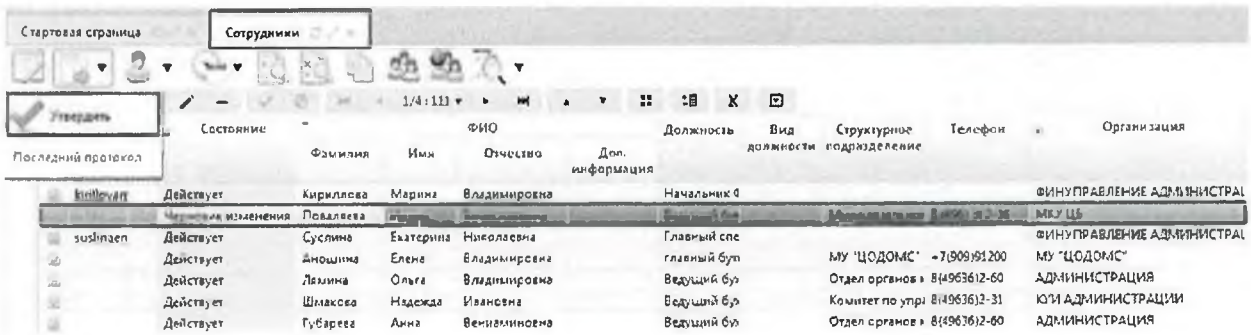
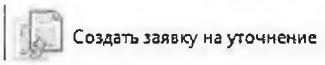


Рисунок 73 – Справочники «Сотрудники» (формирование заявки на изменение)

Заявка на уточнение применяется в случаях, когда у сотрудника атрибуты заполнены, но являются не актуальными, к таким полям относятся фамилия, должность, структурное подразделение, адрес электронной почты.

Для формирования заявки на уточнение необходимо выбрать запись сотрудника и на панели команд нажать кнопку «Действия над документом» - «Создать заявку на уточнение» 

.

Далее у появившейся записи в состоянии «Черновик уточнения» следует изменить значение полей на достоверное, сохранить изменения нажатием на кнопку «Принять изменения» и утвердить, нажав на кнопку «Утвердить», как представлено на рисунке 74.

После успешного завершения операции утверждения запись изменит свое состояние на «Действует».

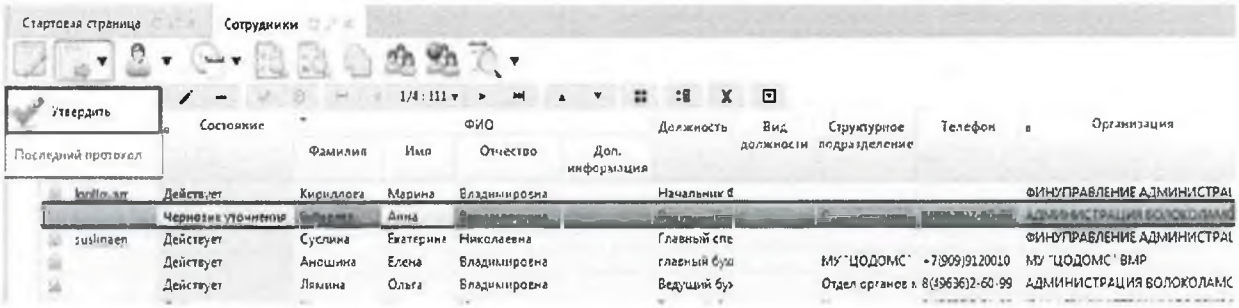


Рисунок 74 – Справочники «Сотрудники» (формирование заявки на уточнение)

17.2.8. Закрытие записи о сотруднике в справочнике «Сотрудники»

Бывают случаи, когда требуется закрытие записи о сотруднике в справочнике «Сотрудники» (например, при увольнении сотрудника из указанной организации).

Последовательность действий по закрытию записи о сотруднике в справочнике «Сотрудники»:

— найти запись о сотруднике в справочнике «Сотрудники» с помощью быстрого фильтра;

— при наличии единой учетной записи у такого сотрудника необходимо деактивировать ее на интерфейсе «Единые учетные записи»;

— вернуться в справочник «Сотрудники», выделить запись о сотруднике и на панели команд справочника нажать кнопку «Закрыть», как представлено на рисунке 75;

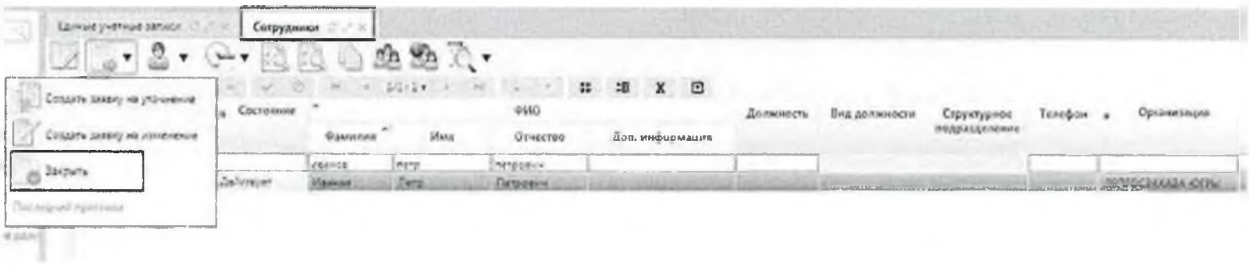


Рисунок 75 – Закрытие записи о сотруднике в справочнике «Сотрудники»

— в диалоговом окне «Дата закрытия» указать дату прекращения действия для записи о сотруднике и нажать кнопку «Применить».

При успешном завершении операции запись о сотруднике исчезнет с интерфейса «Сотрудники» и будет видна только при нажатой на панели команд кнопке  «Показать скрытые/закрытые».

18. Права ведомственных администраторов

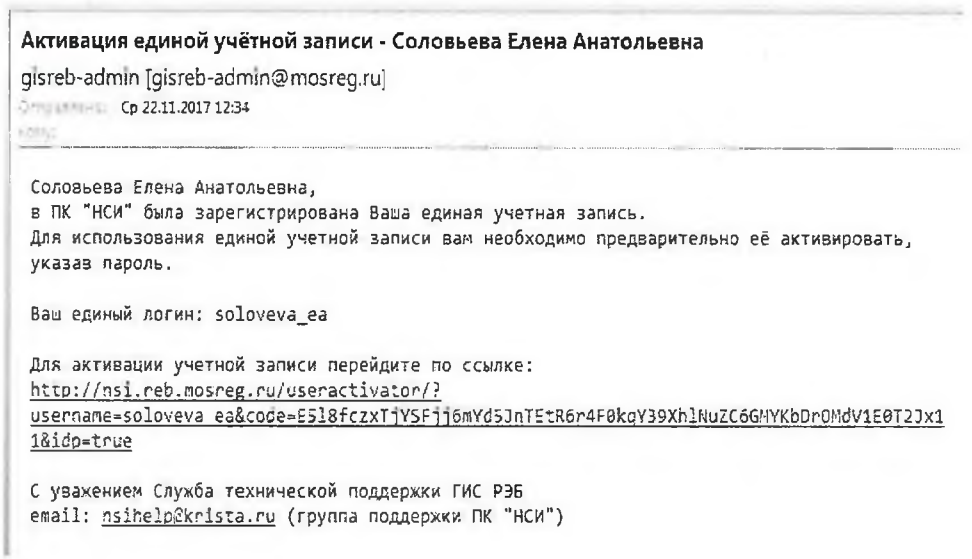
Права ведомственного администратора: добавление, изменение, удаление, активация и деактивация учетных записей, определение прав работы в смежных подсистемах для сотрудников своего ЦИОГВ и сотрудников подведомственных учреждений своего ЦИОГВ.

Права ведомственного администратора – сотрудника финансового органа муниципального образования: добавление, изменение, удаление, активация и деактивация учетных записей, определение прав работы в смежных подсистемах для сотрудников своего финансового органа, ОМСУ своего муниципального образования, муниципальных учреждений своего муниципального образования, ОМСУ поселений.

Регистрация ведомственного администратора пользователей осуществляется финансовым органом, на основании заявки ЦИОГВ, ОМСУ субъекта направленной в установленном порядке.

18.1. Активация учетной записи ведомственного администратора пользователей

После регистрации ведомственного администратора пользователей на указанный в заявке адрес электронной почты направляется письмо с дальнейшими инструкциями по активации учетной записи ведомственного администратора пользователей, как представлено на рисунке 76.



Активация единой учётной записи - Соловьева Елена Анатольевна

gisreb-admin [gisreb-admin@mosreg.ru]

Ср 22.11.2017 12:34

Соловьева Елена Анатольевна,
в ПК "НСИ" была зарегистрирована Ваша единая учетная запись.
Для использования единой учетной записи вам необходимо предварительно её активировать,
указав пароль.

Ваш единый логин: soloveva_ea

Для активации учетной записи перейдите по ссылке:
http://nsi.reb.mosreg.ru/useractivator/?
username=soloveva_ea&code=E5l8fczxTjYSFjj6mYd5JnTEtR6r4F0kqY39XhlNuZC6GMYKbDrOMdV1E0T2Jx1
1&idp=true

С уважением Служба технической поддержки ГИС РЭБ
email: nsihelp@krista.ru (группа поддержки ПК "НСИ")

Рисунок 76 - Активационное письмо

После перехода по ссылке из письма для активации появится окно «Активация учетной записи пользователя», в котором необходимо указать два раза пароль для единой учетной записи и нажать кнопку «Активировать», как представлено на рисунке 77.

Рисунок 77 - Активация единой учетной записи

Существуют требования к сложности пароля: Пароль должен быть не короче 8 символов, содержать не менее 4х латинских букв в верхнем и нижнем регистре и, хотя бы 1 цифру. Если эти требования соблюдены, то появится сообщение об успешной активации единой учетной записи, в противном случае будет выдано соответствующее сообщение об ошибке.

После успешной активации будет выдано соответствующее информационное сообщение.

18.2. Администрирование пользователей

Ведомственные администраторы имеют возможность осуществить следующие операции по администрированию пользователей органа власти, учреждений подведомственной сети (финансового органа, организаций и учреждений муниципального образования):

— добавления и удаления, активации и деактивации единых учетных записей пользователей;
— назначения функциональных ролей единым учетным записям пользователей.

Администрирование пользователей осуществляется с использованием рабочего места «Управление пользователями», доступного в левом вертикальном меню системы, как представлено на рисунке 78.

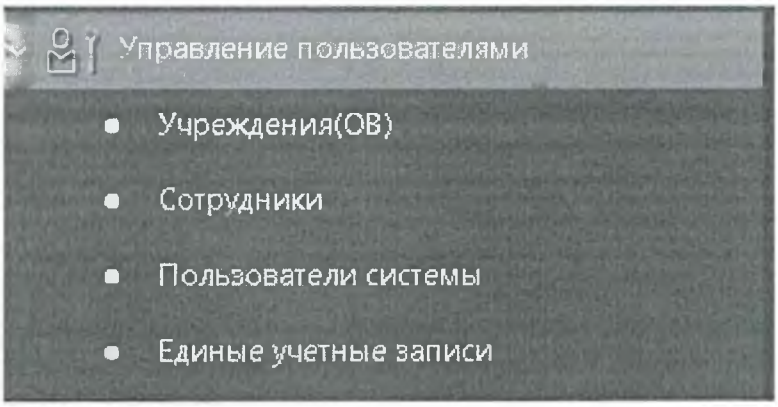


Рисунок 78 – Рабочее место «Управление пользователями»

18.2.1. Состав рабочего места (РМ) «Управление пользователями»

РМ «Управление пользователями» состоит из следующих групп:

— «Учреждения (ОВ)»;
— «Сотрудники»;
— «Пользователи системы»;
— «Единые учетные записи»;

Регистрация пользователей производится в несколько этапов:

— добавление нового сотрудника в справочник «Сотрудники» РМ «Управление пользователями» и автоматическая генерация единой учетной записи при утверждении сотрудника на интерфейсе «Единые учетные записи» РМ «Управление пользователями»;

— назначение прав пользователю через указание функциональных ролей в справочнике «Сотрудники» РМ «Управление пользователями»;
— отправка ссылки активации на адрес электронной почты, указанный у учетной записи, на интерфейсе «Единые учетные записи» РМ «Управление пользователями».

19. Права локальных администраторов

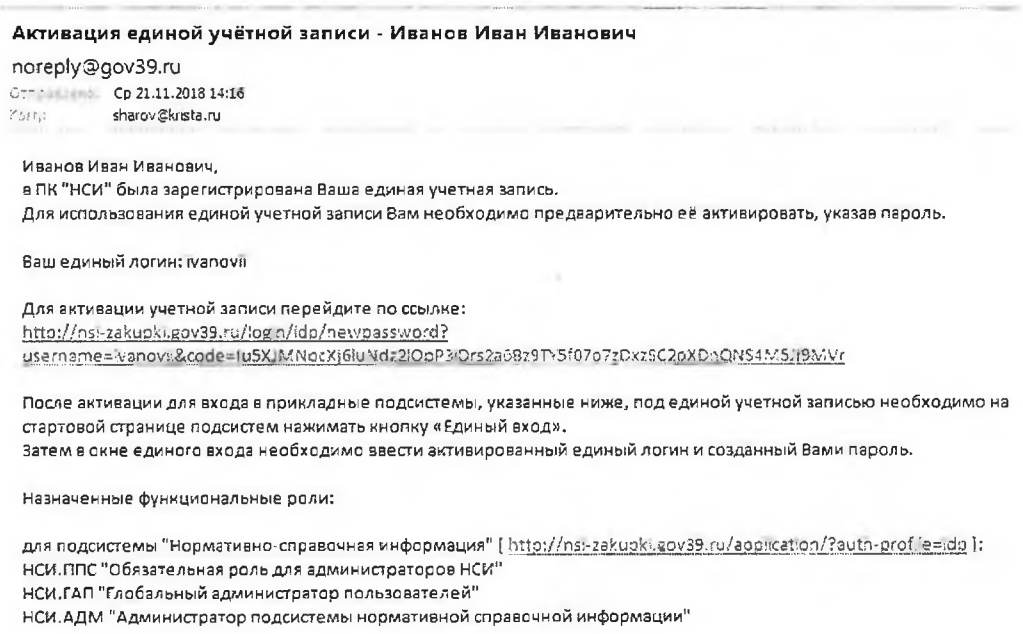
По данным сводного реестра участников и неучастников бюджетного процесса, опубликованного на едином портале бюджетной системы (budget.gov.ru), автоматически формируются учетные записи о руководителях организаций, относящихся к бюджету Тульской области. На адрес электронной почты организации, указанный в сводном реестре, отправляется письмо, содержащее ссылку активации учетной записи руководителя. После активации руководитель автоматически получает права локального администратора пользователей в рамках своей организации и должен зарегистрировать в системе своих сотрудников.

Права локальных администраторов: добавление, изменение, удаление, активация и деактивация учетных записей, определение прав работы в системе только для сотрудников своей организации.

В данной инструкции описывается, как активировать учетную запись руководителя, как зарегистрировать учетные записи для сотрудников организации и назначить им права.

19.1. Активация учетной записи локального администратора пользователей

После регистрации локальных администраторов пользователей на адрес электронной почты организации направляется письмо с дальнейшими инструкциями по активации учетной записи пользователей, как представлено на рисунке 79.



Активация единой учётной записи - Иванов Иван Иванович

noreply@gov39.ru

Ср 21.11.2018 14:16

sharov@krista.ru

Иванов Иван Иванович,
в ПК "НСИ" была зарегистрирована Ваша единая учетная запись.
Для использования единой учетной записи Вам необходимо предварительно её активировать, указав пароль.

Ваш единый логин: ivanovii

Для активации учетной записи перейдите по ссылке:
http://nsi-zakupki.gov39.ru/login/idp/newpassword?
username=ivanovii&code=Iu5XJMNocXj6IuNdz2lOpP3iOrs2a6Bz9T+5f07o7zDxz9C2pXDaQNS4M5/i9MVr

После активации для входа в прикладные подсистемы, указанные ниже, под единой учетной записью необходимо на стартовой странице подсистем нажимать кнопку «Единый вход».
Затем в окне единого входа необходимо ввести активированный единый логин и созданный Вами пароль.

Назначенные функциональные роли:

для подсистемы "Нормативно-справочная информация" [http://nsi-zakupki.gov39.ru/application/?auth-profile=idp]:
НСИ.ППС "Обязательная роль для администраторов НСИ"
НСИ.ГАП "Глобальный администратор пользователей"
НСИ.АДМ "Администратор подсистемы нормативной справочной информации"

Рисунок 79- Активационное письмо

После перехода по ссылке из письма для активации появится окно «Активация учетной записи пользователя», в котором необходимо указать два раза пароль для единой учетной записи и нажать кнопку «Активировать», как представлено на рисунке 80.

Рисунок 80 - Активация единой учетной записи

Существуют требования к сложности пароля: Пароль должен быть не короче 8 символов, содержать не менее 4-х латинских букв в верхнем и нижнем регистре и хотя бы 1 цифру. Если эти требования соблюдены, то появится сообщение об успешной активации единой учетной записи, в противном случае будет выдано соответствующее сообщение об ошибке.

Существуют требования к заданию пароля учетной записи пользователя, которые связаны с усилением мер безопасности работы в системе. Список требований, предъявляемых к паролю
пользователя:

— пароль не должен включать в себя последовательность, указанную в словаре. Словарь представляет собой список запрещенных последовательностей символов. При этом регистр (верхний/нижний) последовательности не учитывается;

— пароль не должен содержать 3 и более одинаковых символов подряд;

— новый пароль пользователя должен быть отличным от предыдущего;

— пароль не должен включать в себя логин.

После успешной активации будет выдано соответствующее информационное сообщение.

19.2. Администрирование пользователей

Локальные администраторы пользователей имеют возможность осуществить следующие операции по администрированию пользователей своей организации:

— добавления и удаления, активации и деактивации учетных записей пользователей;

— назначения функциональных ролей учетным записям пользователей.

Администрирование пользователей осуществляется с использование рабочего места «Управление пользователями» доступного в левом вертикальном меню системы, как представлено на рисунке 81.

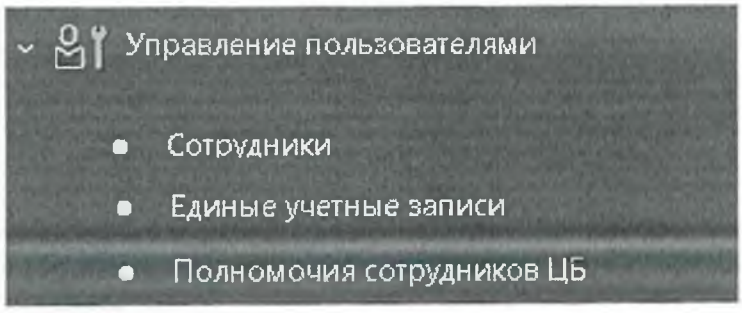


Рисунок 81 – Рабочее место «Управление пользователями»

19.2.1. Состав РМ «Управление пользователями»

РМ «Управление пользователями» состоит из следующих групп:

— «Сотрудники»;

— «Единые учетные записи»;

— «Полномочия сотрудников ЦБ».

Регистрация пользователей производится в несколько шагов:

— добавление нового сотрудника в справочник «Сотрудники» РМ «Управление пользователями» и автоматическая генерация единой учетной записи при утверждении сотрудника на интерфейсе «Единые учетные записи» РМ «Управление пользователями»;

— назначение прав пользователю через указание функциональных ролей в справочнике «Сотрудники» РМ «Управление пользователями»;

— отправка ссылки активации на адрес электронной почты, указанный у учетной записи, на интерфейсе «Единые учетные записи» РМ «Управление пользователями».

20. Базовые формы ввода

Управление формами ввода относится в первую очередь к формам ввода, основанным на гридах.

Все формы ввода можно разделить на базовые и настраиваемые формы ввода. Базовые формы ввода, это те формы ввода, которые создаются разработчиками. Базовые формы ввода заложены в системе, администратор может их только донастраивать.

20.1. Настройки форм

20.1.1. Общие сведения

Механизм настройки форм используется для всех форм. В пунктах 20.1.2 – 20.1.8 описаны возможные настройки форм ввода. Чтобы перейти к настройкам формы ввода необходимо в заголовочной части интерфейса выбрать нужную форму нужного бюджета (или добавить при ее отсутствии в списке) и перейти в детализацию, как показано на рисунке 82.

Рисунок 82 – Интерфейс «Настройки форм»

20.1.2. Настройка панели параметров

На детализации «Настройка панели параметров» администратор настраивает наполнение панели ограничений, то есть может добавить или скрыть какие-то ограничения, которые не нужны для данного региона или МО.

Для того чтобы изменить элемент панели параметров администратору необходимо выбрать параметр панели ограничения, который необходимо изменить и настроить его видимость, как показано на рисунке 83. Если нужно показывать параметр - выбрать «показывать», если нужно скрыть - выбрать «скрывать» или «удалить». Дополнительно можно перекрыть фильтр справочника. Можно также поменять наименование ограничения в поле «Отображаемое наименование», изменив его на более понятное пользователю.

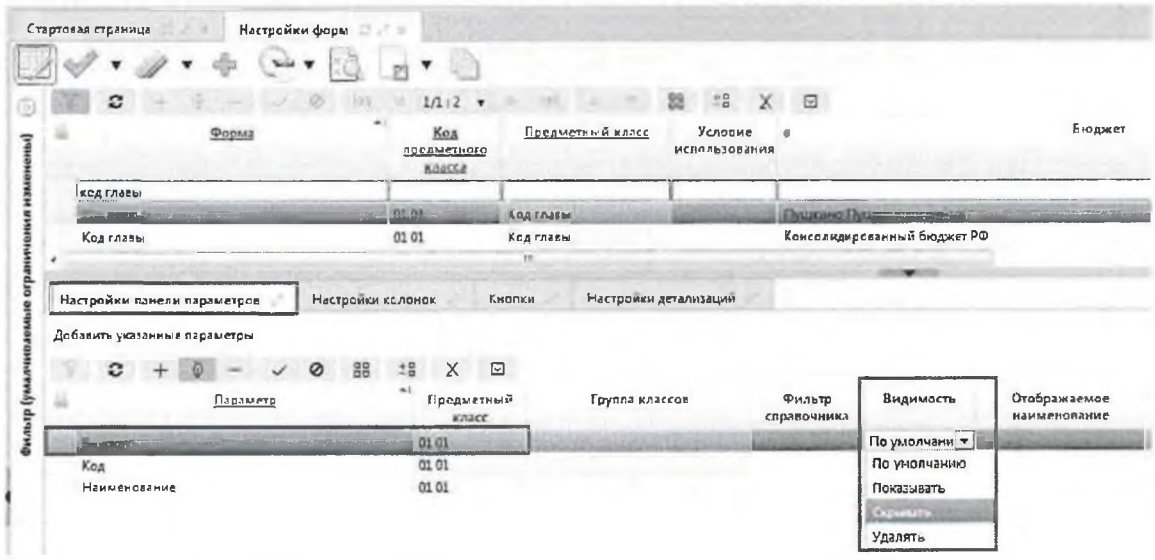


Рисунок 83 – Детализация «Настройки панели параметров» интерфейса «Настройки форм»

20.1.3. Настройка колонок

Пользователь может настраивать видимость колонок с помощью стандартных кнопок управления видимости на интерфейсе формы. Но это же можно сделать и на уровне администратора для всех пользователей выбранного бюджета или вообще всех бюджетов. Например, если какая-то дополнительная классификация не заполняется в регионе, то ее удобней скрыть один раз централизовано, чтобы каждый пользователь не скрывал ее у себя, либо убрать ее централизованно для конкретного бюджета.

Чтобы изменить колонку справочника администратору необходимо перейти на закладку детализации «Настройки колонок», выбрать из справочника нужную колонку, поведение которой необходимо изменить, как показано на рисунке 84.

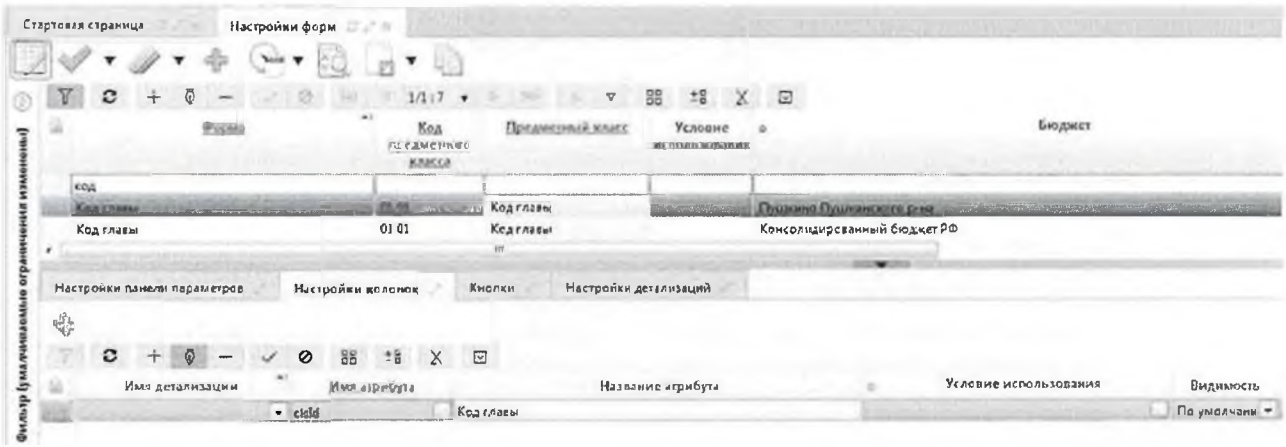


Рисунок 84 – Детализация «Настройки колонок» интерфейса «Настройки форм»

Настройка колонок возможна по следующим параметрам:

— перекрытие отображаемого наименования в поле «Название атрибута», то есть для пользователя будет отображаться перекрытое наименование колонки;

— изменение видимости колонки: в поле «Видимость» установить значение «скрывать»/ «показывать». При этом если колонку пометить скрытой, то колонка будет на интерфейсе, но без возможности открытия;

— удаление колонки: в поле «Видимость» установить значение «Удалять». При этом колонки не будет на форме ввода;

— дополнительно можно указать условие использования. Если нужно скрывать колонки не всегда, а только по условию, то это условие можно указать дополнительно. Например, нужно до конца года использовать колонку «Мероприятия», а со следующего года не нужно. В этом случае можно прописать условие использования: если год 2022, то колонку показывать, если год больше 2022, то колонку скрывать.

20.1.4. Настройка кастомных кнопок

Настройка панели кнопок (toolbar) осуществляется на закладке детализации «Кнопки», как показано на рисунке 85. Есть возможность добавления новых кнопок. Это так называемый механизм кастомных кнопок.

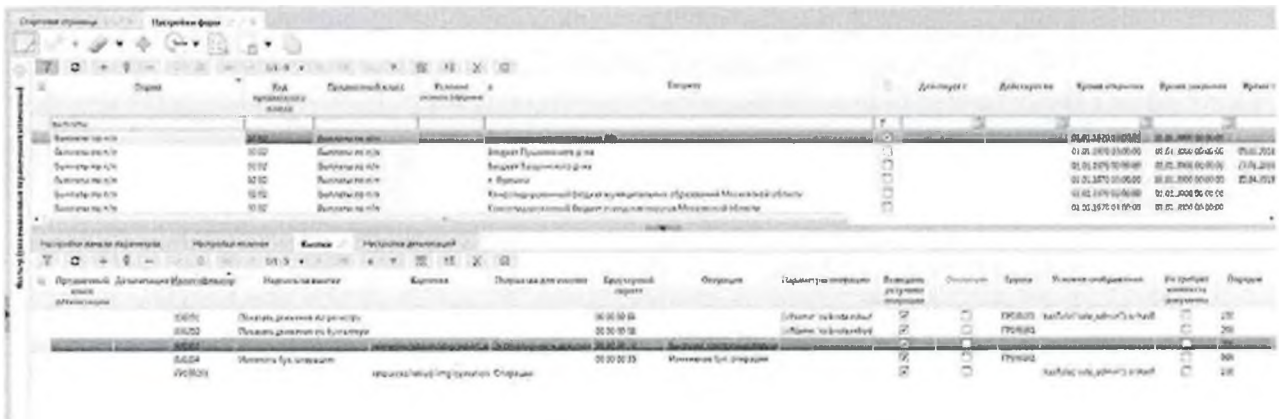


Рисунок 85 – Детализация «Кнопки» интерфейса «Настройки форм»

20.1.4.1. Детализация

Кнопки можно добавлять не только на заголовочную панель кнопок, но и на панель кнопок детализации. Для этого необходимо выбрать нужное значение в поле «Детализация», как показано на рисунке 86.

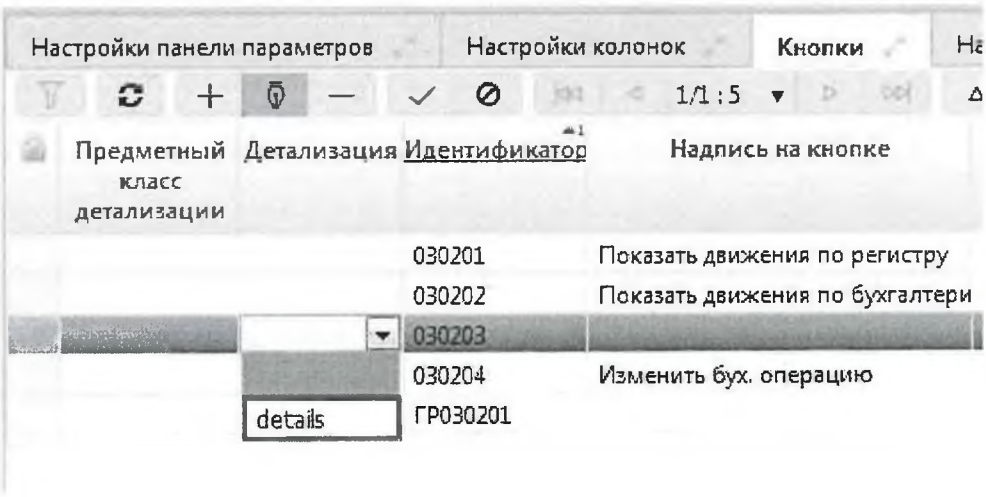


Рисунок 86 – Выбор значения поля «Детализация»

20.1.4.2. Идентификатор

Поле «Идентификатор» заполняется значением идентификатора кнопки. Примеры идентификаторов на рисунке 87.

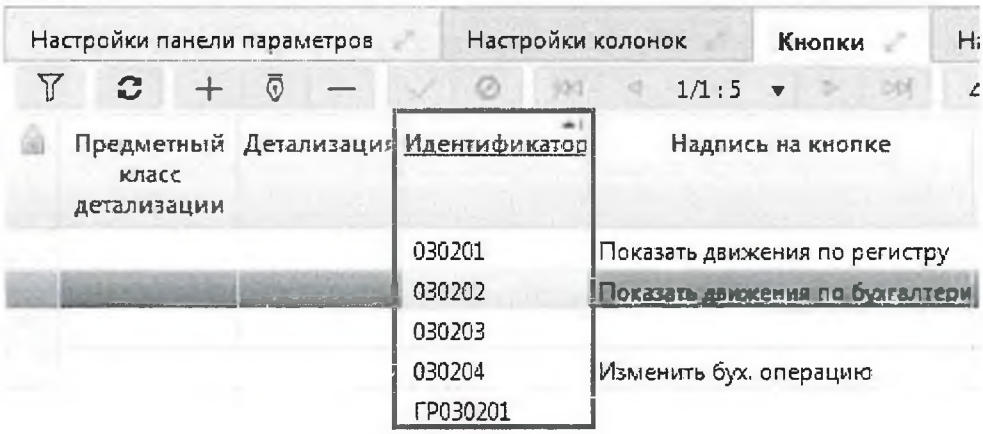


Рисунок 87 – Заполнения поля «Идентификатор»

20.1.4.3. Надпись на кнопке

Поле «Надпись на кнопке» заполняется значением, которое будет видеть пользователь на кнопке. Пример отображения надписи на кнопке для пользователя представлен на рисунке 88.

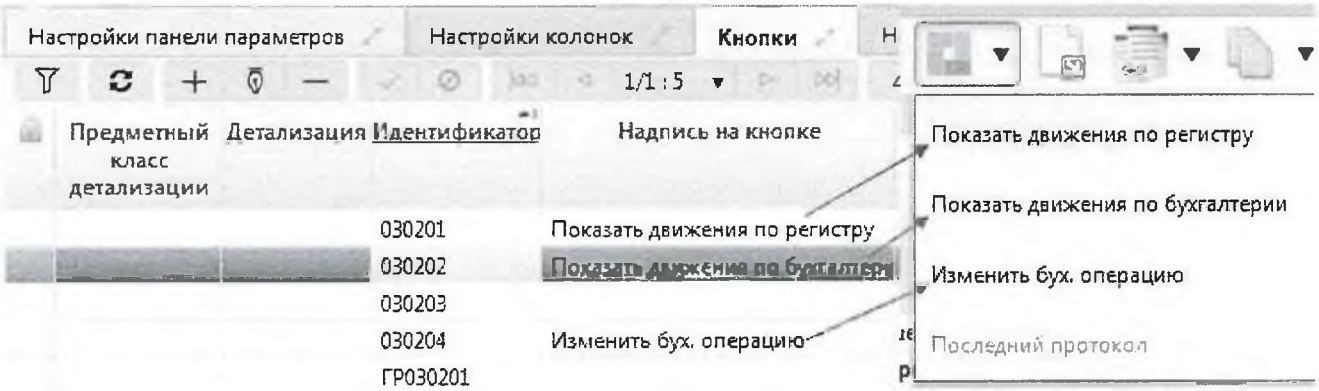


Рисунок 88 – Заполнение поля «Надпись на кнопке»

20.1.4.4. Картинка

В поле «Картинка» возможно добавить картинку, прописав полное имя картинки (или выбрав из списка), которая будет использоваться для визуализации кнопки.

Пример визуализации кнопки картинкой представлен на рисунке 89.

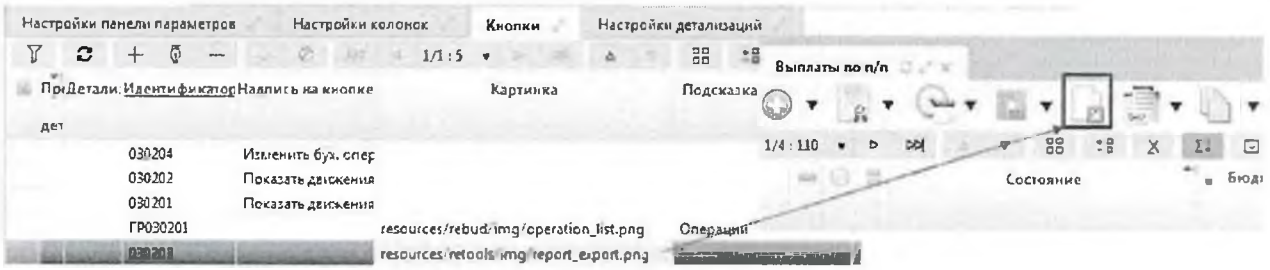


Рисунок 89– Заполнение поля «Картинка»

20.1.4.5. Подсказка для кнопки

В поле «Подсказка для кнопки» указывается всплывающая подсказка для кнопки (хинт). Пример заполнения поля «Подсказка для кнопки» представлен на рисунке 90.

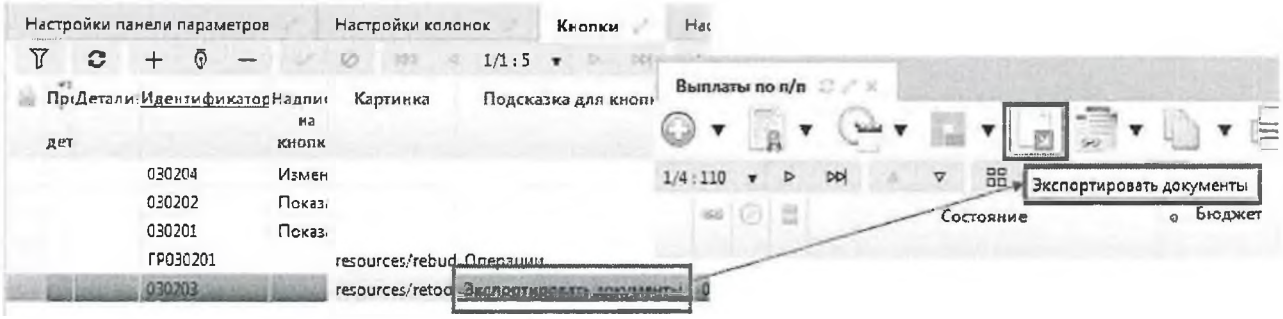


Рисунок 90 – Заполнение поля «Подсказка для кнопки»

20.1.4.6. Браузерный скрипт

Как правило, когда добавляется кнопка, требуется взаимодействие с пользователем, например, показ диалога или какая-то дополнительная логика. Чтобы реализовать это взаимодействие необходимо написать браузерный скрипт.

Пример браузерных скриптов администратор может посмотреть на работающей системе и на их основе создать свой.

На интерфейсе «Настройки системы» осуществляется выбор браузерного скрипта из справочника «Браузерные скрипты», как показано на рисунке 91. Создание собственного браузерного скрипта осуществляется на интерфейсе «Браузерные скрипты».

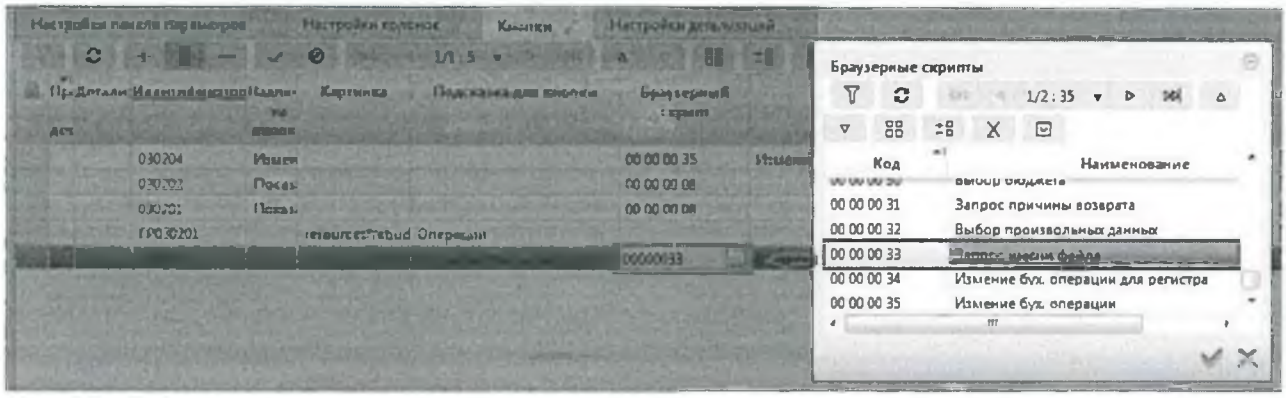


Рисунок 91 – Заполнение поля «Браузерный скрипт»

20.1.4.7. Операция

В системах реализован общий событийный механизм, который основан на сценариях обработки. Для того, чтобы подключить сценарий обработки нужно какую-то событийную точку определить либо через бизнес-процесс, либо через бизнес-операции.

Для кастомных кнопок удобен механизм бизнес-операций. Администратор может добавить новую бизнес-операцию на интерфейсе «Бизнес-операции» или использовать уже существующую. Бизнес-операция – это идентификатор события, на который дальше будет подключен сценарий обработки.

Администратор, при настройке кастомной кнопки выбирает бизнес-операцию в поле «Операция», как показано на рисунке 92.

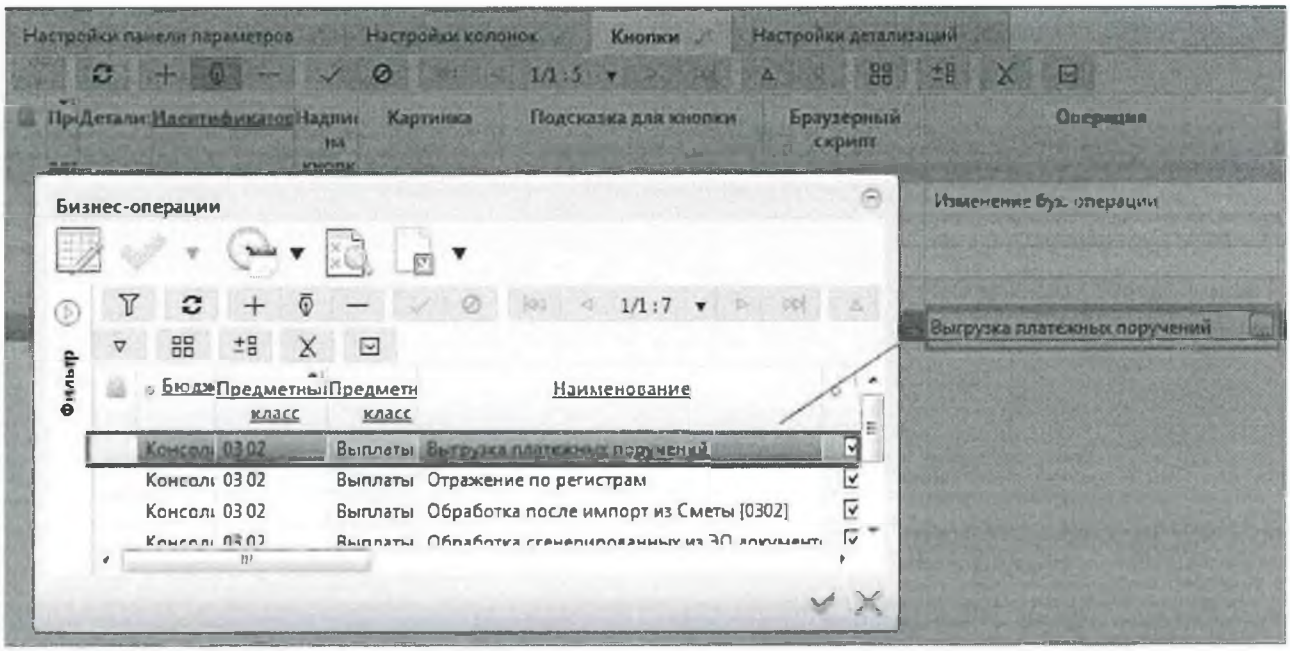


Рисунок 92 – Заполнение поля «Операция»

При нажатии кнопки будет вызываться выбранная бизнес-операция и, соответственно, все сценарии обработки, которые на нее подключены. Администратор может уже на стороне сервера подключить любую логику, например, выполнение контролей, генераций, импортов, дополнительную обработку и т.д.

20.1.4.8. Параметры операции

Поле «Параметры операции» заполняется, когда в поле «Браузерный скрипт» указан общий браузерный скрипт, используемый для нескольких кнопок. Отличия для конкретной кнопки передаются через параметры, указанные в поле «Параметры операции», как показано на рисунке 93.

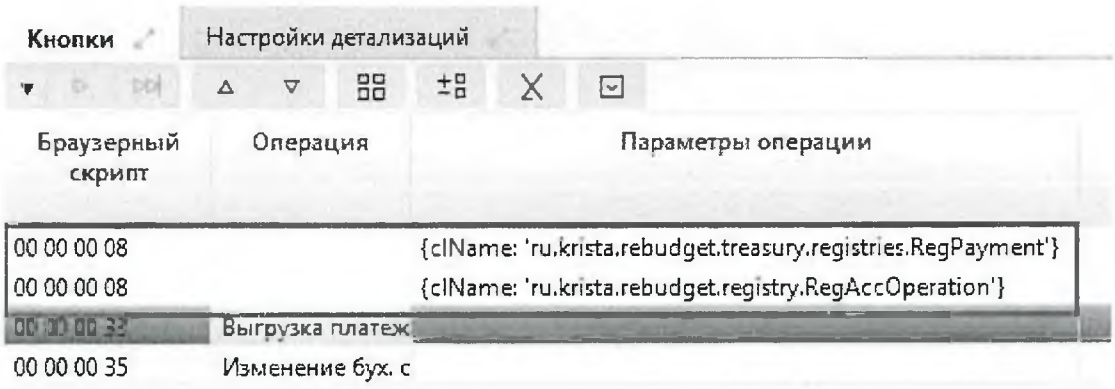


Рисунок 93 – Заполнение поля «Параметры операции»

20.1.4.9. Выводить результаты операции

В поле «Выводить результаты операции» ставится галка, если необходимо показывать протокол операций.

При выполнении операций, таких как контроль, в конце выдается окно с протоколом. Администратор может включить механизм вывода пользователю окна протокола, поставив галку «Выводить результаты операции», как показано на рисунке 94.

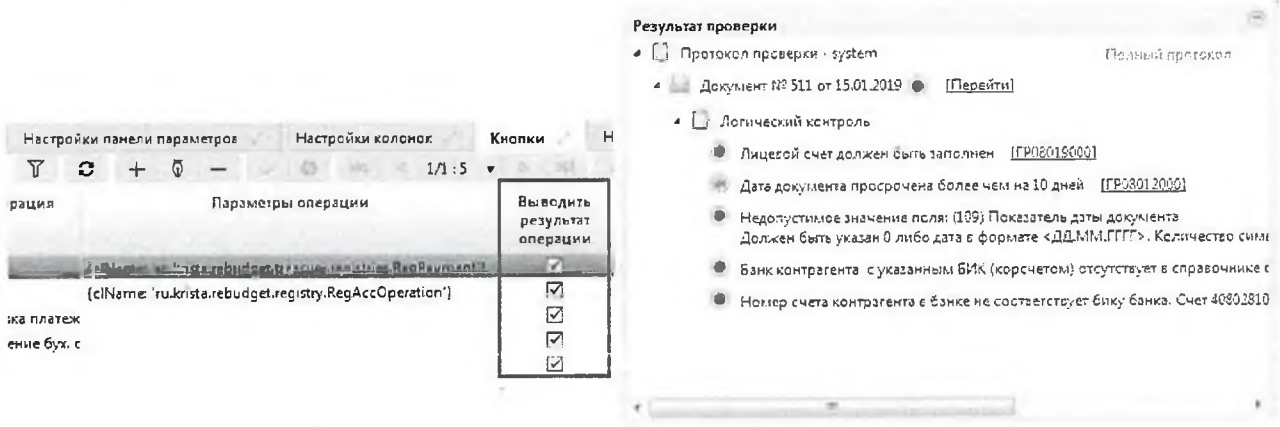


Рисунок 94 – Заполнение поля «Выводить результат операции»

20.1.4.10.Отключить

Администратор может отключить кастомную кнопку на форме ввода, установив галку в поле «Отключен».

20.1.4.11.Группа

Поле «Группа» позволяет объединять несколько кнопок в группу.

Администратор сначала должен создать строку в детализации «Кнопки» для группы, потом строки для вложенных элементов и указать у этих элементов группу, в которую они входят. Пример реализации и отображения на пользовательском интерфейсе группы кнопок представлен на рисунке 95.

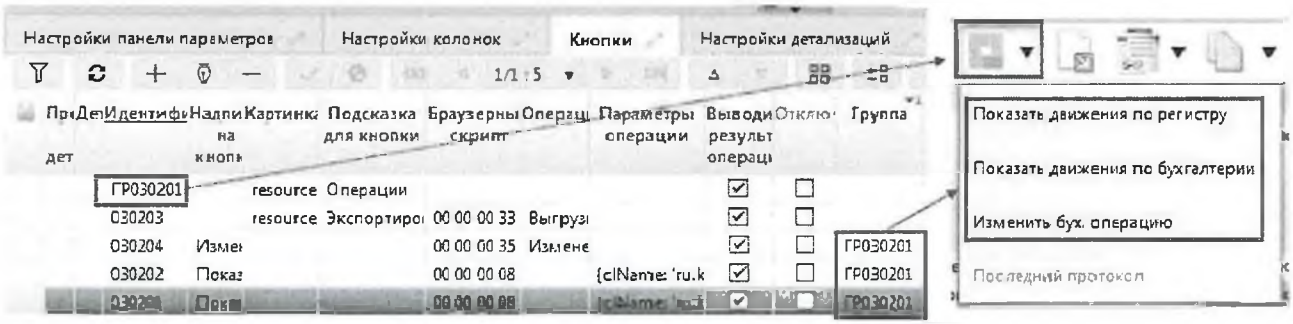


Рисунок 95– Заполнение поля «Группа»

20.1.4.12.Условие отображения

Поле «Условие отображения» может содержать декларативное правило, которое определяет будет кнопка показываться пользователю или нет.

Чаще всего поле «Условие отображения» заполняется условием вхождения пользователя в определенную группу (функция ingroup) или условием наличия у пользователя определенной роли (функция hasRole), как показано на рисунке 96.

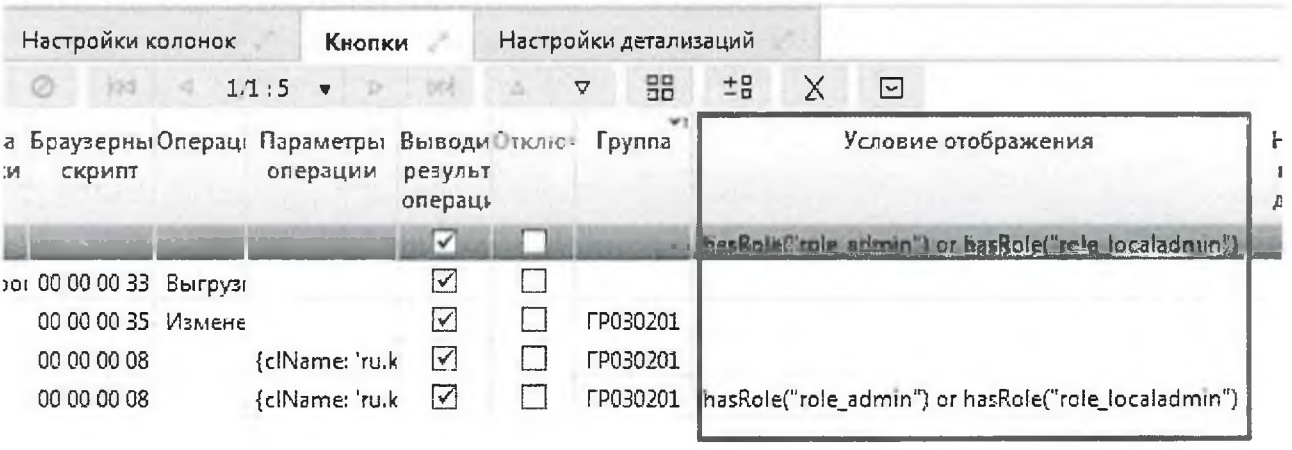


Рисунок 96 – Заполнение поля «Условие отображения»

20.1.4.13.Не требует контекста документа

Чаще всего кастомные кнопки обрабатывают выделенные документы или текущий документ. Но в ряде случаев кастомные кнопки никак не связаны с выделенными документами или текущим документом. Например, когда по кастомной кнопке добавляется новый документ или вызывается генерация. То есть кастомная кнопка в этом случае не получает ни одного документа, но при этом должна отработать и выполнить какие-то действия. В таких случаях ставится галка «Не требует контекста документа».

20.1.4.14.Порядок

Значение в поле «Порядок» определяет порядок кнопки на панели кнопок.

20.1.5. Настройка детализации

Администратор может скрыть детализацию или отобразить ранее скрытую детализацию на закладке «Настройки детализации». Это бывает удобно, когда по требованию регионов добавляется детализация, которая остальным регионам не нужна. Тогда администратор ее по умолчанию скрывает для всех. А те регионы, которым нужна эта детализация, восстанавливают у себя отображение детализации.

Администратор указывает имя детализации и ставит/снимает галку «скрыть», как показано на рисунке 97.

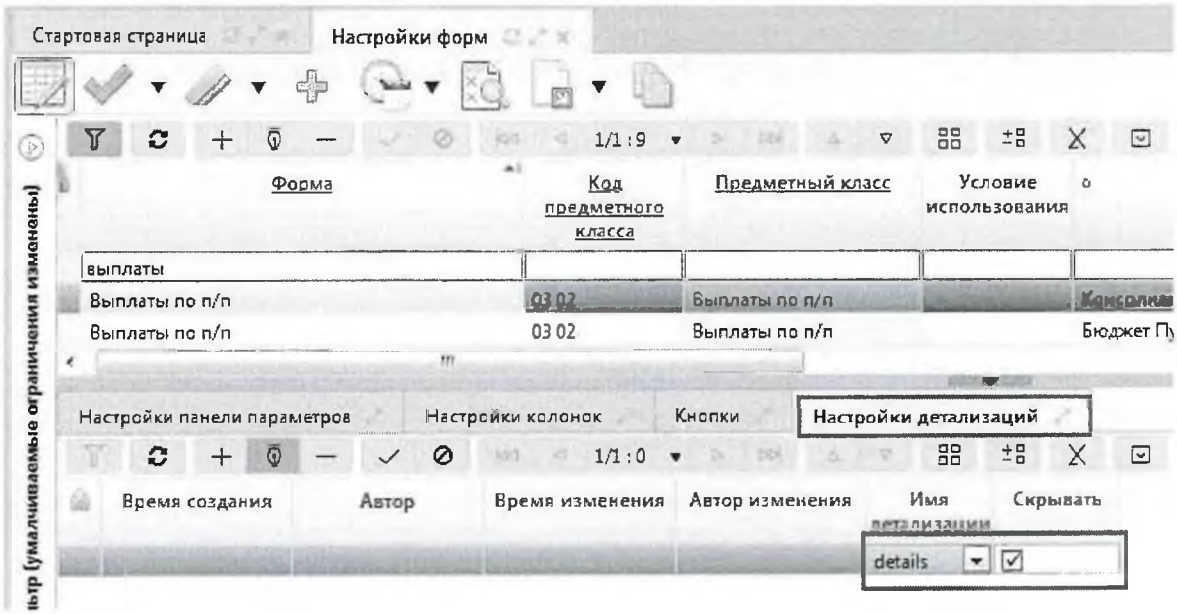


Рисунок 97– Детализация «Настройки детализации» интерфейса «Настройки форм»

20.1.6. Управление пользовательскими настройками

На интерфейсе «Настройки форм» администратор может управлять пользовательскими настройками (например, настройками видимости колонок из интерфейса).

Пользовательские настройки сохраняются в постоянном хранилище данных. Иногда возникает необходимость сбросить все пользовательские настройки, привести их к настройкам по умолчанию, например, чтобы открылась скрытая колонка. Кнопка  «Сбросить настройки пользователя для текущей формы» позволяет сбросить настройки либо всех пользователей, либо конкретного пользователя, как показано на рисунке 98.

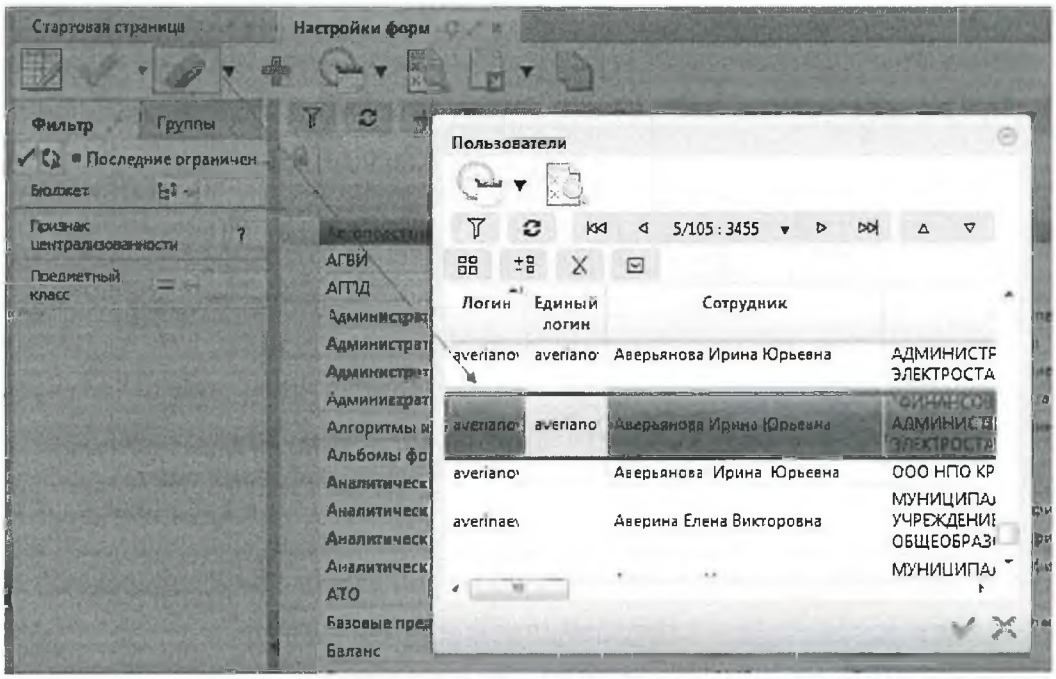


Рисунок 98 – Сбрасывание настроек формы у конкретного пользователя

20.1.7. Перекрытие настроек для конкретного бюджета

Настройка форм может быть привязана и к конкретному бюджету. В этом случае производится механизм наследования.

Пример: форма «Выплаты по п/п». Для платежных поручений существует несколько настроек форм: одна касается консолидированного бюджета, другая консолидированного бюджета городских округов и есть настройки, относящиеся к конкретным бюджетам, как показано на рисунке 99.

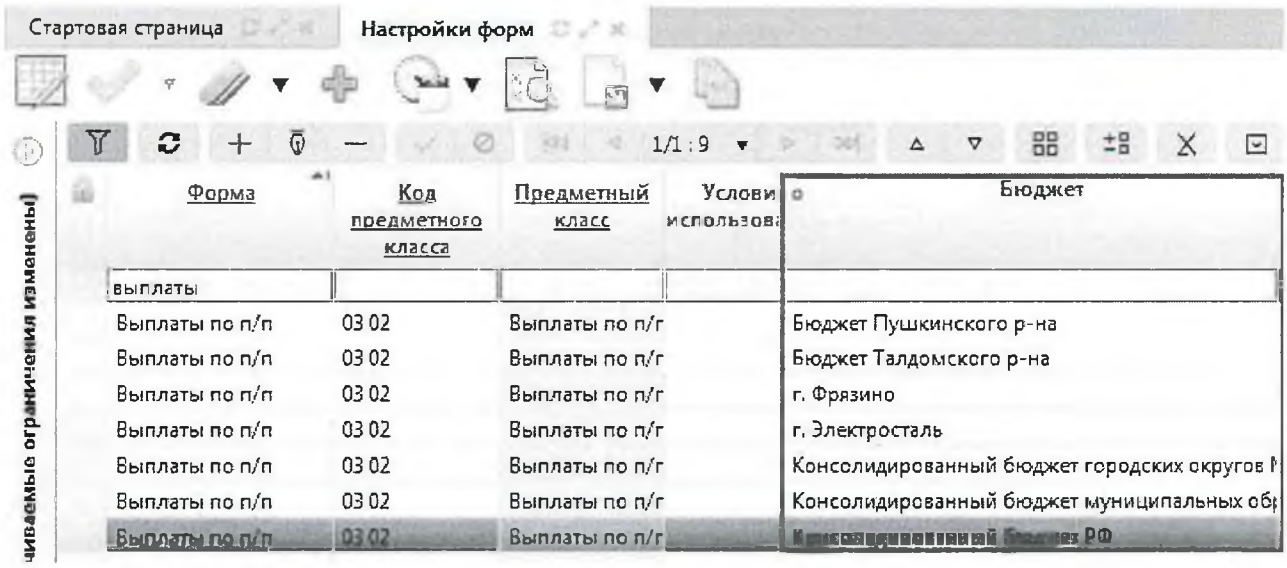


Рисунок 99 – Настройки форм для конкретных бюджетов

Когда пользователь работает на конкретном бюджете, то этому пользователю доступны несколько настроек (собственный и вышестоящие бюджеты) и система сама определяет настройки. Часть настроек берется из конкретного бюджета, а там, где они не перекрыты из более общего (верхнего). За счет этого имеет смысл перекрывать только ту часть, которая действительно должна отличаться. Все остальные настройки копировать не требуется.

20.1.8. Реализация разных настроек для различных групп пользователей

При настройке формы есть возможность скрытия/открытия колонок для определенных групп пользователей, настройки разных наборов колонок.

Разные пользователи могут работать с разным атрибутным составом. Например, если учреждение вводит документ, платежное поручение, то это учреждение работает с одним атрибутным составом. Когда ГРБС проверяет документ, он работает уже с другим атрибутным составом, нужным ему для согласования. Бухгалтер может работать с третьим атрибутным составом. Администратор в подобной ситуации может выделить группы пользователей, и каждой группе привязать свою настройку форм.

21. Синхронизация

Целью синхронизации является получение данных из внешних источников. При этом не требуется перенос данных в точности до атрибута. Требуется перенос только тех данных, которые необходимы системе, где они используются.

21.1. Дополнительные возможности синхронизации

21.1.1. Работа с локальными данными

В первую очередь в синхронизаторе реализован механизм работы с локальными данными. В предметной системе база данных может иметь собственные данные. Синхронизатор должен обновлять данные из внешних систем без ущерба для локальных данных.

Рассмотрим примеры ситуаций, когда при синхронизации в предметной системе могут быть локальные данные.

Замечание! В качестве внешней системы для синхронизации рассматривается ПК «НСИ», так как она является основным поставщиком информации, в частности справочной (здесь и далее, если говорится «синхронизация», то имеется в виду синхронизация справочников из ПК «НСИ»).

Считается, что в предметной системе может находиться свое наполнение справочников. При этом синхронизация не должна затрагивать эти данные. Такая ситуация возможна, если по какой-либо причине данные в справочниках ПК «НСИ» не утверждены, а в предметной системе возникла необходимость использования этих данных. В этом случае данные вводятся в предметную систему локально, а при синхронизации эти данные не дублируются, а используются уже имеющиеся.

21.1.2. Устойчивость к наличию неконсистентных данных

Важной возможностью синхронизации является устойчивость к внештатным ситуациям.

При синхронизации может возникать большое количество различных проблем, как с предметной точки зрения, так и с технической. Под предметными проблемами понимаются логические ошибки данных, например, несоответствующий формат ИНН учреждения. При этом синхронизируются несколько тысяч учреждений, и ошибка заполнения ИНН у одного из них не должна стать причиной несинхронизации всех учреждений.

Также есть множество технологических проблем реализации синхронизации сложных справочников: иерархических, версионных.

В синхронизаторе реализован механизм обработки ошибочных ситуаций или их пропуска.

21.1.3. Интеграция с бизнес-процессами

Справочники предметных систем представляют собой не просто набор данных, а еще привязанный к этим данным бизнес-процесс, в рамках которого выполняются дополнительные действия над данными: согласование и утверждение данных, дополнительные контроли, действия. Поэтому важным требованием для синхронизатора является интеграция с бизнес-процессами.

Реализация интеграции с бизнес-процессами, добавляет возможность вместе с синхронизацией выполнять дополнительные действия: контроли на стороне предметного решения,
генерацию дополнительных данных. Например, автоматическое создание учетных записей при синхронизации сотрудников учреждений. При синхронизации можно реализовать любое действие над данными, которое укладывается в рамки бизнес-процесса.

Так как синхронизация по сути ничем не отличается от ввода данных пользователем на интерфейсе ввода, то логично, что синхронизатор должен иметь возможность выполнять операции по бизнес-процессу.

21.1.4. Асинхронный процесс

Объемы синхронизируемых данных могут быть достаточно большие, до нескольких десятков тысяч единиц. Для синхронизируемых данных так же выполняются дополнительные действия в рамках бизнес-процесса. Таким образом, время синхронизации может быть достаточно долгим. Этот процесс может занимать часы и даже десятки часов.

Исходя из этого, процесс синхронизации реализован так, чтобы он не требовал постоянного внимания пользователя. Так же в процессе синхронизации существует возможность увидеть промежуточные результаты, чтобы оценить процесс синхронизации и целесообразность его продолжения, так же есть возможность прервать процесс в любое время.

Процесс синхронизации автоматизирован, то есть нет необходимости администратору инициировать процесс синхронизации. Существует возможность настройки расписания синхронизации, по которому синхронизация запускается в автоматическом режиме, обеспечивая перенос данных незаметно для пользователя (см. пункт 21.4).

21.2. Интерфейсы для синхронизации

21.2.1. Интерфейс «Справочник внешних систем»

Источников информации, откуда предметные системы могут получать данные достаточно много: ПК «НСИ», различные федеральные источники данных и т.д. Каждый из этих источников предоставляет информацию в своем формате. На стороне синхронизатора поддерживать все эти форматы невозможно. Поэтому было принято решение поддержать один формат, с которым удобно работать разработчику. В связи с этим, был разработан справочник внешних систем.

Справочник внешних систем, представленный на рисунке 100, располагается в группе «Синхронизация с внешними системами» РМ «Администрирование».

Рисунок 100 – Внешний вид интерфейса «Справочник внешних систем»

«Справочник внешних подсистем» - это справочник, который содержит список систем, из которых синхронизатор умеет получать информацию. «Внешняя система» - это отдельная запись в справочнике внешних систем.

В детализации «Перечень доступных справочников» содержится перечень предметных классов, которые эта внешняя система умеет поставлять, как показано на рисунке 101.

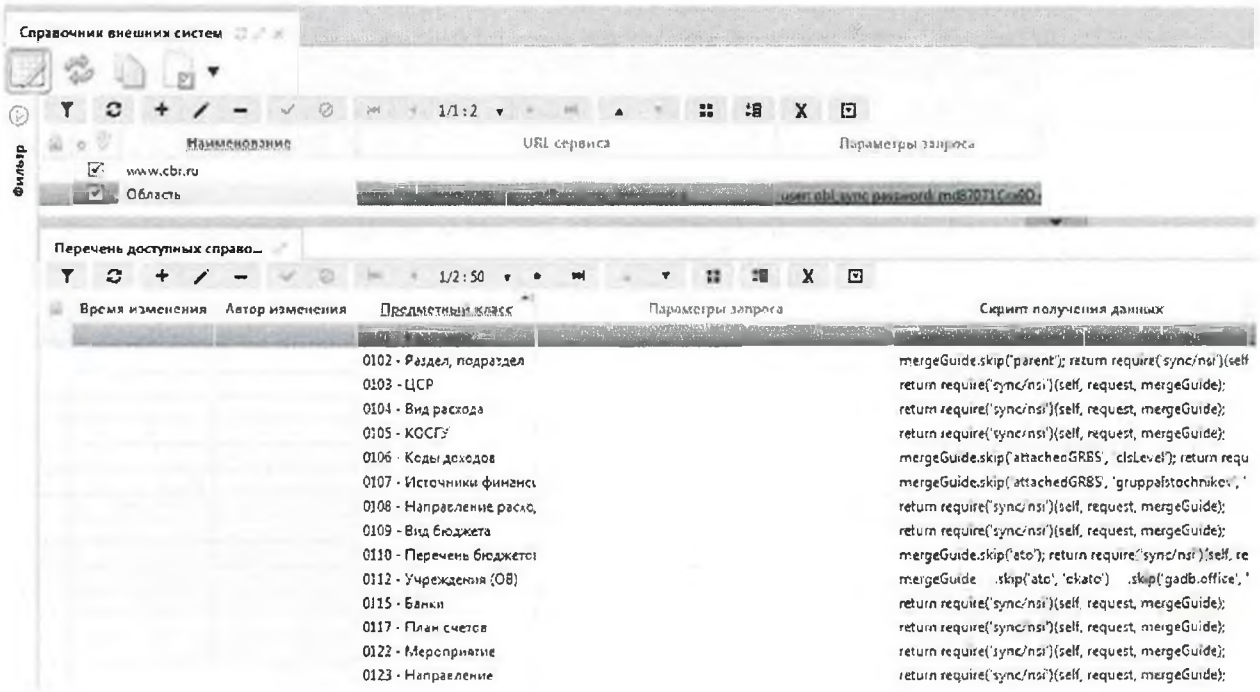


Рисунок 101 – Детализация интерфейса «Справочник внешних подсистем»

Основной задачей внешней системы является получение данных из конкретного внешнего источника данных, которую она представляет, например, ПК «НСИ», cbr.ru и представление этих данных в формате удобном синхронизатору. Это делается скриптом для каждого предметного класса, который преобразует данные в нужный синхронизатору формат. Скрипт вводится в поле детализации «Скрипт получения данных».

Таким образом, внешняя система - это описание для синхронизатора, откуда он может получать данные в нужном ему формате. Внешняя система непосредственно обращается к внешним сервисам, в том числе чтение из файла, и возвращает данные в нужном формате.

Формат данных, используемый синхронизатором - это простой набор значений, то есть имя свойства и значение свойства.

21.2.2. Интерфейс «Синхронизация»

21.2.2.1. Назначение

Сама внешняя система нам ничего засинхронизировать не сможет, она служит только для представления данных в нужном формате. Для того, чтобы запустить процесс синхронизации используется интерфейс «Синхронизация» группы «Синхронизация с внешними системами» РМ «Администрирование», представленный на рисунке 102.

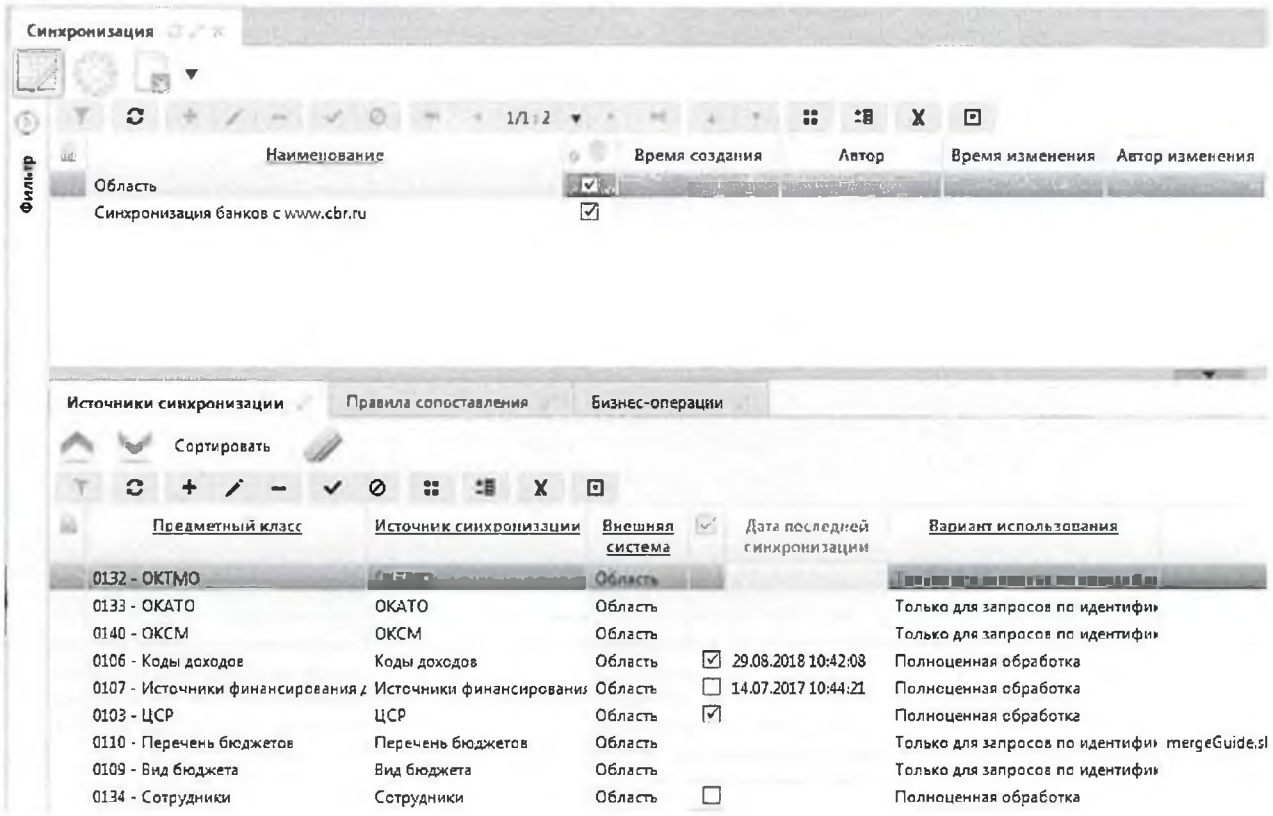


Рисунок 102– Внешний вид интерфейса «Синхронизация»

Рассмотрим на примере необходимость сущности «Синхронизация». Пусть необходимо синхронизировать какой-то конкретный предметный справочник, например, «Сотрудники». Однако сотрудники сами по себе не имеют никакого смысла без учреждения, в котором они работают. Поэтому дополнительно нужно синхронизировать еще справочник «Учреждения (ОВ)», который в свою очередь имеет ссылки на другие справочники: «Код главы», «Перечень бюджетов» и другие. Таким образом, получается довольно объемный список справочников, который необходим для синхронизации справочника «Сотрудники». Для этого и служит сущность «Синхронизация», которая представляет собой набор источников из внешних систем, связанных с конкретными предметными классами системы, и задает порядок обработки этих источников

(не имеет смысла синхронизировать справочник «Сотрудники» раньше справочника «Учреждения (ОВ)»).

Самое главное, что синхронизация позволяет начать процесс синхронизации. Администратор синхронизации выбирает конкретную запись в справочнике «Синхронизация». В рамках синхронизации выбирает конкретные источники предметных классов, которые необходимо получить, правила сопоставления, по которым будут синхронизироваться источники и бизнес-операции (описание источников синхронизации в п. 21.2.2.4, правил сопоставления в п. 21.2.2.2 и бизнес операций в п. 21.2.2.3). Чтобы запустить процесс самостоятельно, администратор синхронизации должен нажать на панели команд кнопку «Запустить процесс синхронизации».

21.2.2.2. Детализация «Правила сопоставления»

Одной из главных особенностей синхронизации является использование локальных данных. То есть, получая данные из внешней системы, синхронизатор не всегда должен создавать новую запись в справочнике. Необходимо сначала проверить: существует ли в справочнике что-то похожее на полученные данные.

Чтобы найти эти похожие данные, необходимо определить для каждого предметного класса некоторый набор правил. Правила задаются на детализации «Правила сопоставления» справочника «Синхронизация», как показано на рисунке 103.

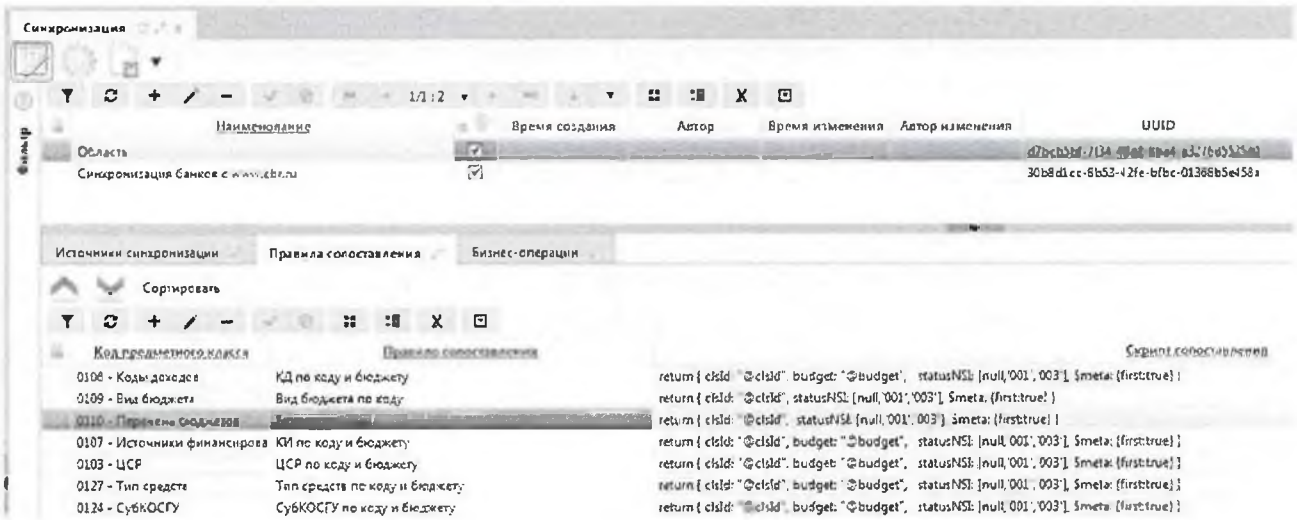


Рисунок 103 – Детализация «Правила сопоставления» интерфейса «Синхронизация»

Правила сопоставления - это набор ключевых атрибутов (полей), которые уникально идентифицируют экземпляр предметного класса. Для классификаторов это обычно поля «Код» и «Бюджет». Правила сопоставления указываются в рамках синхронизации, в них указываются правила, по каким параметрам локальные данные будут сопоставляться с синхронизируемыми.

Для одного предметного класса можно добавить несколько правил. В этом случае сначала будет осуществляться поиск по одному правилу, потом по-другому. Здесь важную роль играет порядок, в котором эти правила определены. Если ни по одному правилу ничего не нашли, то считаем, что такой записи нет и создаем новую запись в рамках синхронизации.

Изначально, правило сопоставления представляло собой скрипт, который выбирал из БД объекты, и выдавал результат поиска экземпляра, подходящего под описание. Пример скрипта представлен на рисунке 104.

Рисунок 104 – Скрипт для правила сопоставления

Со временем выяснилось, что такой подход не очень удобен, потому что он не управляемый и не дает необходимого объема информации. Синхронизатору нужно четко понимать, что именно было найдено с помощью правила сопоставления: был ли создан новый объект или вернулась версия найденного экземпляра и есть ли еще другие версии у этого экземпляра. То есть синхронизатору нужно гораздо больше информации для полноценной работы с разного вида предметными справочниками. Соответственно, анализировать и учитывать все данные в рамках правила сопоставления является нецелесообразным.

Сейчас формат правил сопоставления представляет собой перечисление атрибутов. Пример правила сопоставления представлен на рисунке 105.

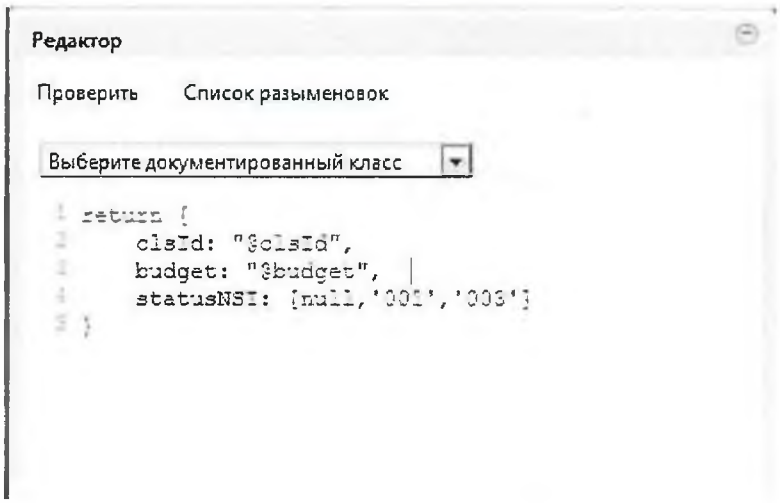


Рисунок 105 – Правило сопоставления

В правилах сопоставления атрибуты (поля) задаются в следующем виде:

<имя атрибута>: <значение атрибута>, где

<имя атрибута> - это атрибут (поле), по которому хотим построить ограничение.

Пример: clsId: “@clsId” - это значит, что в качестве ограничения по clsId нужно подставить значение clsId из описания.

Замечание! В правилах сопоставления используется параметр «statusnsi». Сейчас он уже не используется, и указывать его в новых правилах не нужно. Синхронизатор самостоятельно обрабатывает эти статусы и явно в каждом правиле их прописывать не нужно.

21.2.2.3. Детализация «Бизнес-операции»

При описании синхронизации добавляются также бизнес-операции обработки синхронизируемых данных на детализации «Бизнес-операции» интерфейса «Синхронизация», как показано на рисунке 106.

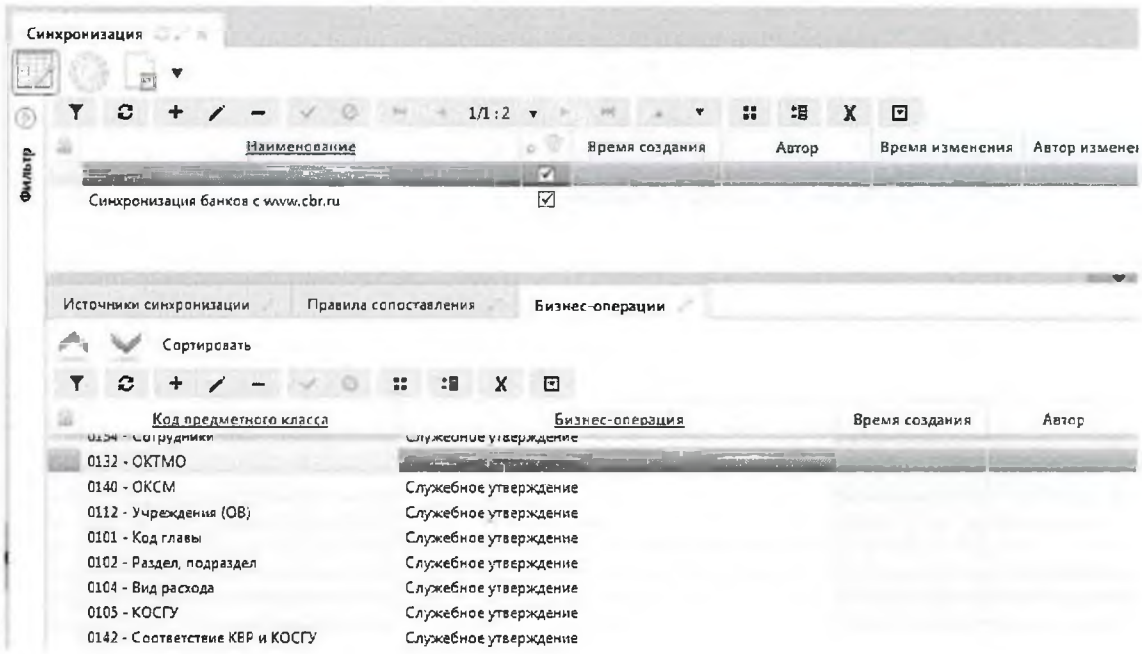


Рисунок 106 – Детализация «Бизнес-операции» интерфейса «Синхронизация»

Бизнес-операции привязываются к конкретному предметному классу. При синхронизации экземпляров предметного класса вызывается привязанная к этому классу бизнес-операция. Далее работает механизм бизнес-процессов и выполняется соответствующий сценарий.

21.2.2.4. Детализация «Источники синхронизации»

Детализация «Источники синхронизации» содержит упорядоченный перечень источников синхронизации, связанных с конкретными предметными классами системы. При этом используется достаточно много важных дополнительных атрибутов.

21.2.2.4.1 Варианты использования

Вариантом по умолчанию для данного поля является значение «Полноценная обработка». Большинство данных синхронизируется по данному варианту, как показано на рисунке107. То есть если необходимо синхронизировать данные, и нет никаких особенностей, то следует выбирать данный вариант. В результате такого варианта использования будет произведен запрос всех данных из внешней системы по определенному источнику.

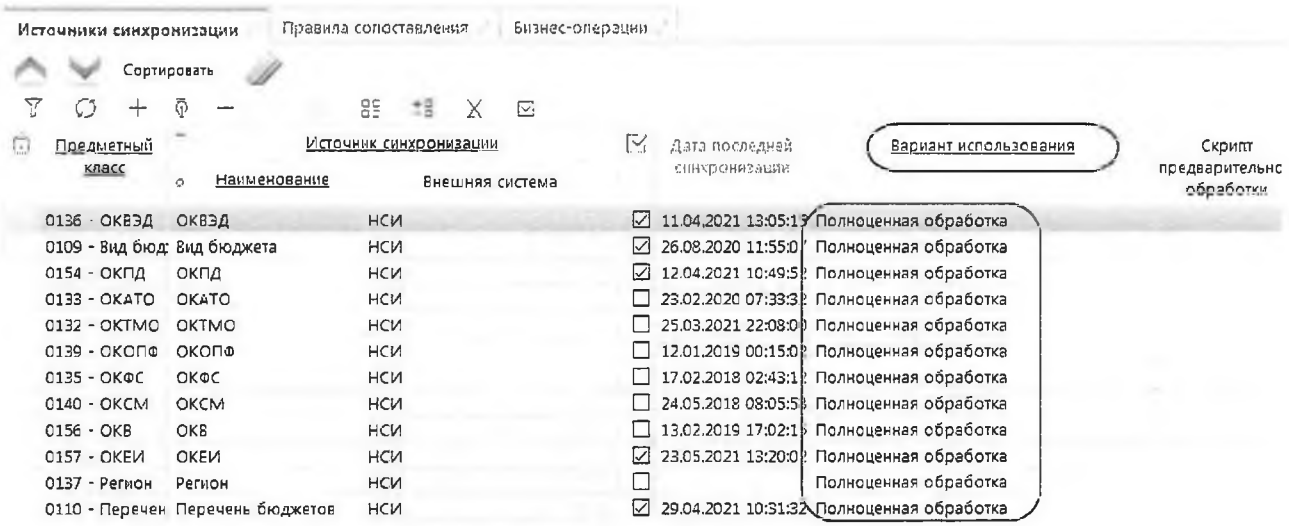


Рисунок 107 – Поле «Вариант использования» со значением «Полноценная обработка»

Бывают случаи, когда вариант использования «Полноценная обработка» нецелесообразен. Например, рассмотрим синхронизацию справочника «Учреждения (ОВ)». Экземпляры справочника ссылаются на множество классификаторов ОКФС, ОКТМО и т.д. Эти справочники достаточно объемные, но используется достаточно небольшое количество значений этих справочников. Поэтому синхронизируя справочник учреждений, хотелось бы не синхронизировать несколько тысяч записей классификаторов, а синхронизировать только те, на которые ссылаются синхронизируемые экземпляры справочника «Учреждения (ОВ)». Для этого используется вариант использования «Только для запросов по идентификатору», представленный на рисунке 108.

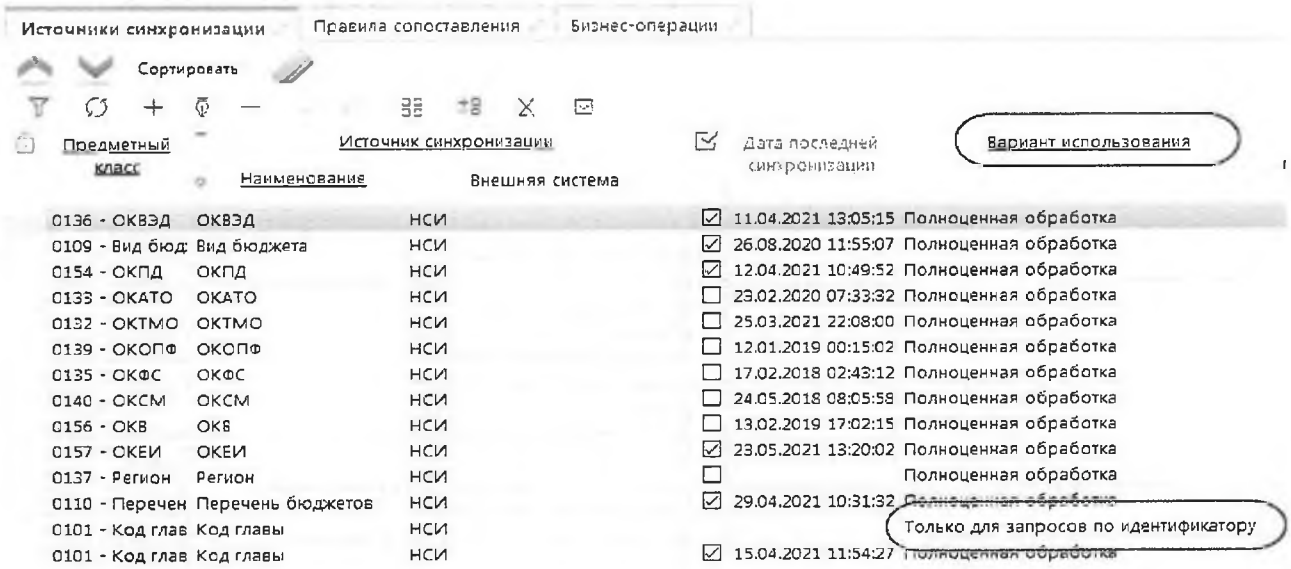


Рисунок 108 – Поле «Вариант использования» со значением «Только для запросов по идентификатору»

Источник синхронизации, для которого установлен вариант использования «Только для запросов по идентификатору», при синхронизации будет пропущен в общем списке, не будет сам инициировать запросы во внешнюю систему.

При синхронизации предметного класса, у которого ссылочным атрибутом является, например, ОКТМО, и экземпляра которого нет в системе, синхронизатор воспользуется источником «ОКТМО» и вариантом использования «только для запросов по идентификатору» для получения нужного экземпляра. Следовательно, получится большое количество единичных запросов во внешнюю систему, но на практике это весьма продуктивно работает.

Таким образом, вариант использования «Только для запроса по идентификатору» применяется, когда справочник сам по себе не используется в предметной системе, но используется в других справочниках (моделях).

Рассмотрим, каким образом некоторые справочники запрашивают все данные, а другие только по конкретному идентификатору.

В детализации справочника «Справочник внешних систем» есть поле «Скрипт получения данных», как показано на рисунке 101. Необходимо дополнительно прописать в скрипт вариант использования. В скрипте за вариант использования отвечает параметр «request». Этот параметр можно дополнительно обработать и скорректируется запрос к внешней системе.

Однако не все внешние системы позволяют изменять вариант использования, например, банки предоставляют архив с XML - файлом, в котором содержится полный перечень банков. Соответственно, в рамках справочника «БИК» невозможно построить запрос по конкретному идентификатору.

21.2.2.4.2 Скрипт предварительной обработки

В моделях предметных систем есть такие ситуации, когда один справочник ссылается на другой, а тот в свою очередь ссылается на первый. Ярким примером являются справочники «Учреждения (ОВ)» и «Код главы». У учреждения есть глава, который в свою очередь является учреждением. Соответственно, бывают ситуации, когда у учреждения установлен код главы, являющийся этим же учреждением. Используя схему синхронизации, когда поочередно синхронизируем каждый предметный класс, возникнет ситуация, что такую цепочку не будет возможности синхронизировать, возникнет зацикленность.

Рассмотрим вариант решения этой проблемы. Логично предположить, что значений в справочнике «Код главы» меньше, чем значений в справочнике «Учреждения (ОВ)». Поэтому можно справочник «Код главы» синхронизировать 2 раза, как показано на рисунке109.

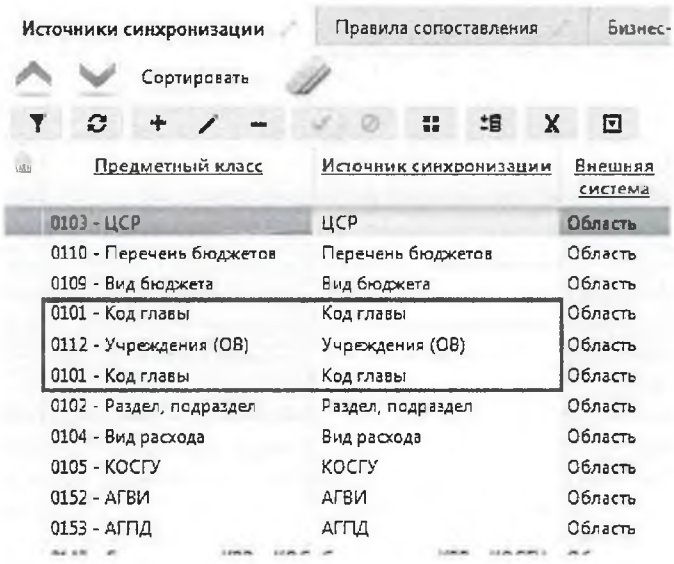


Рисунок 109– Двойная синхронизация справочника «Код главы»

Первый раз синхронизируется справочник «Код главы» без обязательного требования заполнения ссылки на учреждение. Для того, чтобы осуществить такую синхронизацию, нужно еще одно поле «Скрипт предварительной обработки», представлено на рисунке 110, в котором можно к уже полученным описаниям из внешней системы добавить дополнительную информацию. Например, если написать «mergeGuide.optional('office')» в скрипте, то это значит, что атрибут «office» (ссылка на учреждение) у экземпляра справочника «Код главы» является опциональным, то есть необязательным к заполнению.

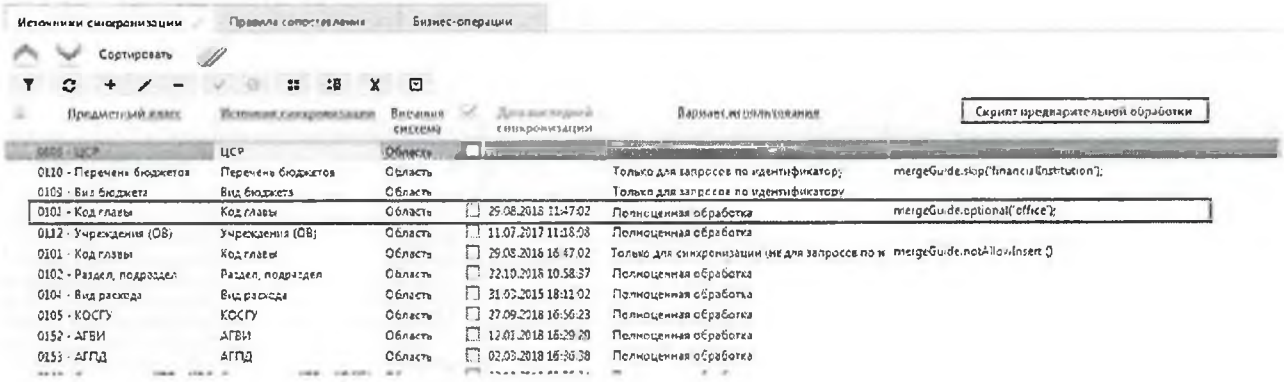


Рисунок 110 – Поле «Скрипт предварительной обработки» детализации «Источники синхронизации» справочника «Синхронизация»

Когда идет разрешение ссылочных атрибутов (описание процесса разрешения ссылочных атрибутов описано в пункте 21.3), синхронизатор пытается найти нужное учреждение по правилам сопоставления. Но если такое учреждение не находится, то синхронизатор считает, что этого атрибута в описании нет.

После первой синхронизации справочника «Код главы» выполняется обычная синхронизация справочника «Учреждения (ОВ)».

Далее добавляется еще одна синхронизация справочника «Код главы», у которой в варианте использования указывается «Только для синхронизации (не для запросов по идентификатору)». Указание такого варианта использования необходимо, чтобы второй источник синхронизации справочника «Код главы» никогда не использовался для запроса недостающих данных. Вариант использования «Только для синхронизации» - это та же полноценная обработка. Но при второй синхронизации справочника «Код главы» нет необходимости снова добавлять новые коды, нужно лишь у имеющихся кодов глав проставить ссылку на организацию. Для этого так же используется скрипт предварительной обработки. Необходимо прописать в скрипте «mergeGuide.notAllowInsert ()» - это значит, что для всех описаний, полученных из источника, не разрешается добавлять новые коды, как представлено на рисунке 111. То есть, если синхронизатор по правилу сопоставления не нашел подходящего кода в справочнике, то просто игнорирует пришедшее из внешней системы описание, не создавая новой записи.

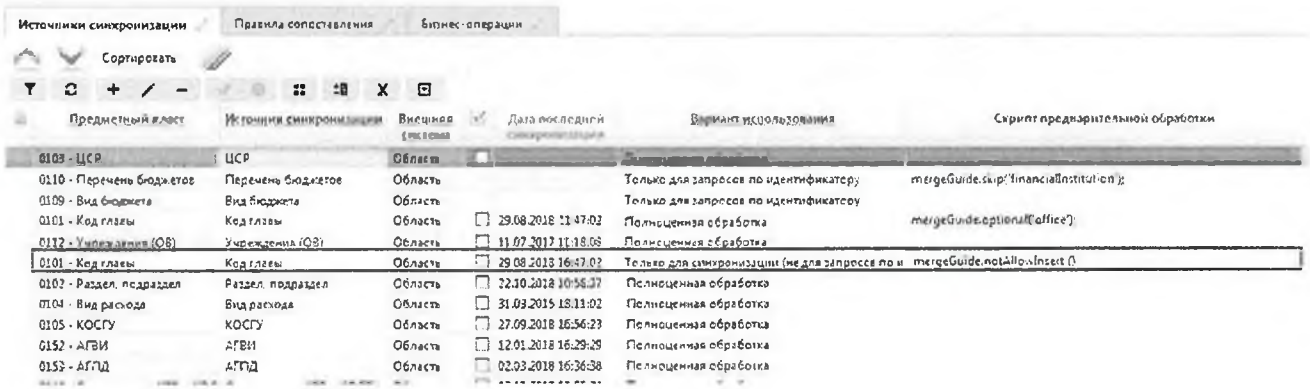


Рисунок 111 – Синхронизация с вариантом использования «Только для синхронизации»

Существуют также другие аналогичные циклические цепочки:

— между учреждением, вышестоящим учреждением и ЦБ, то есть сначала надо синхронизировать учреждения без ЦБ, а потом заполнять ЦБ;

— между учреждением и бюджетом.

21.2.2.4.3 Поле «Используется»

Поле «Используется» заполняется только для варианта использования «Полноценная обработка». Когда требуется синхронизация предметного класса, флаг возводится, когда не требуется, соответственно не возводится (сбрасывается).

Если используется другой вариант использования, то поле «Используется» не заполняется и не учитывается.

21.2.2.4.4 Дата последней синхронизации

Во внешних системах присутствуют достаточно объемные и тяжеловесные справочники, например, «Учреждения (ОВ)». Если синхронизатор каждые 10 минут будет синхронизировать весь объем данных, то в 10 минут, естественно, не уложится. Синхронизация может идти часами.

Поэтому синхронизация позволяет получить не все данные, а данные на определенный момент времени (метку времени). Для этого предназначено поле «Дата последней синхронизации», как представлено на рисунке 112.

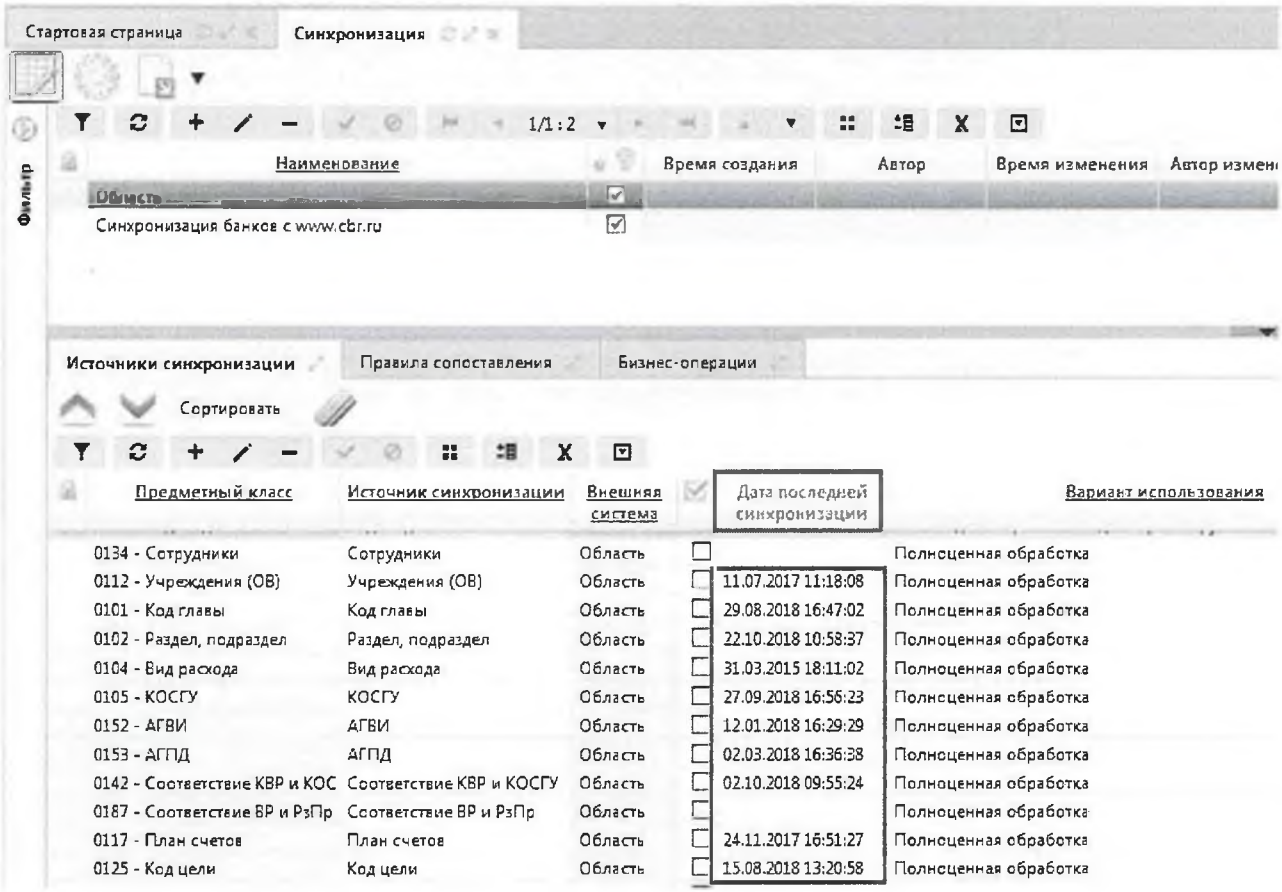


Рисунок 112 - Поле «Дата последней синхронизации» детализации «Источники синхронизации» справочника «Синхронизация»

То есть запоминается, когда данные были получены из ПК «НСИ» в последний раз. Соответственно, при следующей синхронизации, запрашиваются не все данные, а только те, которые изменились с момента времени последней синхронизации. Это делается на уровне скрипта в справочнике «Справочник внешних подсистем» в детализации «Перечень доступных справочников», как показано на рисунке 101. Для этого используется параметр «request».

Замечание! Параметр «request» имеет 3 значения:

— получить все данные;

— получить данные по некоторой метке времени;

— запросить данные по конкретному идентификатору.

Дату последней синхронизации можно изменить. Рассмотрим случаи, когда это бывает полезным.

Самый простой вариант, ее можно очистить и попытаться синхронизировать полностью весь справочник, когда это требуется.

Можно дату изменить. Например, был запущен сеанс синхронизации, который отработал с ошибкой. При повторном запуске синхронизации эта ошибка остается в прошлом. Соответственно, синхронизатор двигает дату с расчетом, что при следующей синхронизации получатся все данные, в том числе и ошибочные с прошлого раза. Это с одной стороны снижает быстродействие синхронизации, а с другой стороны не позволяет забыть про ошибочные данные.

Однако не все ошибки можно исправить, с некоторыми приходится мириться. В этом случае помогает ручная корректировка даты вперед от даты последней синхронизации.

Очищать дату рекомендуется также тогда, когда у учетной записи администратора синхронизации расширили права, например, синхронизировали по одному бюджету и добавили новый. Дата синхронизации устанавливается одна на все данные всех бюджетов. Соответственно, чтобы администратор синхронизации мог получить все данные по добавленному бюджету, а не только с даты последней синхронизации, дату необходимо очистить.

Так же рекомендуется штатно сбрасывать дату, когда возникает ошибка синхронизации со стороны ПК «НСИ».

На панели команд детализации «Источники синхронизации» есть кнопка  «Очистить момент времени последнего изменения во внешней системе». Если синхронизируются данные внешней системы, в частности ПК «НСИ», синхронизатор прикладной системы сохраняет дату последнего изменения данных во внешней подсистеме. Это время используется и для задач оптимизации, когда обрабатывается расписание. Эта дата сравнивается с датой последнего изменения в текущей прикладной системе и если они совпадают, то считаем, что синхронизация для такой записи не нужна.

Кнопка «Очистить момент времени последнего изменения во внешней системе» нужна для сброса даты в случае нештатной ситуации. При нажатии на эту кнопку у выбранных справочников очищаются даты последнего изменения во внешней системе, начиная с даты, заданной в поле «дата последней синхронизации». В случае нештатной ситуации, после очистки даты последней синхронизации и нажатия кнопки «Очистить момент времени последнего изменения во внешней системе», синхронизатор обновит все данные без пропусков.

21.2.3. Интерфейс «Сеансы синхронизации»

21.2.3.1. Общие сведения

Интерфейс «Сеансы синхронизации» располагается в группе «Синхронизация с внешними системами» РМ «Администрирование». Внешний вид интерфейса представлен на рисунке 113.

При старте синхронизации автоматически создается запись сеанса синхронизации, которая является протоколом выполнения конкретного процесса синхронизации.

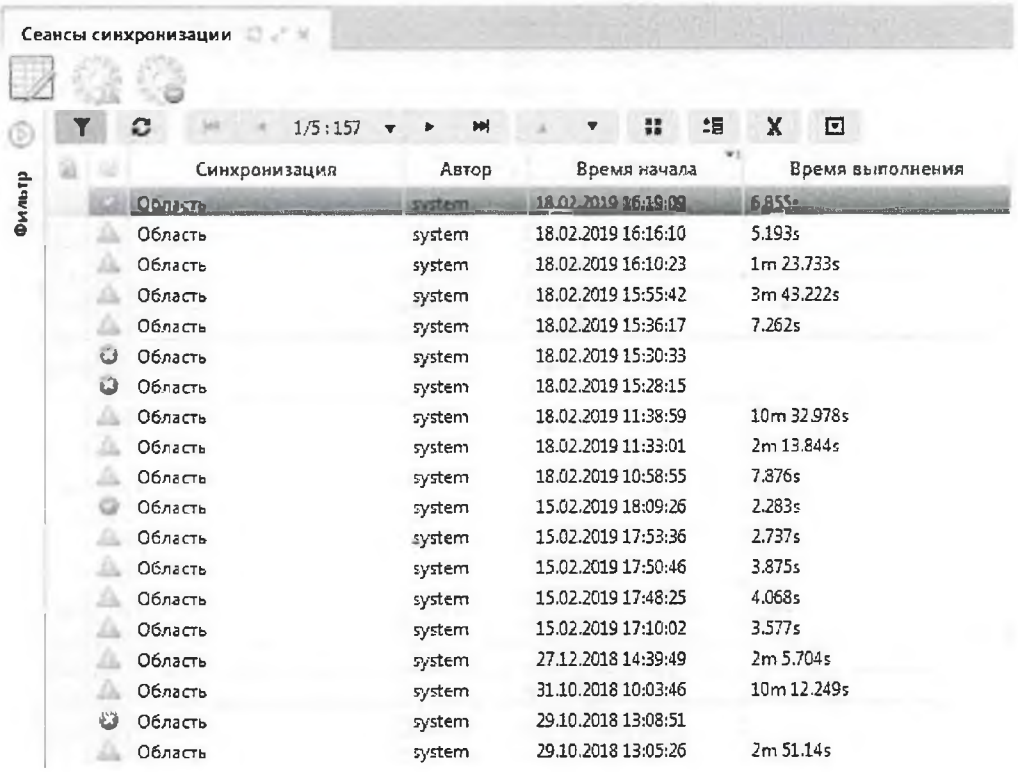


Рисунок 113 – Внешний вид интерфейса «Сеансы синхронизации»

Запись сеанса синхронизации содержит всю необходимую информацию: какая синхронизация была запущена, в какое время она завершилась (если завершилась), сколько времени занял процесс синхронизации и статус завершения.

Существуют следующие статусы завершения синхронизации:

— «Завершен», означает, что загрузка выполнена без ошибок;

— «Завершен с ошибками», означает, что синхронизация завершилась с ошибками. Такое завершение не является критичной проблемой, так как одно из условий синхронизации - устойчивость к ошибкам. Тем самым возможно некоторые экземпляры не синхронизировать. Если синхронизация выполнилась с ошибками, то ставится соответствующий статус и в протоколе выводятся эти ошибки;

— «Завершенаварийно», означает, что во время синхронизации произошли ошибки, из-за которых дальнейшая синхронизация стала невозможна или нецелесообразна. Процесс завершился прерыванием.

21.2.3.2. Журнал ошибок синхронизации

Если синхронизация завершилась с ошибками, то в детализации сеанса синхронизации содержится журнал ошибок синхронизации, как показано на рисунке 114.

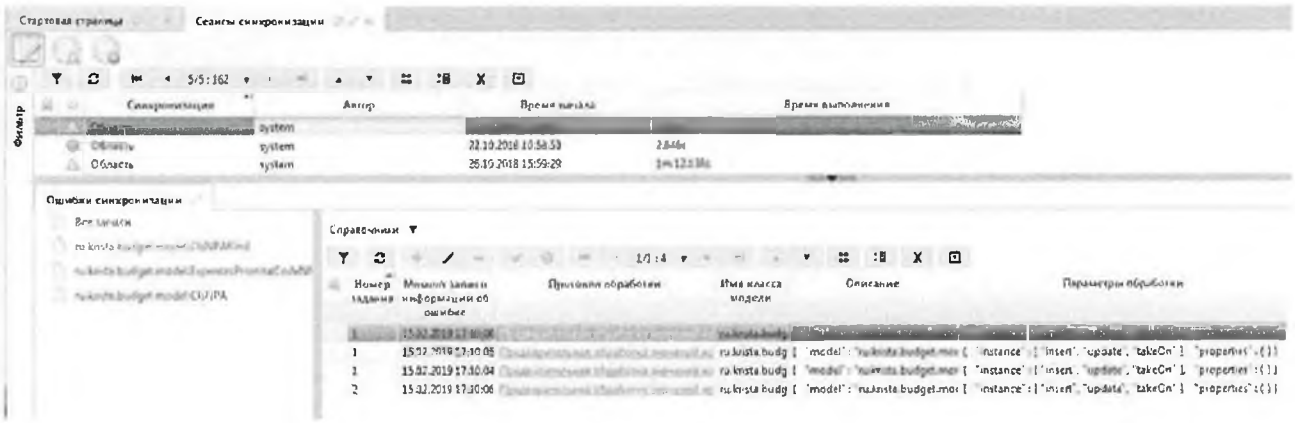


Рисунок 114– Детализация «Ошибки синхронизации» справочника «Сеансы синхронизации»

Ошибка синхронизации представляет собой запись, с указанием момента времени, когда произошла ошибка, имени класса объекта, описания. Самое полезное в записи ошибки синхронизации - это протокол обработки, просмотрев который администратор синхронизации может понять, что пошло не так и, возможно, исправить ошибку. Пример протокола обработки представлен на рисунке 115.

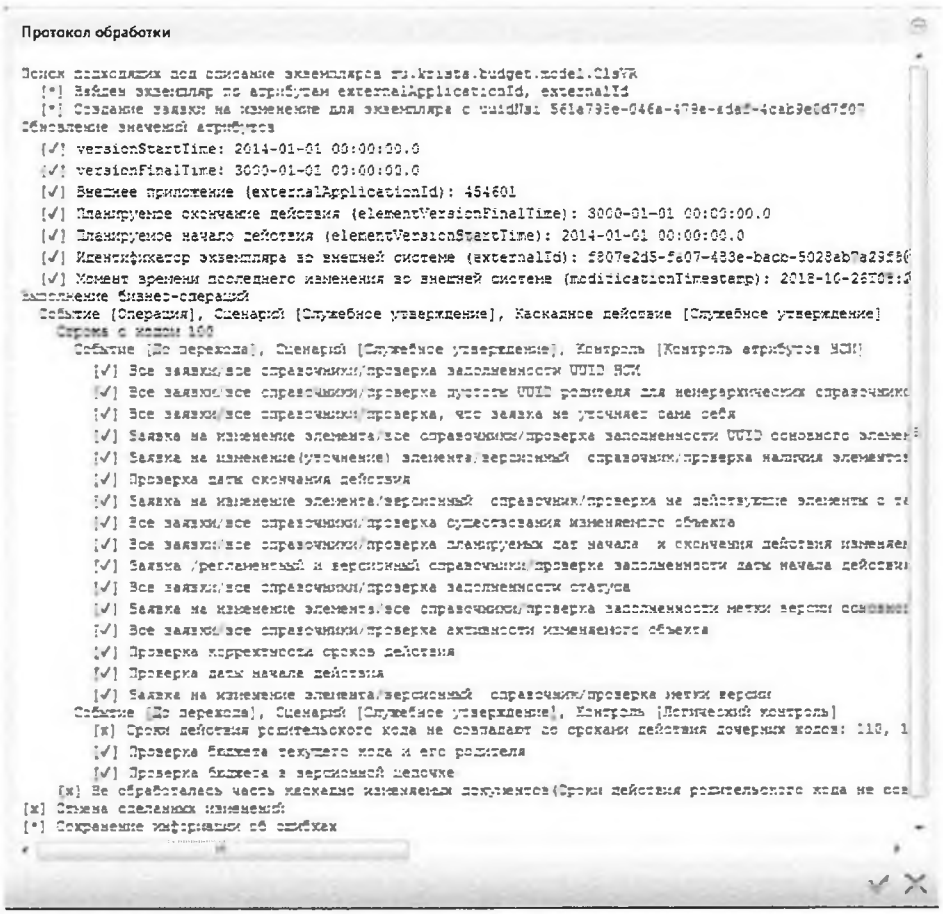


Рисунок 115 – Протокол обработки ошибки синхронизации

Для администратора синхронизации доступны следующие действия с сеансом синхронизации:

—  «Прервать процесс синхронизации», позволяет прервать запущенный процесс синхронизации;

— «Запустить процесс синхронизации повторно с ошибочными описаниями», позволяет запустить синхронизацию ошибочных экземпляров.

Повторная обработка ошибочных экземпляров выполняется локально, то есть никакого взаимодействия с внешней системой не происходит. У синхронизатора есть все необходимые данные.

Если взять конкретный ошибочный экземпляр, то для синхронизатора он выглядит так, как показано на рисунке 116.

Рисунок 116 – Описание ошибочного экземпляра

Это по сути json, который содержит имя свойства и значение. Теоретически администратор синхронизации можем понять, что ошибка была, например, в том, что значение поля было указано неверно. Чтобы избавиться от этой ошибки администратор синхронизации может отредактировать описание ошибочного экземпляра, сохранить его и запустить повторную синхронизацию. Повторно уже будет обрабатываться исправленное описание. Такой метод является одним из механизмов решения проблем синхронизации.

21.3. Процесс синхронизации

Процесс синхронизации состоит из нескольких этапов.

Замечание! Процесс получения данных из внешних систем – это отдельный процесс, который в рамках работы синхронизатора не рассматривается.

Предположим, что данные получены синхронизатором в нужном формате. Дальше синхронизатор начинает обрабатывать каждое пришедшее описание.

Алгоритм работы синхронизатора при обработке отдельного описания:

1. Преобразование значений. Синхронизатор просматривает все значения атрибутов и пытается их преобразовать в нужные типы, например, дата пришла строкой, ее нужно преобразовать в тип «дата».

1.1. Разрешение ссылочных атрибутов. Есть поля типа ссылки на другую сущность, то есть ссылки на другое описание, например, поле «Бюджет». Соответственно, чтобы получить значение для поля «Бюджет», нужно сначала по описанию бюджета найти запись, соответствующую этому бюджету, то есть по сути рекурсивно решить исходную задачу. Таким образом, для всех ссылок синхронизатор пытается сопоставить значение из соответствующего справочника, которое мы в дальнейшем будем использовать при обновлении этого атрибута.

При этом может возникнуть проблема отсутствия подходящей ссылки. Это является сигналом к тому, что можно прекращать обработку описания, потому что мы не можем привести конкретный экземпляр в соответствие с описанием.

Однако существует вариант решения этой проблемы. Синхронизатору известно, из какой внешней системой получены данные, и, возможно, в текущей синхронизации уже есть источник для этой модели, например, для бюджета, как показано на рисунке 117.

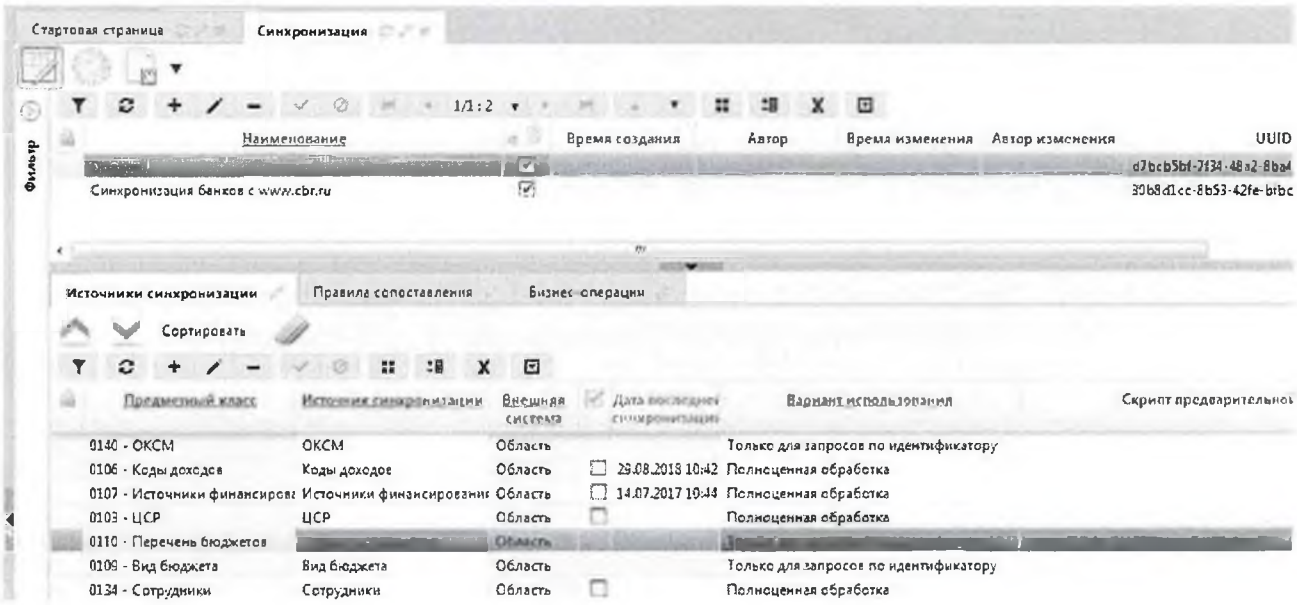


Рисунок 117 – Источник синхронизации для справочника «Перечень бюджетов»

Синхронизатор найдя такой источник может запросить у этого источника по идентификатору нужной ссылки дать полные данные, чтобы сначала этот объект засинхронизировать, а потом вернуться к обработке исходного объекта и поставить на него ссылку. Это один из основополагающих моментов обработки.

2. Поиск подходящего экземпляра. Если преобразование значений прошло успешно, то далее с помощью правил сопоставления ищется подходящий экземпляр. Берутся все правила сопоставления по нужному предметному классу. На основе правил определяются ограничения. Далее осуществляется запрос в базу. Если этот запрос находит подходящий экземпляр, то поиск завершается. Если не находит, то осуществляется поиск по следующему правилу сопоставления. Если ни одно правило сопоставления ничего не нашло, то синхронизатор считает, что это новый экземпляр и добавляет его в предметный класс.

2.1. Определение способа обновления. Когда найден экземпляр по правилу сопоставления, синхронизатор должен решить обновить у него атрибуты или необходимо создать новую версию. Это имеет смысл только для версионных справочников, которые имеют не только сроки действия, но еще и различные версии.

Кроме того, при обновлении справочников региональной ПК «НСИ» из Федеральной нормативно-справочной информации синхронизатор должен уметь работать с механизмом заявок, то есть создавать заявки на изменение, уточнение и т.д.

3. Обновление атрибутов.

4. Выполнение бизнес-операций, если они есть, для измененных атрибутов.

Важно! Все эти этапы происходят внутри одной транзакции. То есть каждое описание обрабатывается в рамках своей транзакции. Это позволяет откатывать конкретные неудачные описания, что позволяет синхронизировать как можно больше описаний.

Операция обновление атрибутов синхронизатором сопоставима с тем, что пользователь вручную меняет на интерфейсе атрибут. Все проверки, автоподстановки, декларативные правила и др., все будет выполняться и при действиях синхронизатора. Синхронизация - это некий стресс-тест всей системы. Отсюда и возникает большое количество ошибок. Любая ошибка контроля или автоподстановки в синхронизаторе выглядит как ошибка синхронизации.

21.4. Настройка выполнения синхронизации по расписанию

Одним из требований к процессу синхронизации - выполнение синхронизации по заданному расписанию. В предметных системах есть возможность выполнения заданий по расписанию.

21.4.1. Интерфейс «Задания»

Настройка расписания начинается с создания задания на интерфейсе «Задания» группы «Выполнение по расписанию» РМ «Администрирование», представленном на рисунке 118.

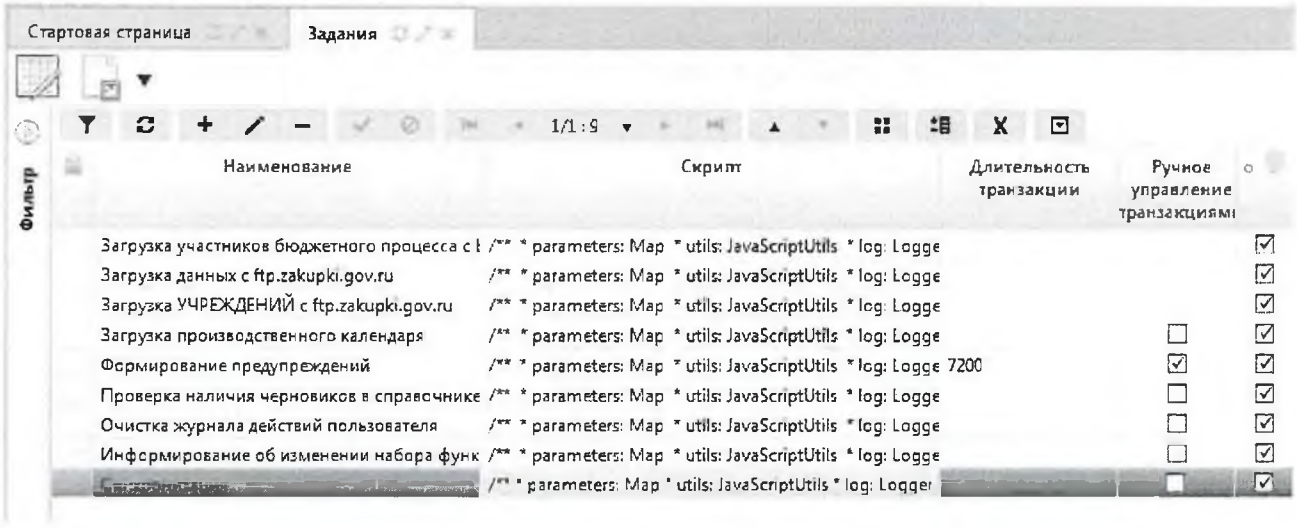


Рисунок 118 – Внешний вид интерфейса «Задания»

Задания представляют собой набор действий, которые можно выполнить. Задание представляет собой скрипт, как представлено на рисунке 119.

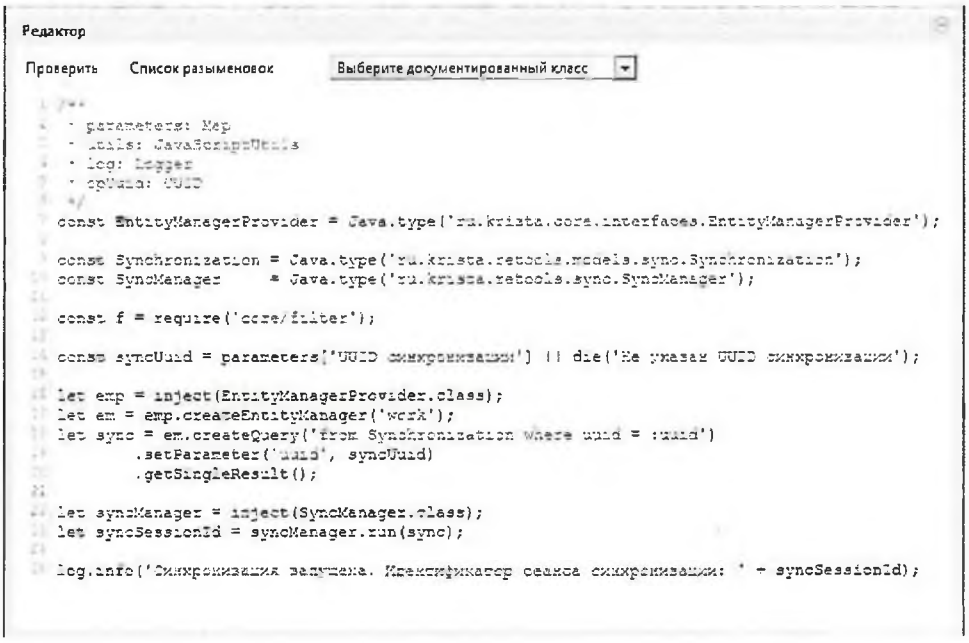


Рисунок 119 – Скрипт задания

Важно! В списке заданий есть централизованное задание, которое запускает синхронизацию. Скрипт этого задания представлен на рисунке 119. Все что оно делает - это запускает синхронизацию. У этого задания есть параметр «UUID синхронизации, как представлено на рисунке 120, который используется при построении расписания на интерфейсе «Расписание».

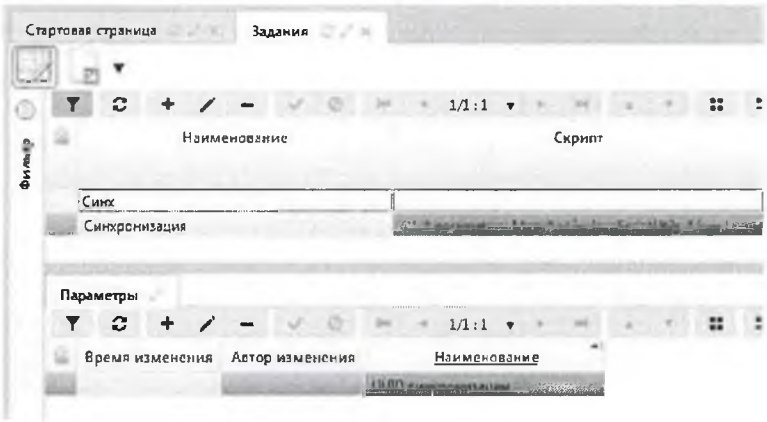


Рисунок 120 – Задание «Синхронизация»

21.4.2. Интерфейс «Расписание»

Для каждого задания можно задать конкретную периодичность выполнения на интерфейсе «Расписание» группы «Выполнение по расписанию» РМ «Администрирование». Периодичность задается в определенном формате, показанном на рисунке 121.

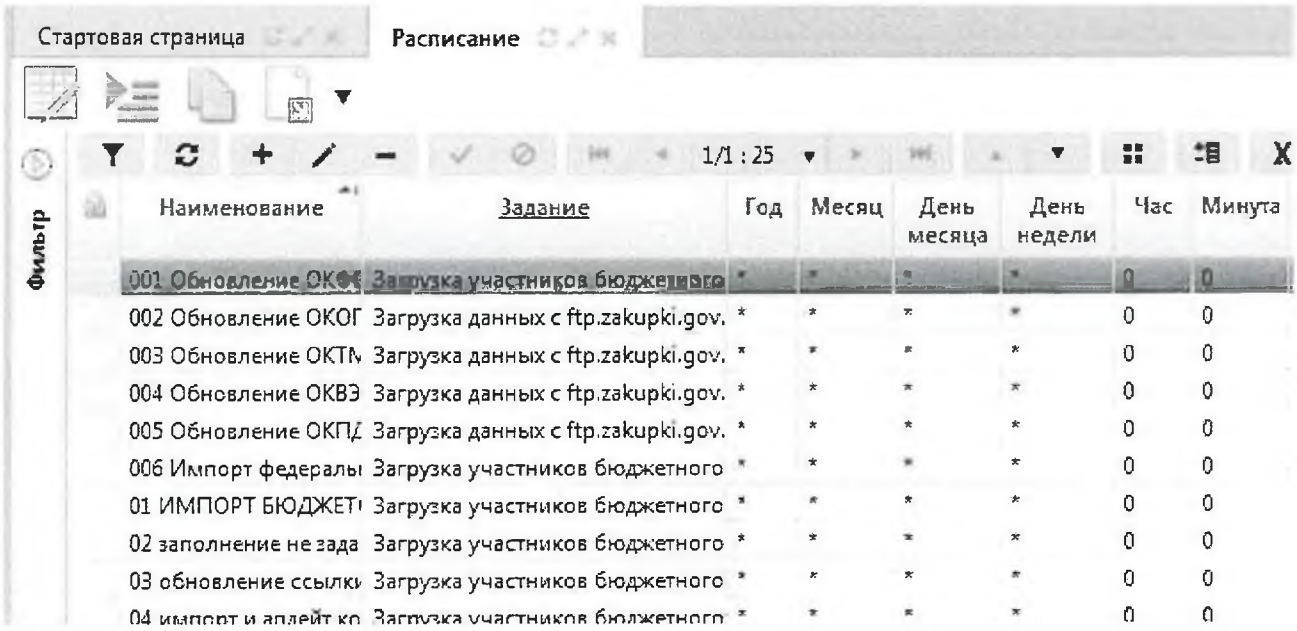


Рисунок 121 – Внешний вид интерфейса «Расписание»

В расписании присутствует запись для синхронизации с ПК «НСИ», в детализации которой определяется конкретный UUID, определенный на интерфейсе «Синхронизация», как показано на рисунке122.

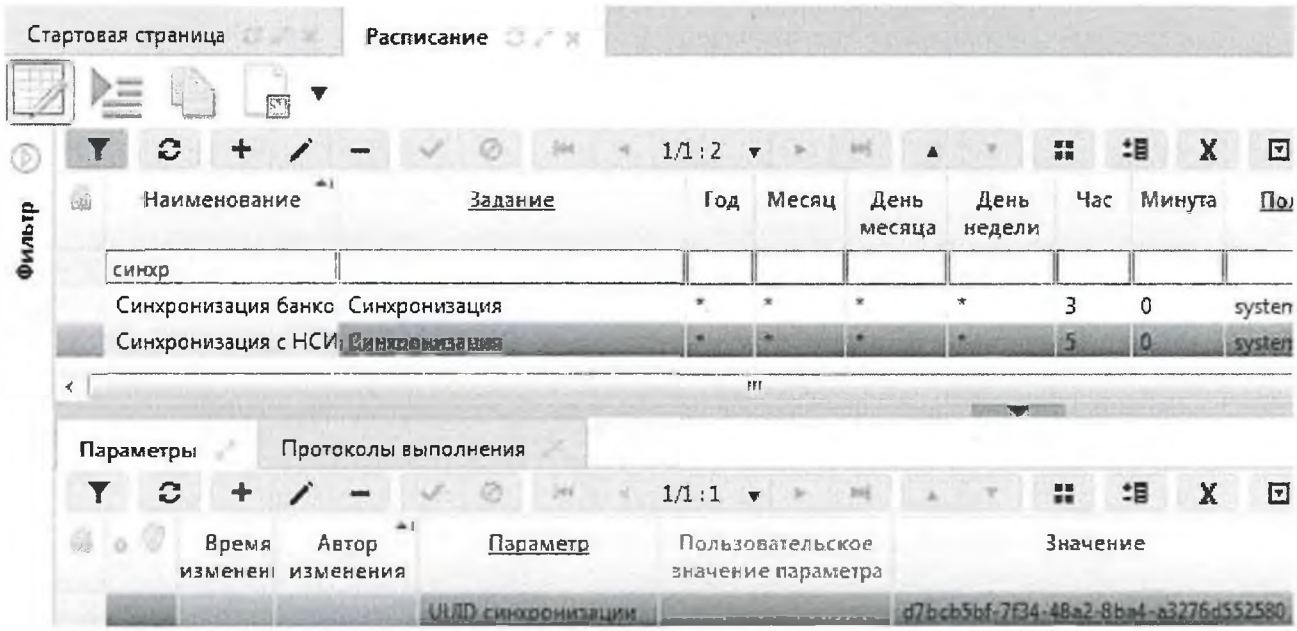


Рисунок 122 – Расписание для синхронизации с ПК «НСИ»

В предметных системах есть централизованное расписание, которое выполняется ежедневно ночью. Если необходимо более частое обновление, то администратор синхронизации может создать пользовательское расписание.

21.5. Диагностические инструменты администратора синхронизации для анализа ошибок синхронизации

21.5.1. Анализ полного протокола

Протокол загрузки доступен на интерфейсе «Сеансы синхронизации». В детализации для каждого завершившегося с ошибками сеанса представлен список ошибочных описаний с протоколами их загрузки. Соответственно можно посмотреть протокол обработки конкретного экземпляра. Пример протокола обработки конкретного экземпляра представлен на рисунке 123.

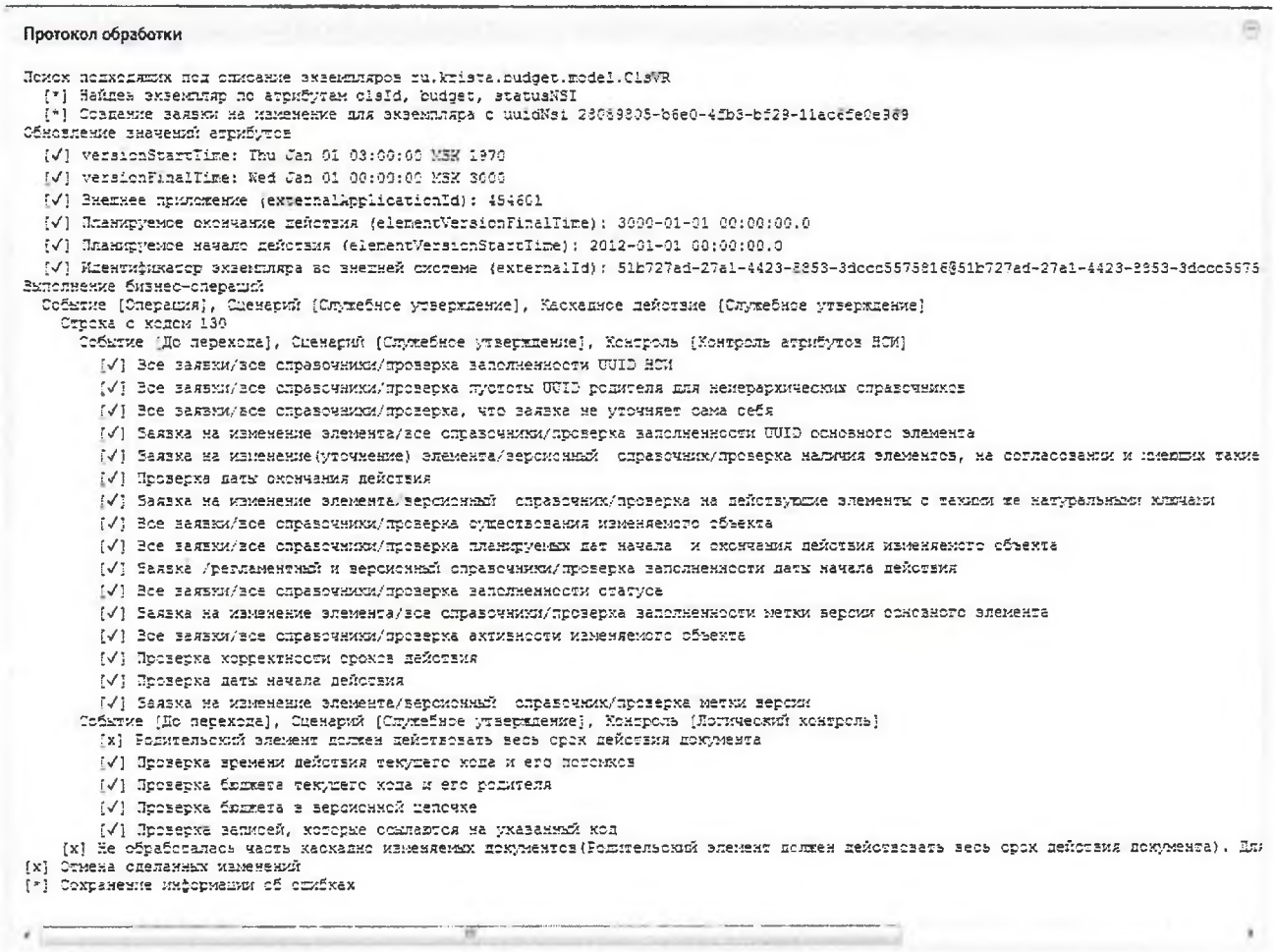


Рисунок 123 – Протокол обработки конкретного экземпляра сущности

В примере, представленном на рисунке 123, видно, что сначала шло все успешно. Потом началось выполнение бизнес-операций, а в рамках них контроль и одно из условий этого контроля выдало ошибку и такой экземпляр не удалось добавить.

В перечне ошибок можно увидеть только протоколы по конкретным ошибкам.

Если нажать на ⚠ в статусе сеанса синхронизации, то в новом окне браузера откроется полный протокол синхронизации, в котором будет уже полная информация, в том числе к какому источнику обращались, какой запрос делали. И здесь есть протоколы обработки абсолютно всех полученных данных. Эти протоколы достаточно громоздкие и открывать их в браузере не всегда целесообразно. При анализе протокола администратору синхронизации следует правой кнопкой кликнуть по иконке статуса и выбрать «saveLinkas...», сохранить протокол локально на жестком диске и потом с ним работать.

Полный протокол полезен, когда нужно узнать, а обрабатывался ли вообще конкретный экземпляр, а приходили ли эти данные в систему. Так как бывают ситуации, что синхронизация прошла успешно, а изменений в системе не произошло. Тогда используется полный протокол, в котором есть возможность посмотреть приходил ли конкретный экземпляр и сделать выводы.
Может экземпляр приходил, но в нем никакие атрибуты не изменились.

В протоколе отображаются только те атрибуты, которые были изменены. То есть синхронизатор меняет только те атрибуты, которые необходимо поменять. Это необходимо для того, чтобы лишний раз не запускать бизнес-операции. Если пришел объект, который не изменился, то синхронизатор его обработал, а бизнес-операции не выполнялись, так как никакие атрибуты не изменились. Таким образом, бизнес-операция выполняется только над измененными или новыми атрибутами.

Также полный протокол используется, когда при обработке одного экземпляра есть ссылка на обработку другого экземпляра. Ссылка идет по номеру задания. То есть ошибка случилась раньше обработки текущего кода: при обработке более ранних экземпляров, которые могут быть связаны с текущим. Для таких случаев тоже полезен полный протокол, чтобы понять, что же происходило.

21.5.2. Быстрый переход во внешнюю систему к ошибочным данным

Рассмотрим другой инструмент анализа ошибок.

Например, синхронизируется справочник «ЦСР». При загрузке одного экземпляра бизнес-операция выполнилась с ошибкой «Некорректный бюджет». Администратору синхронизации необходимо выяснить причину этой ошибки. Почему в ПК «НСИ» указан именно такой бюджет у этого экземпляра. Для этого необходимо перейти в ПК «НСИ» и проанализировать данные там. Для этого есть специальная кнопка НСИ в детализации интерфейсе «Сеансы синхронизации», которая доступна только в том случае, если администратор синхронизации вошел в систему под единой учетной записью.

Выделив запись конкретной ошибки, есть возможность перейти к этой записи в ПК «НСИ». В ПК «НСИ» можно понять, в чем проблема, исправить данные и потом повторно запустить синхронизацию.

21.6. Настройка прав на синхронизацию

21.6.1. Основная настройка прав

Настройка прав входит в компетенцию администратора синхронизации.

При настройке синхронизации, сначала настраивается на интерфейсе «Справочник внешних систем» подключение к внешней системе. При этом в поле «Параметры запроса» задается логин/пароль учетной записи, под которой будет осуществляться вход во внешнюю систему, как показано на рисунке 124.

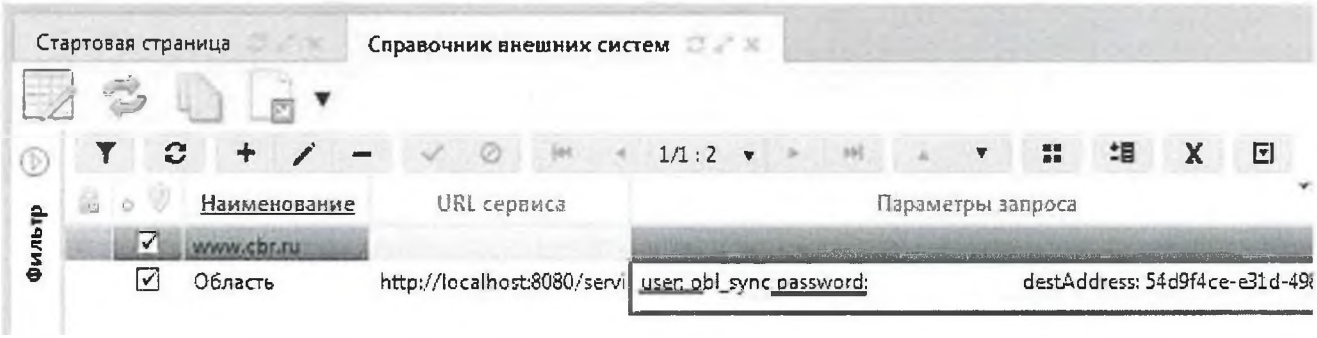


Рисунок 124 – Параметры запроса к внешней системе

Перед тем как указать логин/пароль в параметрах внешней системы необходимо завести соответствующую учетную запись в ПК «НСИ». Рассмотрим, как в ПК «НСИ» лучше заводить такие учетные записи.

Учетная запись должна иметь минимально необходимые права для синхронизации справочников, то есть права должны быть только на чтение.

Права настраиваются во всех системах, основанных на web-решениях, с помощью интерфейса «Права на видимость» группы «Права» РМ «Администрирование», как показано на рисунке 125.

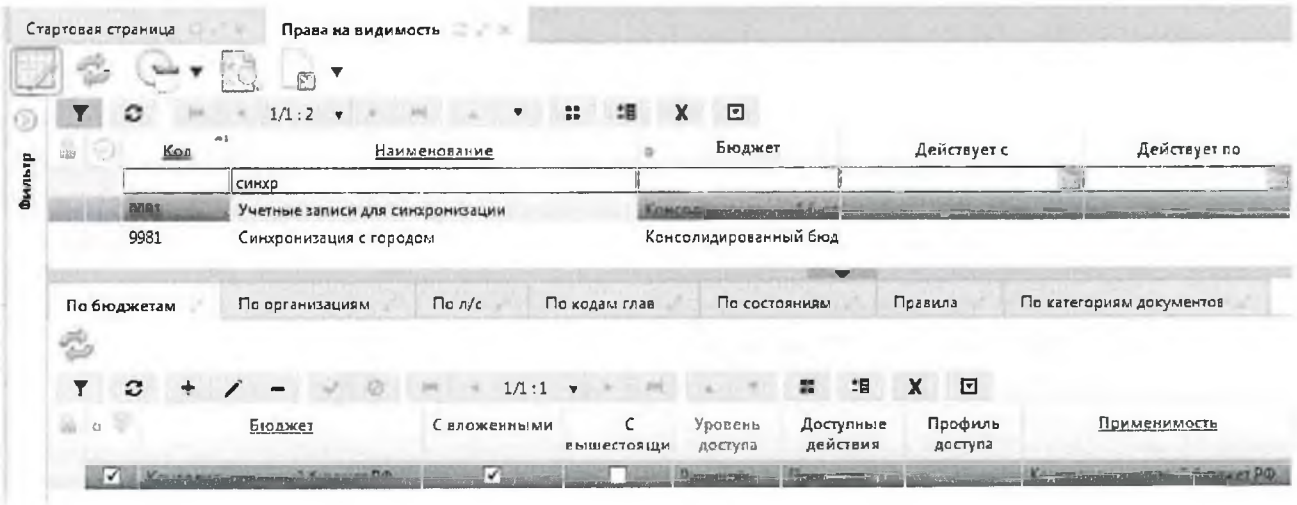


Рисунок 125 – Внешний вид интерфейса «Права на видимость»

В ПК «НСИ» администратор синхронизации может создать учетную запись и настроить на нее как полные права, так и ограниченные.

Под полными правами понимаются права на все бюджеты. В ряде случаев требуются права не на все бюджеты, а только на часть или права на часть справочников на полную закачку, а на часть справочников на частичную закачку.

Важно! Поле «Доступные действия» заполняется всегда значением «Просмотр». Никогда для учетных записей для синхронизации не назначаются права на ввод или согласование. На всех закладках должен быть только «Просмотр». То есть создается учетная запись с минимальными правами на чтение.

21.6.2. Дополнительные параметры настройки прав

Рассмотрим ситуации, когда требуются дополнительные настройки прав. Например, необходимо синхронизировать не все учреждения, а только ГРБС. Или нужно синхронизировать только учреждения субъекта или только учреждения определенных МО, если предметная система охватывает не все бюджеты субъекта.

Замечание! Для каждой предметной системы, которая синхронизируется с ПК «НСИ», нужно делать отдельную учетную запись.

21.6.2.1. Особенности выдачи прав на бюджеты

Рассмотрим ситуацию, когда нужно настроить права на синхронизацию справочников по конкретным бюджетам.

В этом случае на интерфейсе «Права на видимость» для учетной записи для синхронизации в детализации «По бюджетам» добавляется необходимый бюджет, как показано на рисунке 126.

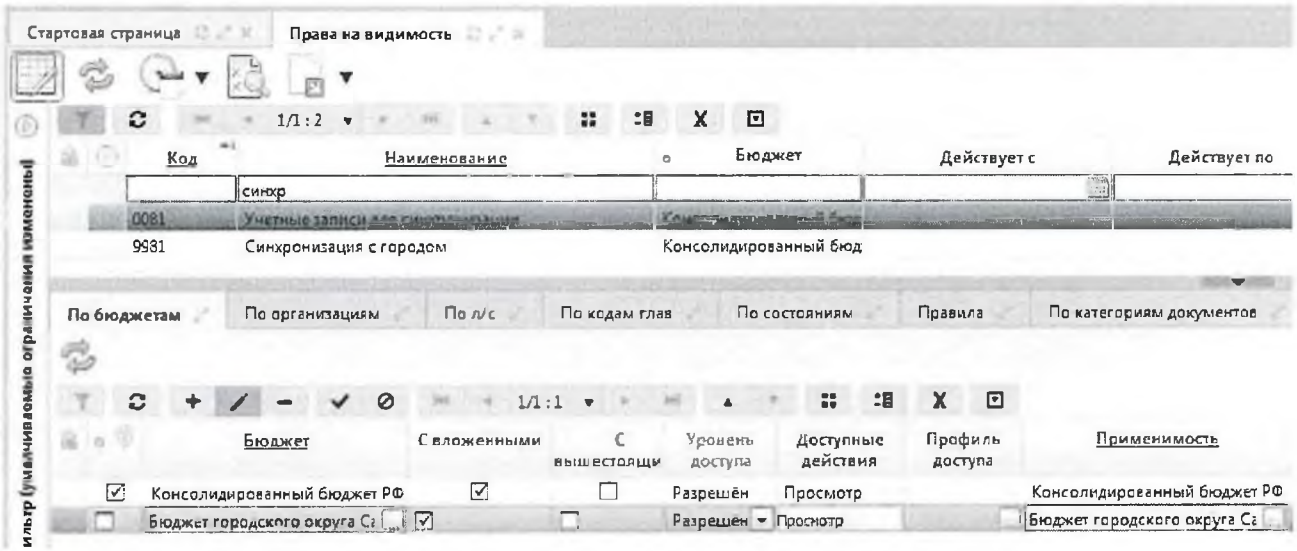


Рисунок 126 – Добавление бюджета в права на видимость

При необходимости ставится галка «с вложенными», чтобы можно было задавать права на консолидированный бюджет и все нижестоящие. На этом настройка прав заканчивается.

После настройки необходимо нажать кнопку «Обновить права на документы».

21.6.2.2. Особенности выдачи прав на учреждения

Другой случай, когда нам нужно настроить права на справочник «Учреждения (ОВ)», и соответственно на справочники «Сотрудники», «Счета». В справочнике учреждений особенность заключается в модели. Здесь могут быть как бюджетные учреждения, так и контрагенты, юридические лица, то есть не обязательно учреждения бюджетной сферы. Поэтому в модели у учреждений нет привязки к бюджету на базовом классе. Привязка к бюджету появляется у классов наследников, которые наследуются от базового класса учреждений.

Когда администратор задает права, он работает не с классом наследником, а с базовым классом и по учреждению автоматически не подхватываются права, если просто задать права на бюджет.

В случае, когда надо настроить права на учреждения определенных бюджетов, и не нужно получать учреждения других бюджетов, тогда на закладке «По организациям» детализации интерфейса «Права на видимость», необходимо завести новую запись и у нее указать «бюджет учреждения», как показано на рисунке 127. Если необходимо синхронизировать несколько бюджетов, то нужно добавить запись на каждый бюджет.

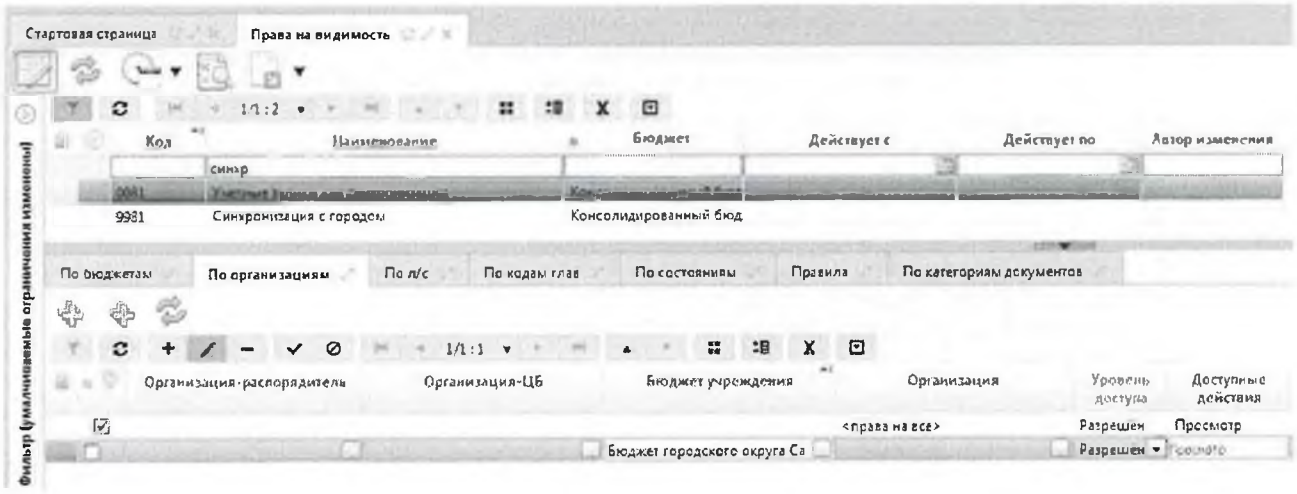


Рисунок 127 – Добавление бюджета организации в права на видимость

После сохранения, необходимо нажать кнопку «Обновить права на документы».

В результате система будет автоматически отфильтровывать учреждения, и оставлять учреждения только нужных бюджетов. Цель достигнута - будут синхронизироваться только организации нужных бюджетов. Вместе с учреждениями будут синхронизироваться и все зависимые сущности: сотрудники, счета и так далее.

Остальные закладки для настройки прав синхронизации обычно не используются.

21.6.2.3. Поддержка нескольких учетных записей подключения к ПК «НСИ»

Пример. Допустим, необходимо одни справочники синхронизировать целиком, а другие только в части определенных бюджетов. Например, есть задача, что классификация требуется для всех бюджетов, в том числе и для бюджетов МО, а учреждения требуются не все, а только ГРБС и ФО. Для того, чтобы не синхронизировать большой объем не используемых учреждений, необходимо ограничить синхронизацию, например, по ГРБС и ФО.

Такой вариант поведения тоже настраивается. Раньше такая ситуация решалась с помощью добавления нескольких внешних систем, но это оказалось не очень хорошим решением.

Сейчас подобные варианты использования настраиваются в рамках одной внешней системы - ПК «НСИ», но создается несколько учетных записей для синхронизации. Одна учетная запись делается для синхронизации справочников всех бюджетов, кроме справочников учреждений и сотрудников. Другая учетная запись делается для синхронизации справочников учреждений и сотрудников, и для этой учетной записи настраиваются права так, чтобы выбирались только учреждения, являющиеся ГРБС и ФО.

В детализации «Перечень доступных справочников» интерфейса «Справочник внешних подсистем» у каждого справочника есть возможность перекрытия параметров запроса. То есть можно взять запрос из поля «Параметры запроса» нужной внешней системы, скопировать его в справочник, в рассматриваемом случае «Учреждения (ОВ)», и затем отредактировать его, указав логин и пароль второй учетной записи, как показано на рисунке 128.

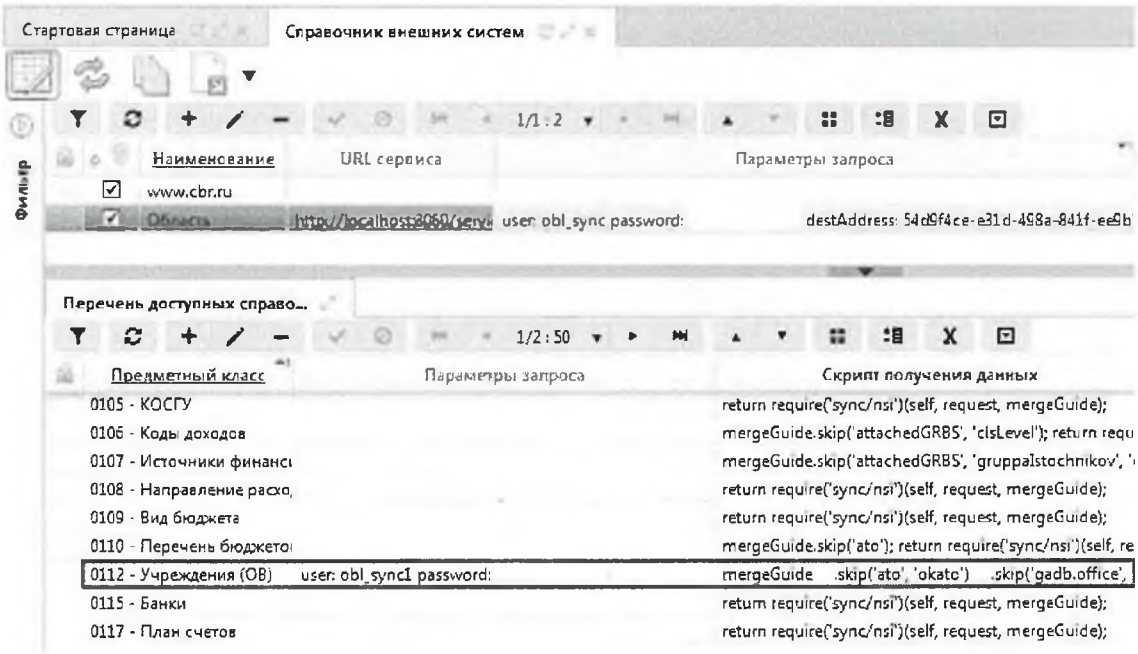


Рисунок 128 – Перекрытие параметров запроса

В этом случае синхронизатор, когда будет синхронизировать справочник «Учреждения (ОВ)», то для всех справочников, у которых параметры запроса не перекрываются, будет брать единые параметры запроса. А для тех справочников, у которых перекрыты параметры, возьмет параметры, указанные в параметрах запроса справочника, в частности другую учетную запись. Соответственно, справочник «Учреждения (ОВ)» синхронизируется уже с правами другой учетной записи.

21.6.2.4. Особенность ограничения прав

Есть особенность по ограничению прав учетных записей ПК «НСИ»: в том случае, если запрашиваются полные данные, то работает ограничение по правам. Если запрашиваются данные по идентификатору, то ограничений по правам не происходит. Реализовано это для разрешения

ссылок, когда из синхронизируемого экземпляра, на который у учетной записи есть права есть ссылка на справочник, права на который у учетной записи отсутствуют.

Такие ссылки система тоже умеет разрешать. Она сделает запрос по идентификатору, ПК «НСИ» по этому идентификатору возвратит значение, даже если на него нет прав.

22. Редактор внутридокументных контролей

Внутри документные контроли (далее – ВДК) работают с атрибутами документа. Их цель – определить правильно ли введен документ пользователем или неправильно. ВДК, как правило, работает только с одним текущим проверяемым документом. Междокументные контроли (далее – МДК) в отличие от ВДК работают с остатками. Они анализируют не только текущий документ, но и другие документы.

Основной интерфейс, который использует администратор для настройки ВДК, называется «Внутридокументные контроли», представлен на рисунке 129.

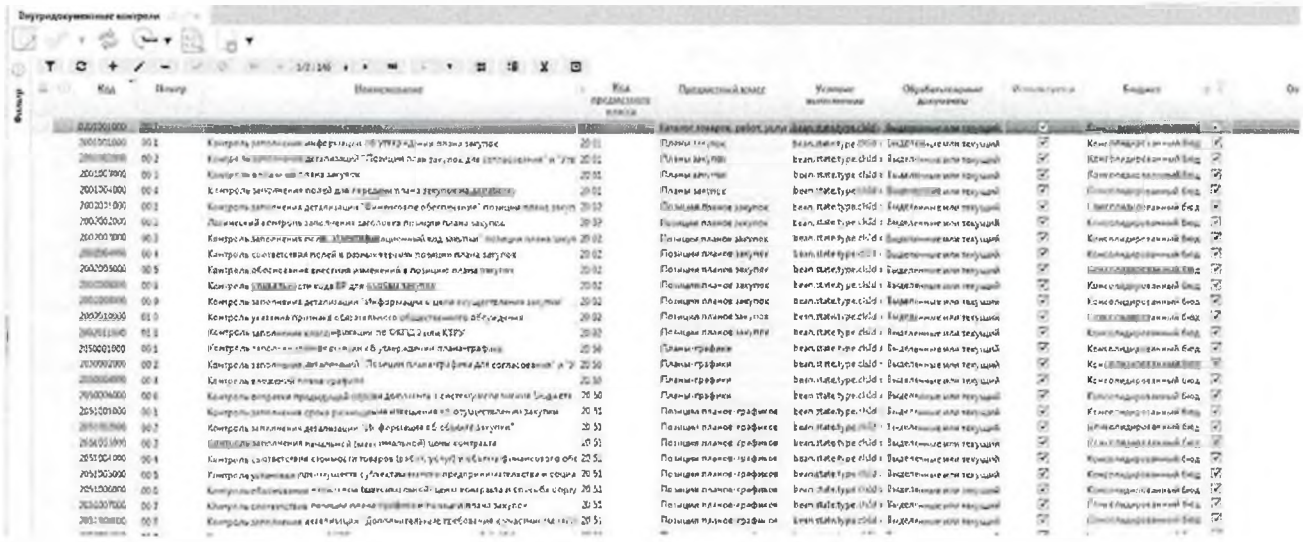


Рисунок 129 – Интерфейс «Внутридокументные контроли»

Назначение основных полей в заголовке интерфейса «Внутридокументные контроли» приведено в таблице 7. Назначение остальных полей такое же как на других интерфейсах.

Таблица 7 - Назначение основных полей в интерфейсе «Внутридокументные контроли»

Поле	Назначение
Наименование	Наименование контроля, которое отображается в документах. Все ВДК называются, как правило, одинаково, потому что редко бывает больше 1 контроля на первичный документ. Стандартным считается значение «Логический контроль».
Обрабатываемые документы	Настройка возможности выполнения контроля по выделенным или всем документам. Возможные значения: «Выделенные или текущий», «Все доступные»

Поле	Назначение
Используется	Включение/отключение контроля для всего сервера в целом (глобальная настройка). Кроме этого, есть более тонкая настройка, когда присутствует несколько бюджетов и необходимо для каждого бюджета сделать свою настройку использования/неиспользования контроля

Рассмотрим атрибут «Обрабатываемые документы». Значение «Выделенные или текущий» означает, что контроль будет срабатывать только для текущей записи или для выделенных записей, показано на рисунке 130.

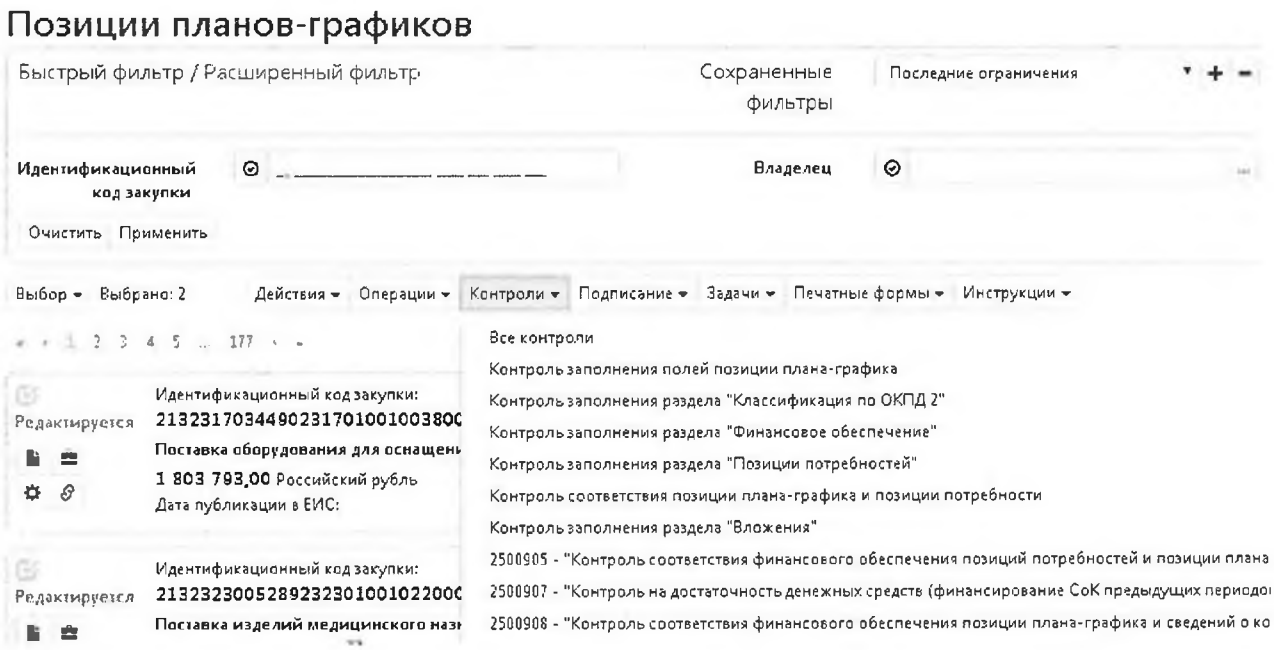


Рисунок 130 – Выделение записей в интерфейсе «Позиции планов-графиков» перед выполнением контроля

В ряде случаев требуется проверять не только текущий или выделенные документы, а вообще все документы. Чаще всего это требуется на справочниках, например, ЦСР. Выделять большое количество строк или проверять по частям неудобно. Поэтому для таких случаев предназначено значение «Все доступные» атрибута «Обрабатываемые документы». В этом случае пользователь может выполнить контроль для текущего или выделенных документов, а также дополнительно сможет выполнить контроль для всех документов, заведенных на предметном классе. В интерфейсе предметного класса в выпадающем меню действия «Проверить документы» появится новый пункт «Проверить все доступные документы», показано на рисунке 131.

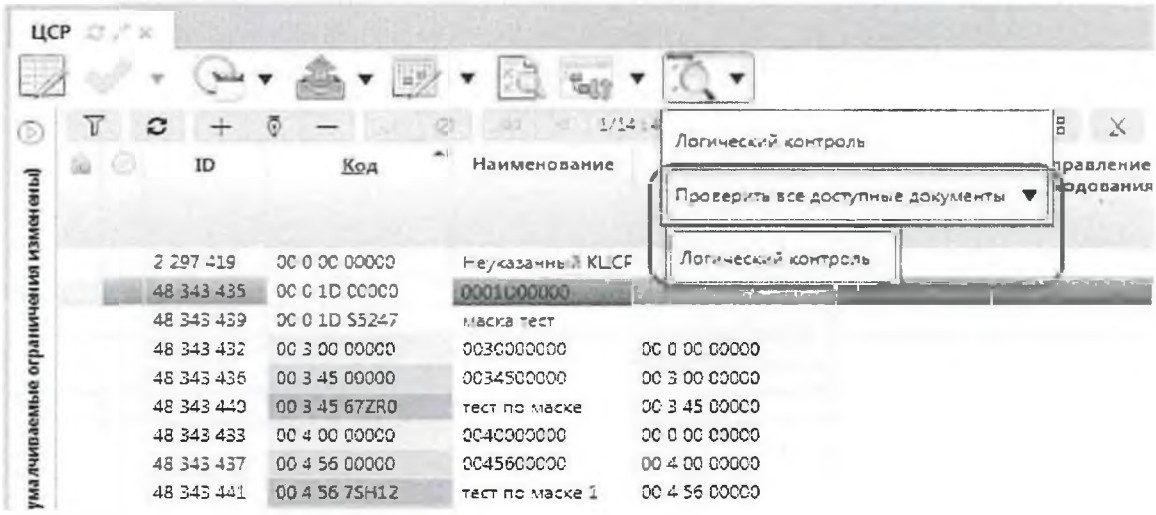


Рисунок 131– Контроль со значением «Все доступные» для интерфейса «ЦСР»

Администратор, в основном, работает в детализации интерфейса «Внутридокументные контроли», представлено на рисунке 132, именно в ней определяется наполнение ВДК декларативными правилами. Добавление правил в ВДК производится по кнопке + «Добавить запись» или по кнопке «Добавить проверки» (добавление сразу нескольких декларативных правил). Особенностью кнопки «Добавить проверки» является то, что для выбора отображаются правила, которых нет в контроле и которые могут быть добавлены в текущий предметный класс.

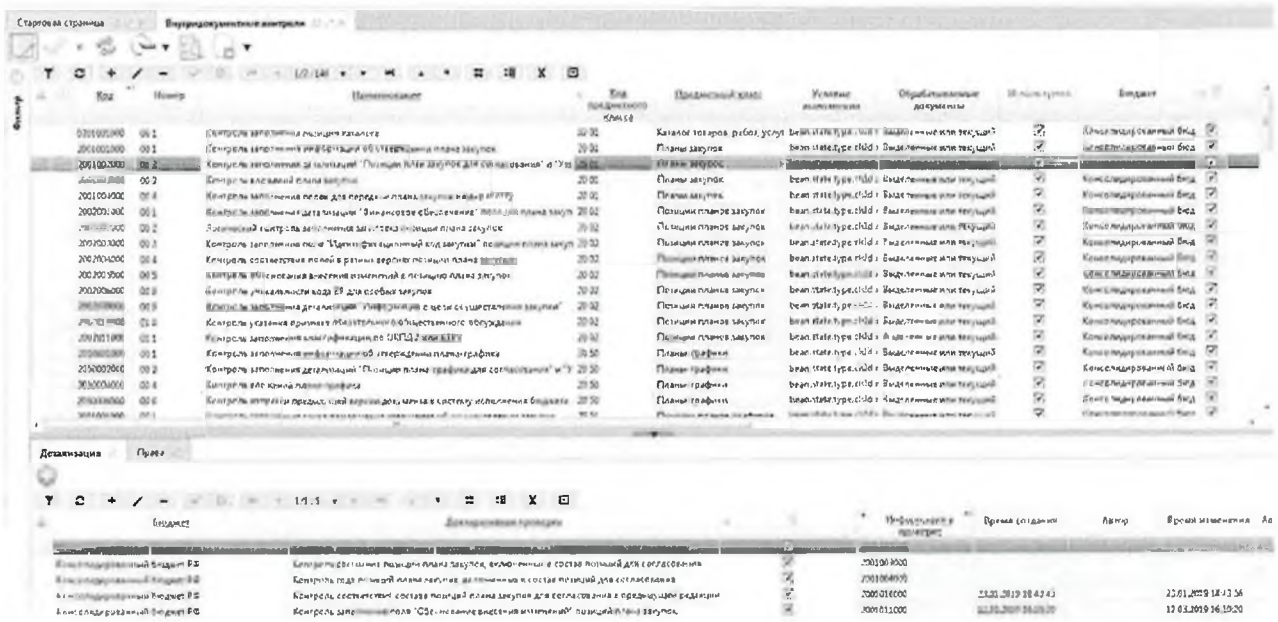


Рисунок 132 – Детализация интерфейса «Внутридокументные контроли»

Региональный администратор может создать новое правило, отсутствующее в стандартной поставке. Это новое правило необходимо включить в ВДК. Существует два способа включения:

— способ 1 - создание нового регионального ВДК. Новое региональное правило включается в новый ВДК. Этот способ имеет ряд неудобств:
  — новый ВДК придется включать в бизнес-процесс;
  — пользователь будет видеть несколько пунктов при выборе контролей (ВДК централизованный, ВДК региональный);
— способ 2 - добавление нового правила в уже существующий централизованный ВДК, показано на рисунке 133. Этот вариант реализации является рекомендуемым. На региональных базах при добавлении регионального правила поле «Бюджет» будет заполнено значением регионального бюджета. Система при выполнении ВДК производит фильтрацию правил. Если пользователь относится к определенному бюджету, то для него будут выполняться централизованные и региональные правила, относящиеся к его бюджету. При таком варианте реализации пользователь не увидит изменений в системе (останется всего один централизованный контроль), дополнительных подключений в бизнес-процесс не потребуется.

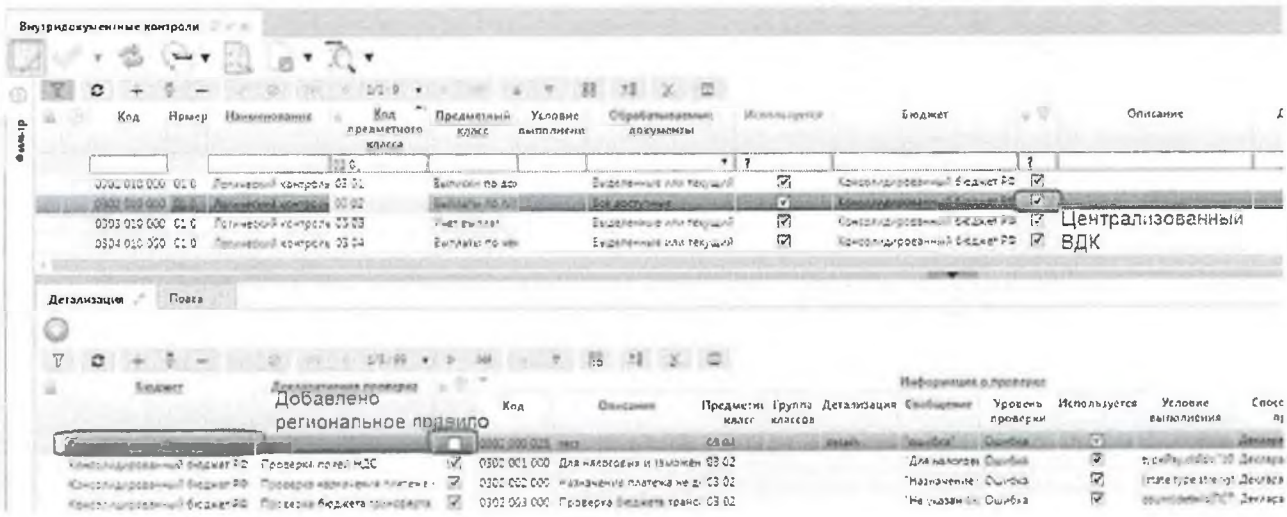


Рисунок 133 – Пример добавления регионального правила в централизованный контроль

23. Декларативные правила

23.1. Типы правил

Создание новых региональных правил для контролей, а также их редактирование производится в интерфейсе «Декларативные правила», представлено на рисунке 134.

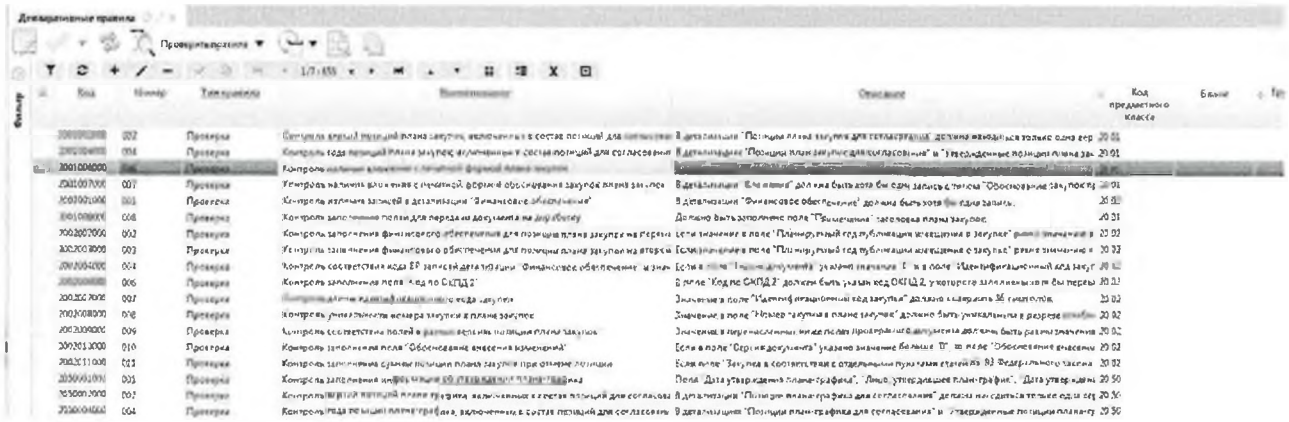


Рисунок 134 – Интерфейс «Декларативные правила»

В таблице 8 приведены значения для атрибута «Тип правила».

Таблица 8 - Значения атрибута «Тип правила»

Значение	Назначение
Проверка	Проверка атрибута документа на правильность выполнения какого-либо логического выражения
Фильтр	В случае, если необходимо работать с атрибутом, являющимся справочником, и в случае, если пользователь может выбирать из этого справочника не все значения, а только определенные, то возникает задача фильтрации справочника. Например, в документе нужно для КУ выбирать лицевые счета КУ, а лицевые счета АУ и БУ отфильтровывать. Администратору в таком случае необходимо написать декларативное правило с типом «Фильтр». Правило с типом «Фильтр» будет применяться **к каждой строке** справочника. Например, если в справочнике 100 лицевых счетов, то правило фильтрации будет последовательно выполняться для каждой строки. Если правило фильтрации не выполняется, то такая строка будет исключена из выбора. Если правило фильтрации выполняется, то строка будет оставлена пользователю для возможности выбора.

Значение	Назначение
Проверка + Фильтр	на практике часто возникают случаи, когда описанное правило фильтрации удобно использовать и для проверки, потому что пользователь не только выбирает значение из справочника, но и может его ввести вручную с клавиатуры, скопировать и т.д. Поэтому, чтобы одну и ту же логику не писать дважды как фильтр и как проверку, удобно использовать тип «Проверка + Фильтр»

23.2. Фильтры. Особенности задания

При работе с правилами фильтрации дополнительно в поле «Атрибут для фильтра» должен быть указан тот справочник, который требует фильтрации, представлено на рисунке 135.

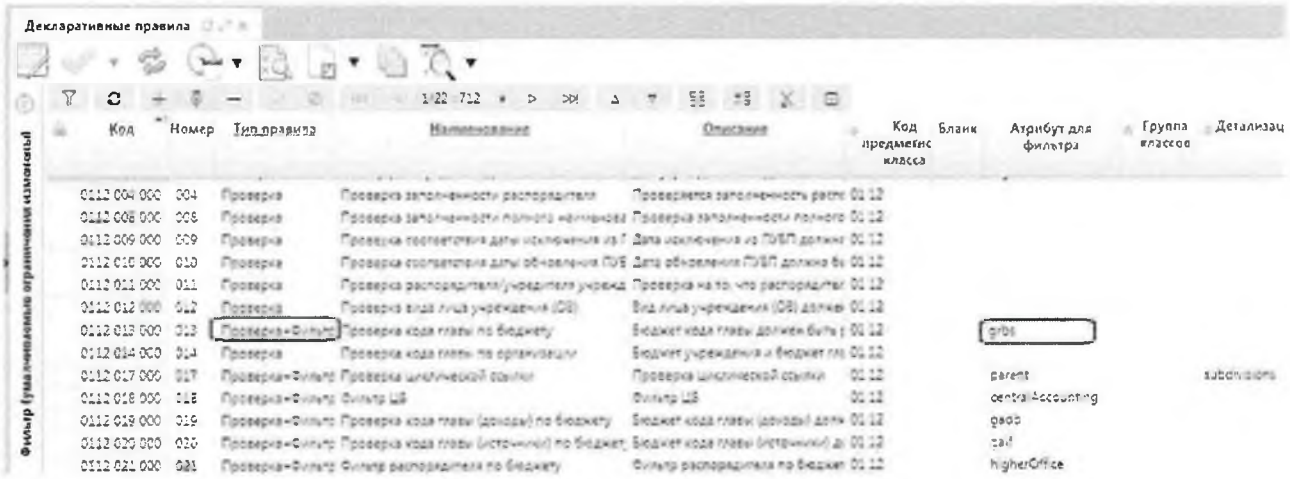


Рисунок 135 – Пример заполнения «Атрибут для фильтра» для правила фильтрации

Если пользователь не указывает никакого значения (особенно при типе «Проверка+Фильтр»), то система автоматически считает разрешенными пустые значения. То есть, администратору нет необходимости в «Условии выполнения» дополнительно писать: «если условие не пустое».

По сравнению с правилами проверки, правила фильтрации несколько сложнее. Правило проверки на одну строку выполняется всего 1 раз, а правило фильтрации – столько, сколько строк в справочнике.

23.3. Понятие контекста

В ряде случаев необходимо явно указывать, к атрибуту какой сущности идет обращение: к атрибуту проверяемого документа или к экземпляру справочника. Как правило, система находит нужный атрибут по имени. Но бывают случаи, когда имя не уникально и может возникнуть коллизия. Для решения таких ситуаций предназначено понятие «контекста». В декларативных правилах есть несколько доступных контекстов, которые администратор может использовать.

Существует два контекста: «bean»–это дефолтный контекст (контекст по умолчанию) и «ownerbean» – это контекст документа. В правиле фильтрации для справочника «bean» это экземпляр справочника, а доступ к экземпляру проверяемого документа мы можем получить через «ownerbean».

Пример: «bean.higherAccount». Здесь используется обращение к атрибуту через контекст. В данном случае используется зарезервированное слово «bean», которое означает, что работаем с текущей записью.

Есть еще один контекст «global». Подробнее о нем в пункте 23.12 «Оптимизация декларативных правил».

23.4. Правила на класс и на группы классов

В интерфейсе «Декларативные правила» есть атрибуты «Код предметного класса» и «Группа классов».

Атрибут «Код предметного класса» указывает, что правило предназначено для конкретного класса.

В ситуациях, когда у нескольких предметных классов есть одинаковые атрибуты, которые проверяются по одним и тем же правилам, для того, чтобы одно правило не описывать несколько раз используется поле «Группа классов». Одно правило может быть использовано на всех предметных классах, входящих в группу. Например, группа классов «Лицевые счета» содержит 3 класса. В хинте (когда наводишь курсор на кнопку или на поле появляется всплывающая подсказка) отображаются конкретные классы, которые входят в данную группу, показано на рисунке 136. В группе «Классификаторы» число входящих классов 107, то есть одно правило может быть использовано для 107 справочников. При этом, если администратор создает правило на группу классов, то он берет на себя ответственность, что во всех классах будут присутствовать нужные атрибуты.

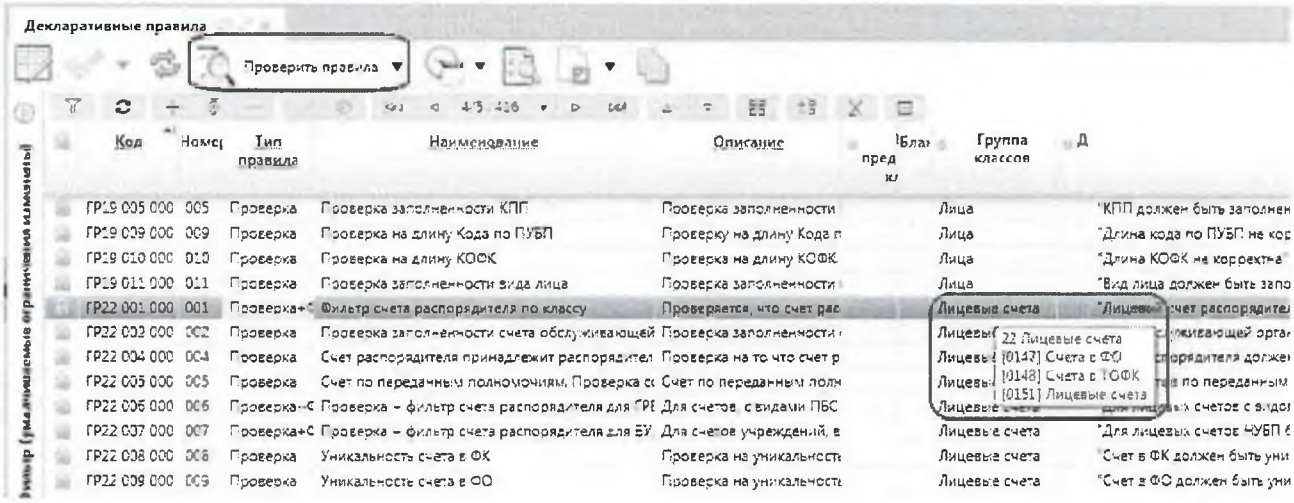


Рисунок 136 – Пример использования группы классов «Лицевые счета»

В интерфейсе «Декларативные правила» существует возможность проверки правил по кнопке 

«Проверить правила». При этом проверяется соответствие атрибутного состава у классов группы.

23.5. Уровень проверки

У атрибута «Уровень проверки» предусмотрены два уровня проверки: «Ошибка» и «Предупреждение», описаны в таблице 9.

Таблица 9 - Назначение уровней проверки

Уровень проверки	Цвет индикатора	Назначение
«Ошибка»	Красный	Жесткий контроль. Документ не переходит в следующее состояние, действия над документом не совершаются
«Предупреждение»	Оранжевый	Мягкий контроль. Документ переходит в новое состояние, пользователю выводится сообщение, что проверка прошла с предупреждением

На рисунке 137 показаны оба уровня проверки.

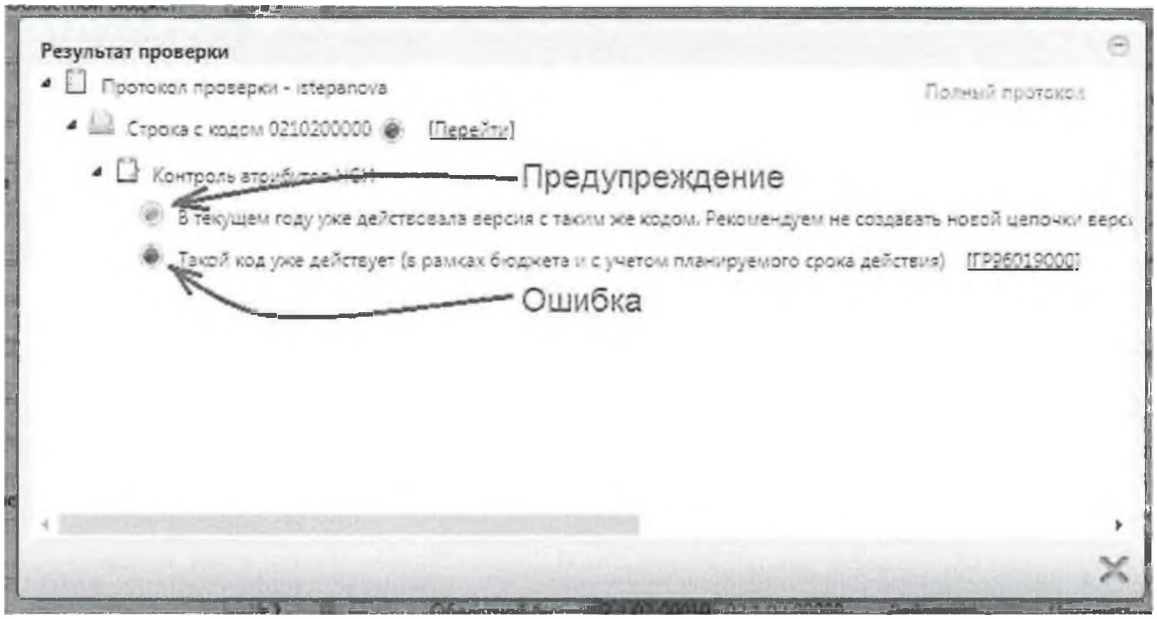


Рисунок 137 – Протокол контроля

Администратор может гибко использовать уровень проверки. Если какое-то правило контроля надо отключить, то предпочтительным является способ, когда не просто выключается правило контроля, а оно делается предупреждением. Например, если в платежном поручении требуется использование ЭП, но в ряде случаев допускается использование визы (например, когда учреждение приносит нам печатную версию, подписанную обычной подписью). Требование использования ЭП в контроле отключать не надо, необходимо понизить уровень проверки с уровня «ошибка» на уровень «предупреждение». В этом случае оператор будет видеть предупреждение, что ЭП не использовалась при заверении документа. Он сможет обработать этот документ, но должен проверить наличие платежки подписанной обычной подписью.

23.6. Права на выполнение правил

Рассмотрим, как администратор контролей может понизить уровень проверки контроля или отключить правило.

Отключение контроля доступно только глобальному администратору системы (system). Администраторам, имеющим меньшие права, эта возможность недоступна. У правила, выполнение которого не требуется, необходимо снять галку в поле «Используется». Для всех пользователей региона, независимо от бюджета, это правило перестанет выполняться. Способ не очень хороший. Он может использоваться при начальной настройке в регионе.

Когда система уже полноценно работает в регионе, лучше использовать механизм прав. Это гибкий механизм.

По умолчанию считается, что права на декларативные правила определяются в заголовке декларативного правила. Если стоит галочка «Используется» и проставлен уровень проверки «Ошибка», то считается, что на это декларативное правило есть право на использование и на уровень проверки «Ошибка», и на уровень проверки «Предупреждение» (так как уровень проверки «Ошибка» выше уровня проверки «Предупреждение», то при выполнении этого правила система выдаст ошибку).

Если уровень проверки установлен «Предупреждение», то система считает, что по умолчанию права на уровень «Ошибка» нет, есть только право на уровень проверки «Предупреждение».

Это дефолтное право может быть перекрыто. Причем оно может быть перекрыто для определенной группы пользователей определенного бюджета. Это делается в детализации «Права». Наиболее часто права перекрываются для всех сотрудников (указывается группа «Все сотрудники»). Но это необязательно. При необходимости можно указать конкретную группу пользователей.

Важный атрибут «Бюджет документа». Частая задача – это отключение правила не для всех, а для какого-то конкретного бюджета, либо для какой-то группы бюджетов. Например, правило должно работать для субъекта и не должно работать для муниципальных образований (или наоборот). Или для какого-то конкретного МО работать не должно, а для всех остальных должно. В таких случаях в поле «Бюджет документа» указывается конкретный бюджет или группа бюджетов (консолидированный бюджет).

На рисунке 138показан пример, где правило отключено для всех сотрудников определенного бюджета. В поле «Группа» указано «Все пользователи», в поле «Бюджет документа» – конкретный бюджет, в «Уровень доступа» – «Запрещен». В поле «Уровень проверки»: если поле пустое, то запрет будет распространяться и на «Ошибку», и на «Проверку», то есть для всех сотрудников выбранного бюджета это правило не выполнится ни с каким уровнем.

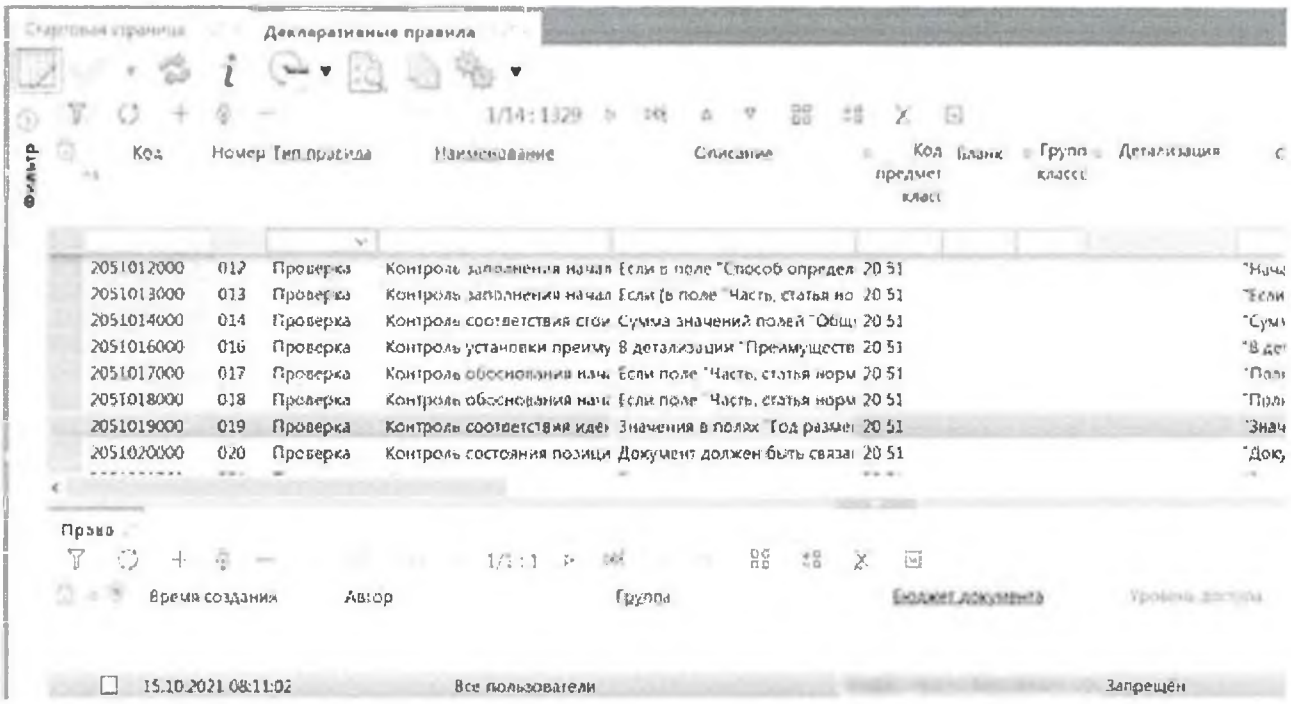


Рисунок 138 – Пример отключения правила для определенного бюджета

Если требуется для всех сотрудников отдельного бюджета перевести правило из ошибки в предупреждение, то надо установить запрет только для ошибки (поле «Уровень проверки» равно «Ошибка»). В этом случае уровень проверки «Ошибка» будет запрещен, а уровень проверки «Предупреждение» останется, потому что дефолтные права давались на оба уровня.

Можно по-другому перевести правило для всех сотрудников определенного бюджета из уровня проверки «Ошибка» в уровень проверки «Предупреждение», как представлено на рисунке сначала сделать запрет и для «Ошибки», и для «Предупреждения», а потом добавить новую запись с уровнем доступа «Эксклюзивный» для уровня проверки «Предупреждение».

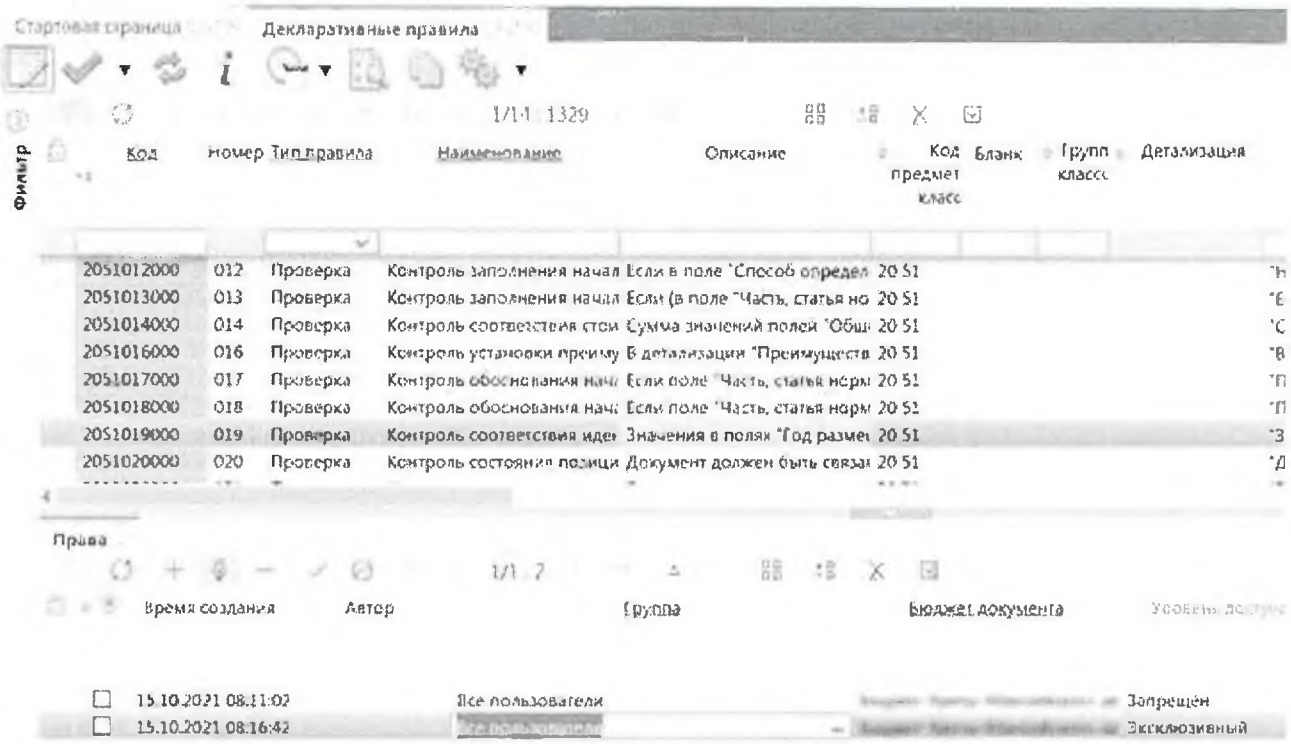


Рисунок 139 – Пример перевода правила из ошибки в предупреждение для определенного бюджета

23.7. Бюджет документа

Что такое атрибут «Бюджет документа»? Раньше бюджет рассчитывался так: брался бюджет текущего пользователя. Если сотрудник работает в организации, у этой организации смотрели бюджет, и по этому бюджету делали фильтрацию прав. У этого способа были недостатки. Например, учетная запись администратора, который не привязывается ни к одному из бюджетов. Так как если администратор работает со многими бюджетами, то нет смысла его привязывать к какому-то конкретному бюджету. Кроме этого, есть технологические учетные записи для синхронизации, которые тоже не относятся ни к одному бюджету, так как не привязаны ни к сотруднику, ни к организации. В результате у таких учетных записей нет возможности определить бюджет и раньше по таким учетным записям выполнялись все контроли, то есть для них мы не могли отключить контроли с помощью механизма прав. Это было не удобно. Администратор отключил правило и контроль для пользователя. Для пользователя все работает – правило и контроль отключены, но сам администратор отключения контролей не видит.

23.8. Запрет изменения прав

Существует несколько уровней администраторов: глобальный администратор, локальные администраторы конкретных бюджетов.

Глобальный администратор может настроить правило, которое не должно быть отключено локальными администраторами. Для этого в поле заголовка «Запрет на изменение прав» нужно поставить галку, представлено на рисунке 140. При этом локальные администраторы не смогут на своем уровне изменить правила, настроенные вышестоящим администратором.

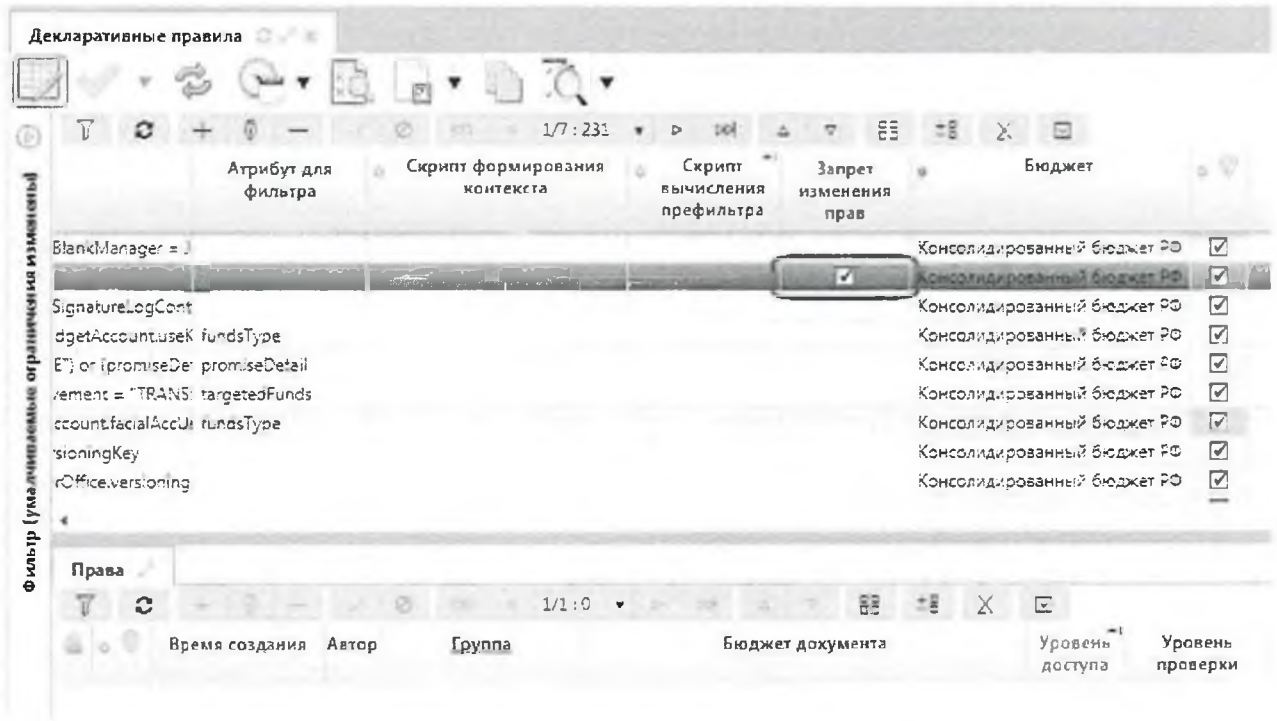


Рисунок 140 – Пример запрета изменения прав

Концепцию запрета изменения прав планируется развить. Сейчас, если стоит запрет на изменение прав, то права могут изменять только крайне ограниченное количество администраторов. Планируется расширить эти правила, чтобы изменения всегда мог вносить еще и автор правила. То есть автор правила всегда может снять запрет или изменить на него права. Если установлен запрет, и ты не автор правила, и не администратор соответствующего уровня, то права изменить не сможешь.

23.9. Область действия правила

Атрибут заголовка «Область действия» имеет значения: «Документ» и «Изменяемые атрибуты».

Если требуется проверить правильность ввода конкретного атрибута (например, в документе лицевой счет должен быть введен обязательно), то в этом случае область действия должна иметь значение «Изменяемые атрибуты». Для правил с такой областью действия система вызовет проверку раньше – уже в момент сохранения изменений. Если пользователь ввел неправильное значение, то получит ошибку сразу же при сохранении.

Если необходимо проверять не один атрибут, а набор атрибутов на соответствие значений друг другу (например, итоговая сумма в заголовке должна быть равна сумме всех строк детализации), то в этом случае нельзя задавать область действия «Изменяемые атрибуты». Потому что при завершении ввода одного связанного атрибута, значение другого может еще пользователем быть не введено, проверка не пройдет, и пользователь получит преждевременную ошибку. Для таких случаев используется область действия «Документ».

В этом случае система не вызывает проверку на сохранение значения, эта проверка будет выполнена позже. Проверки с областью действия «Документ», как правило, вызываются уже из бизнес-процессов или при явном вызове ВДК по кнопке «Контроли». При вызове контролей по кнопке «Контроли» выполняются правила и с областью действия «Изменяемые атрибуты», и с областью действия «Документ».

Проверки с областью действия «Изменяемый атрибут» требуют более простого конфигурирования. Если декларативное правило не включить в ВДК, то оно все равно выполнится. Если забыть включить в ВДК декларативное правило с областью действия «Документ», то оно может не выполниться никогда (оно может быть выполнено, если его явно прописать в сценарий обработки). Поэтому важно не забывать включать декларативные правила с областью «Документ» в ВДК.

Декларативное правило с областью «Изменяемые атрибуты» так же рекомендуется включать в ВДК, т.к. лишний раз пройденная проверка на более поздних этапах может найти ошибку.

23.10. Способ задания правила, условие выполнения

В атрибуте «Правило» задается декларативное правило или JavaScript.Для этого в поле «Способ задания правила» необходимо указать соответствующее значение: «Декларативное правило» или «Код на JavaScript».

На практике, в большинстве случаев, синтаксиса декларативного правила достаточно для описания правила. Оно проще в написании и понимании, поэтому если декларативного правила достаточно, то разработчик использует синтаксис декларативного выражения.

Синтаксис JavaScript используется только в тех случаях, когда декларативным выражением задачу решить трудно или невозможно.

Кроме атрибута «Способ задания правила» важным является атрибут «Правило». Он содержит текст декларативного выражения или текст JavaScript.

Поле «Условие выполнения» предназначено для явного указания условий, при которых правило должно работать. Например, проверка, что расчетный счет для КУ и лицевой счет должен быть тоже КУ. Это пример условия выполнения: необходимо сначала проверить, что если расчетный счет казенный, то используем правило, что лицевой счет должен быть тоже казенным. Если расчетный счет не казенный, то правило, что лицевой счет должен быть казенным, выполняться не должно.

Условие выполнения не предполагает выбора способа задания правила. Условие выполнения всегда задается с помощью декларативных правил. В том случае, когда возможности декларативных правил не хватает, можно это условие выполнения перенести в тело правила.

Рекомендуется использовать условие выполнения тогда, когда это возможно. Для пользователя условие выполнения будет предпочтительней, т.к. система сразу просчитывает доступные и недоступные правила и в списке сразу не увидим контролей, которые не могут выполняться для текущего документа. Если не использовать условие выполнения, то пользователь выполнил бы контроль, который бы выдал результат, что данный контроль не применим к документу. Времени и сил было бы потрачено больше, а результат тот же.

Синтаксис декларативных правил подробно описан в предыдущих темах. Здесь рассмотрим вспомогательные опции, реализованные в редакторе декларативных правил

Редактор декларативных правил поддерживает «горячие клавиши» Ctrl + Space – доступ к атрибутному составу. Например, правило «Проверка на уникальность счета в банке». В условии выполнения в редакторе по Ctrl + Space показываются атрибуты класса «Счета в банке», представлено на рисунке 141.

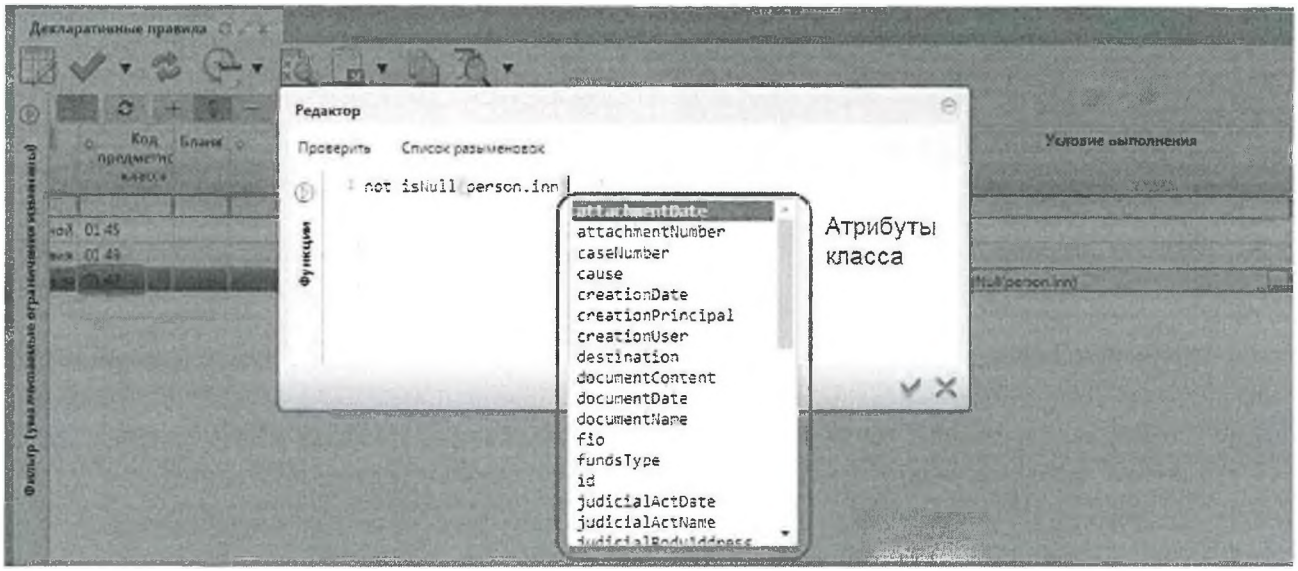


Рисунок 141 – Вызов в редакторе декларативных правил атрибутного состава по Ctrl + Space

Следующая опция, облегчающая работу, кнопка «Список разыменовок». Если по английскому имени сложно выбрать необходимый атрибут, то по кнопке «Список разыменовок» нажав «Показать тип» можно увидеть название атрибута, которое видно в названии колонки. По разыменовке можно легко выбрать необходимый атрибут, представлено на рисунке 142.

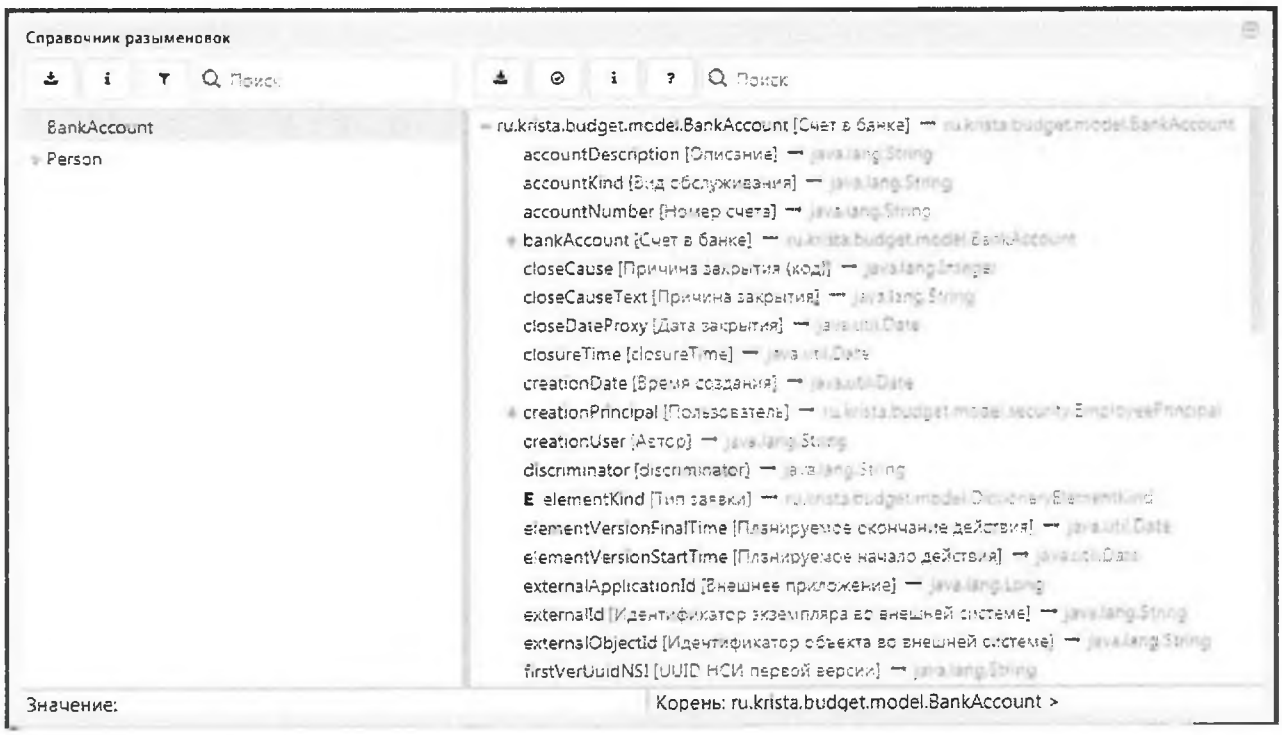


Рисунок 142 – Вызов в редакторе декларативных правил списка разыменовок

Кроме атрибутов, декларативные правила состоят из функций. Нотация декларативных правил очень похожа на нотацию формул, которая используется в Excel. Формула в Excel состоит из функций и параметров этой функции. Так же и в декларативном правиле. В качестве параметров могут выступать результаты других функций и атрибуты документа.

Полный список функций доступен в правой части редактора, представлено на рисунке 143. В списке функций доступен поиск по названию, описание функции и параметры функции, представлено на рисунке 144.

Рисунок 143– Вызов в редакторе декларативных правил списка функций

По кнопке «Проверить» осуществляется проверка правил, представлено на рисунке 144.

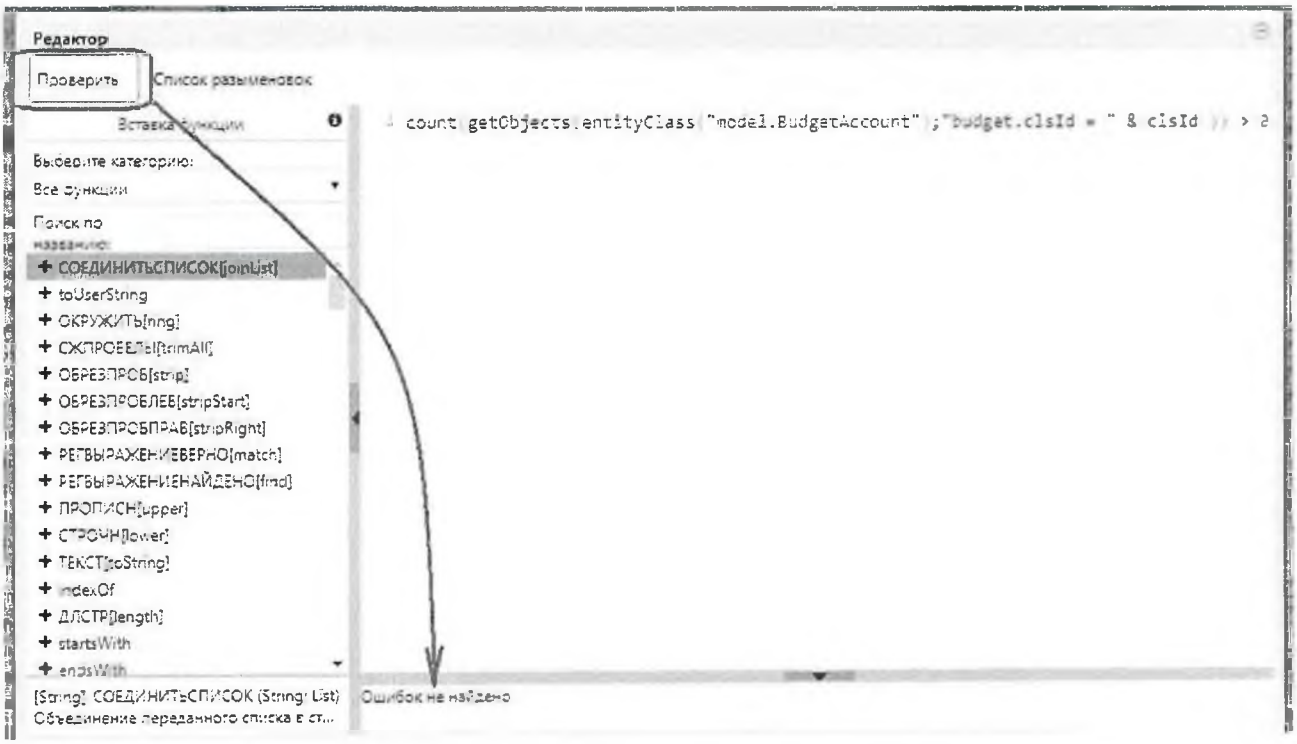


Рисунок 144 – Проверка правил в редакторе декларативных правил

Рассмотрим задание JavaScript правил. Редактор JavaScript, представлено на рисунке 145, похож на редактор декларативных правил, но только нет панели, отвечающей за выбор функции. Так же есть вспомогательные опции: «Список разыменовок» с доступными атрибутами, «Выберите документированный класс». На текущий момент задокументированы некоторые основные классы. Документация представляет стандартный для Java сгенерированный help-файл, в котором прописан список методов и их краткое описание.

Рисунок 145 – Редактор JavaScript

23.11. Формирование сообщения об ошибке

Если сработало правило, то сообщение об ошибке должно быть максимально информативным, чтобы пользователь понял, почему, какой конкретно атрибут введен неправильно.

Для описания сообщения об ошибке используется поле «Сообщение».

Для указания сообщения об ошибке используется синтаксис декларативного правила. Есть штатный способ указания сообщения об ошибке. Но не всегда достаточно статического сообщения, иногда требуется указание дополнительных атрибутов в самом тексте сообщения. На рисунке 146 приведен пример как в тексте сообщения вывести код конкретного лицевого счета.

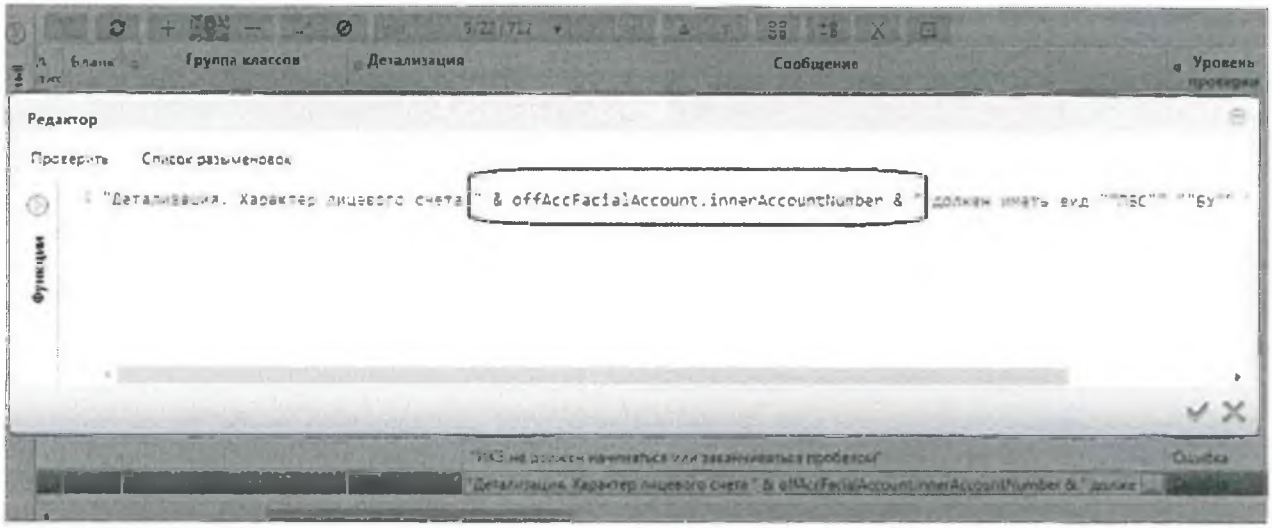


Рисунок 146 – Вывод значения атрибута «Лицевой счет» в сообщении об ошибке

Иногда требуется ещё более сложный текст ошибки. Для JavaScript есть возможность формирования произвольного текста ошибки любой сложности.

Пример:

```
if (params.length> 0) {
errorMsg = "Следующие параметры не допустимы: ".concat(params.join(", "));
}
let result = errorMsg == null || errorMsg.isEmpty();
letruleResult = new RuleResult(result, result ? null : errorMsg);
returnruleResult;
```

23.12. Оптимизация декларативных правил

Декларативные правила гораздо проще, чем МДК и выполняются гораздо быстрее. Но тем не менее для них тоже возникает вопрос оптимизации, потому что количество декларативных правил может быть большое. Соответственно, выполнение нескольких десятков правил на большом количестве документов может вызывать существенную временную задержку. Так же проблемы с задержками возникают тогда, когда выполняются правила фильтрации. Правила фильтрации выполняются над каждой строкой справочника. Если справочник достаточно большой, содержащий до 10 тыс. записей (например, коды целей, ЦСР), то правило фильтрации выполнится 10 тыс. раз, что создаст существенную временную задержку. В этих случаях возникают задачи по оптимизации декларативных правил.

Существует два способа оптимизации скорости выполнения декларативных правил.

Первый способ – использование предварительной фильтрации. Зачем выполнять правило на всех 10 тыс. строках справочника, если известно, что 9000 строк не нужны. Лучше сделать предварительную фильтрацию и оставить 1/10 строк, а потом применить правило на оставшейся 1/10 части справочника. Предварительная фильтрация может делаться средствами платформы на базе данных. В этом случае она может быть намного эффективней, чем проход по циклу с фильтром по каждой записи. Эта идея реализована в подходе с использованием скрипта вычисления префильтра (поле «Скрипт вычисления префильтра»), пример использования приведен на рисунке 147.

Пример, «Фильтр бух.операций по правилам использования». Тип правила «фильтр». Скрипт вычисления префильтра – это всегда JavaScript. На JavaScript формируется платформенный фильтр – это объектный фильтр, который выполняется hibernate, преобразуется в SQL ограничение и выполняется на базе данных. База данных эффективней фильтрует данные на порядок или 2 порядка, чем это делали бы мы. В результате опция фильтрации бухопераций упрощается. Вместо того, чтобы работать с большим справочником, мы работаем с более маленьким справочником.

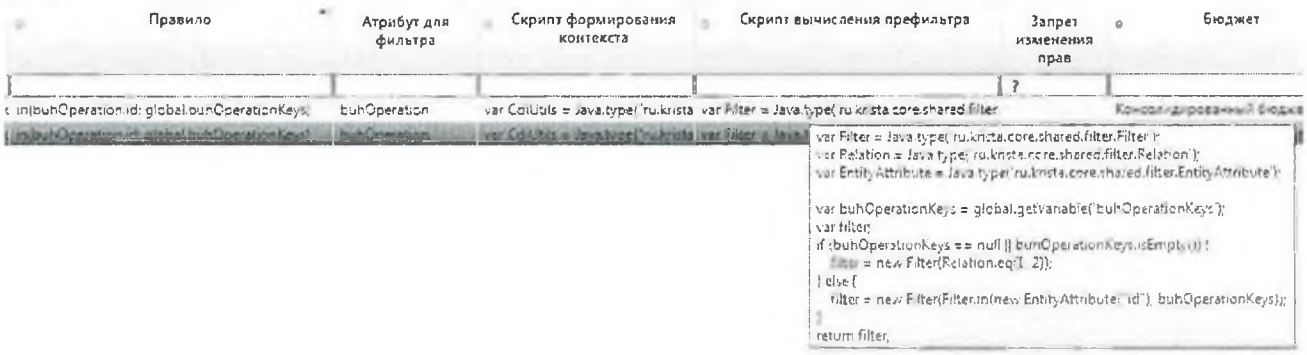


Рисунок 147– Пример использования поля «Скрипт вычисления префильтра»

Второй способ, который также используется для оптимизации работы декларативных правил – скрипт формирования контекста. Идея механизма: есть алгоритм фильтрации для каждой записи, который просчитывает одно и тоже: по записи справочника находится какой-то другой связанный справочник, по нему еще что-то определяется и т.д. Проверка занимает очень много времени. Причем в принципе можно проверку сделать 1 раз. Например, если работа идет со справочником только одного бюджета, и проверка будет заключаться в том, чтобы посчитать уровень этого бюджета. Так как работа будет со справочниками одного бюджета, то проверка для всех записей будет одна и та же. Это нерационально. Проблема в том, что декларативное правило не предполагает сохранение промежуточного результата, то есть нельзя вычислить один раз результат, его куда-то сохранить и потом дальше не вычислять, а использовать этот результат в декларативном правиле.

Во втором способе можно использовать еще один контекст – контекст global. Это фактически глобальные параметры. Можно общую часть посчитать один раз, результат вычисления положить в глобальные параметры и дальше из правила фильтрации использовать результат из глобальных параметров.

На рисунке 148 показан пример «Фильтра бухопераций по правилам использования». Один раз посчитали список бухопераций, положили его в глобальный параметр и дальше в правиле нужно проверить, что наша строка справочника есть в этом списке. В результате правило фильтрации выполняется на порядок быстрее, т.к. список просчитан один раз.

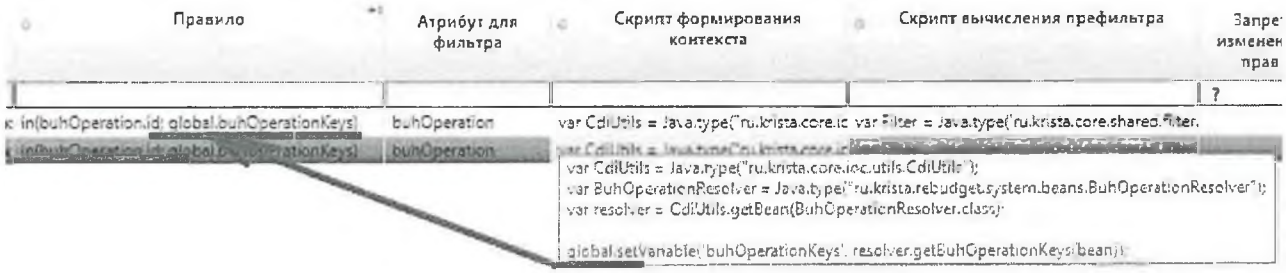


Рисунок 148 – Пример использования контекста global в поле «Скрипт формирования контекста»

24. Программный вызов внутридокументных контролей и правил из сценариев бизнес-процессов, бизнес-операций

Пользователь может вызывать ВДК по кнопке контролей. А что делать, если пользователь эту кнопку не нажал? Для этого случая администратор системы должен ВДК интегрировать в бизнес-процесс с помощью сценариев обработки (интерфейс «Сценарии обработки»), показаны на рисунке 149.Сценарии обработки подключаются к соответствующим бизнес-процессам и бизнес-операциям. Это событийный универсальный механизм.

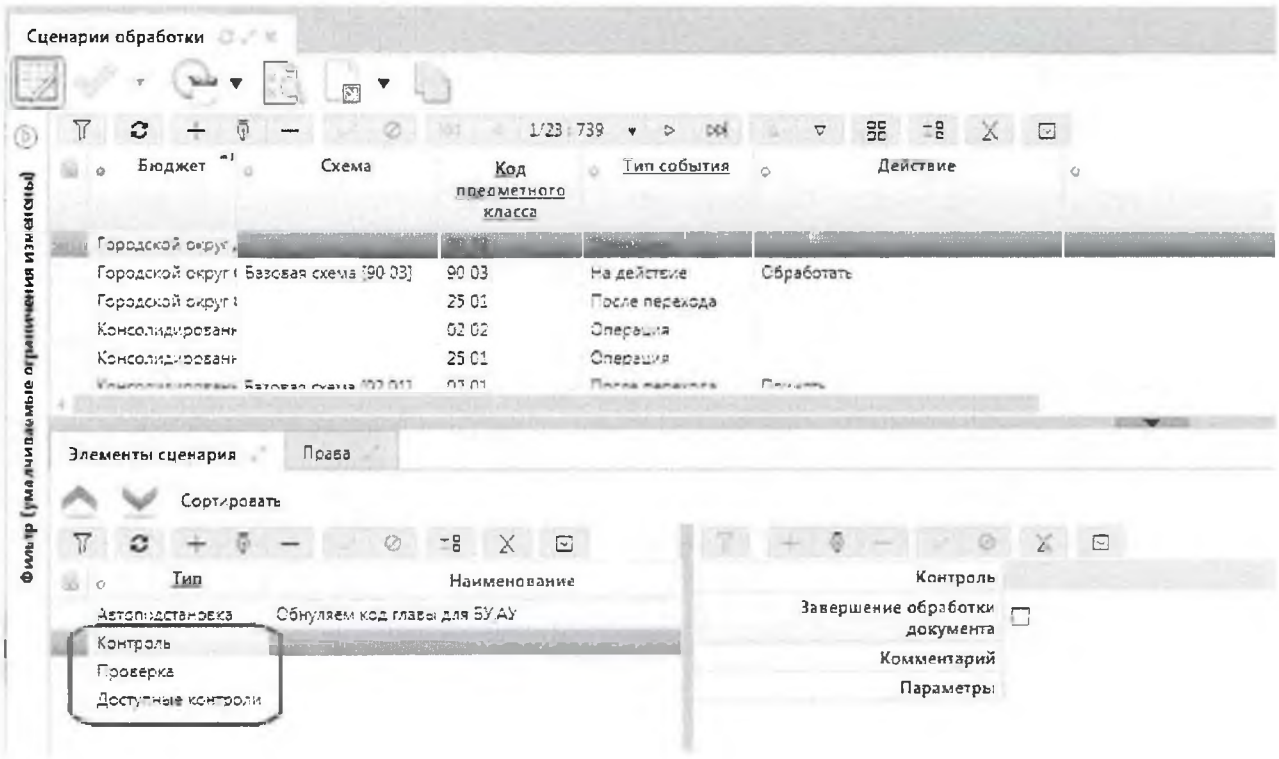


Рисунок 149– Элементы сценария для контролей

Сценарий обработки подключается к какой-то событийной точке. В сценарии обработки можно использовать элементы сценария. В таблице 10 приведен перечень элементов сценария, которые относятся к выполнению контролей.

Таблица 10 - Значения атрибута «Тип правила»

Элемент сценария	Использование
Контроль	Указывается конкретный ВДК контроль из списка. В этом случае будет выполнен только этот контроль

Элемент сценария	Использование
Доступные контроли	Указывается галочками, что нужно выполнить все доступные ВДК или все доступные МДК, или и те, и другие. Чаще всего выполняются все контроли. Не нужно уже указывать конкретные ВДК или МДК, система автоматически определяет список доступных контролей
Проверка	Подключается уже не контроль, а конкретное правило. Правило можно выбрать из списка или написать текст правила в поле «Текст фильтра». Это полезно, когда текст правила достаточно уникален и не имеет смысла выносить его в общий справочник декларативных правил, так как он нигде больше повторно использоваться не будет

Еще один нужный атрибут в элементах сценариев – галочка «Завершение обработки документа». Она определяет завершать обработку документа на первой ошибке сразу или выполнять все контроли до конца. В последнем случае пользователь получит полный список ошибок, но он будет дольше формироваться.

25. Вопросы профилирования и оптимизации работы внутридокументных контролей

Данный пункт касается общего профилирования. Если ВДК состоит из нескольких десятков декларативных правил, то ВДК может выполняться долго. Требуется определить, какие из декларативных правил тормозят, чтобы заняться их оптимизацией.

Для того, чтобы профилировать ВДК (узнать какие правила вызывают задержку) существует специальный параметр включения расширенного логгирования (вывода времени выполнения 10 самых долгих декларативных правил в лог контроля).

<loggercategory="ru.krista.retools.control.SimpleDocumentControlProvider" use-parent-handlers="true">

– <levelname="FINE"/>

</logger>

Это должен делать администратор системы или разработчик на своем сервере. Если региональному администратору нужно узнать дополнительную информацию по профилированию ВДК, то ему необходимо обратиться к разработчикам для включения дополнительного логгирования.

Когда дополнительное логгирование включено, профилировать время работы может уже любой администратор. В системе для администраторов есть специальный интерфейс «Серверный лог», который показывает результаты серверных логов.

На рисунке 150 приведен пример вывода времени выполнения правил в контроле. Используя эти данные легко определить какое правило стоить оптимизировать.

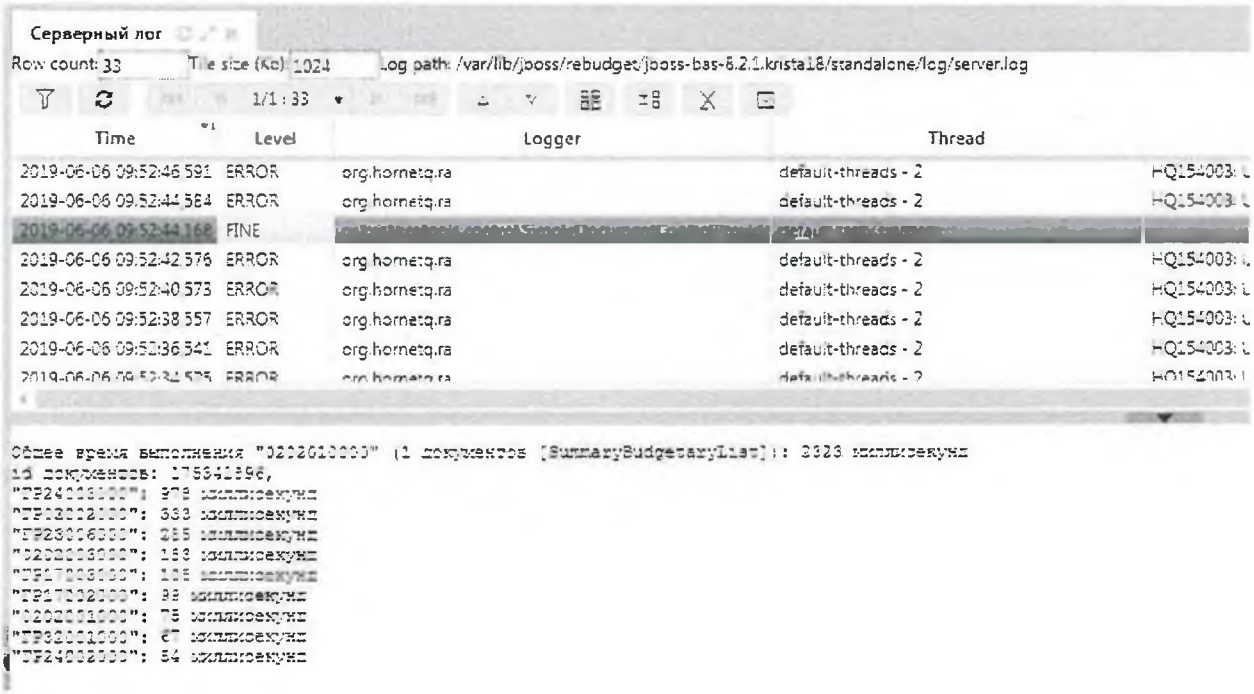


Рисунок 150 – Вывод времени выполнения декларативных правил в «Серверном логе»

26. Проверка Системы

Проверка осуществляется для остановленного сервера среднего звена Системы.

Система считается работоспособной, при условии:

— успешного запуска Системы;

— после успешного запуска работа Системы соответствует критериям штатного функционирования Системы.

27. Аварийные ситуации

Нарушение условий выполнения технологического процесса проявляется в виде невозможности выполнения и/или завершения технологической операции. Причиной нарушения условий выполнения технологического процесса, как правило, являются сбои в аппаратном обеспечении и программном обеспечении.

При невозможности выполнения и/или завершения технологической операции пользователь должен обратиться в подразделения технической поддержки ООО «НПО «Криста» (gz23@krista.ru) для восстановления работоспособности системы.

Пример настройки политик блокировки пользователей
при выявлении признаков перебора паролей

ru.krista.auth.login-blocking-policy-names – перечень используемых политик

ru.krista.auth.login-blocking.fast.fail-count - число неверных попыток для срабатывания политики

ru.krista.auth.login-blocking.fast.fail-count-time – горизонт времени для подсчета попыток аутентификации

ru.krista.auth.login-blocking.fast.lock-time – время блокировки

ru.krista.auth.login-blocking.fast.count-by-ip – использовать подсчет неверных попыток в разрезе ip-адреса пользователя

ru.krista.auth.login-blocking.fast.captcha – использовать вместо блокировки капчу

Пример настройки домена безопасности для поддержки политик блокировки

```
<security-domainname="krista" cache-type="default">
<authentication>
<login-module code="Remoting" flag="optional">
<module-option name="password-stacking" value="useFirstPass"/>
</login-module>
<login-module code="ru.krista.jaas.DataBaseStatiscticLoginModule"
flag="optional">
<module-option name="dsJndiName" value="java:/jdbc/dataaccess"/>
<module-option name="insertStats" value="insert into b_loginstats(id, login,
loginuuid, remoteaddr, success, logintime, useragent)
values(nextval('hibernate_sequence'), ?login, ?loginuuid, ?remoteaddr, ?success,
?logintime, ?useragent)"/>
<module-option name="selectUuid" value="select uuid from security_principal
where name = ?login"/>
</login-module>
<login-module code="UsersRoles" flag="sufficient">
<module-option name="unauthenticatedIdentity" value="guest"/>
<module-option name="usersProperties" value="/var/lib/jboss/rebudget/jboss-
bas-8.2.1.krista18/standalone/configuration/krista-users.properties"/>
<module-option name="rolesProperties" value="/var/lib/jboss/rebudget/jboss-
bas-8.2.1.krista18/standalone/configuration/krista-roles.properties"/>
<module-option name="password-stacking" value="useFirstPass"/>
</login-module>
<login-module code="ru.krista.auth.undertow.IdpClientLoginModule"
flag="optional">
<module-option name="roles" value="user"/>
</login-module>
<login-module code="ru.krista.jaas.DataBaseMultiLockPolicyLoginModule"
flag="requisite">
<module-option name="dsJndiName" value="java:/jdbc/dataaccess"/>
<module-option name="selectLock" value="select max(unlocktime), captcha
from b_loginblock where loginuuid = ?loginuuid and (remoteaddr is null or
remoteaddr = ?remoteaddr) and unlocktime&amp;gt; ?time group by captcha"/>
```

<module-option name="insertLock" value="insert into b_loginblock(id, login, loginuuid, remoteaddr, unlocktime, captcha, locktime, lockname) values(nextval('hibernate_sequence'), ?login, ?loginuuid, ?remoteaddr, ?unlocktime, ?captcha, ?locktime, ?lockname)"/>

<module-option name="deleteLocks" value="delete from b_loginblock where loginuuid= ?loginuuid"/>

<module-option name="clearLocks" value="delete from b_loginblock where unlocktime is null or unlocktime< ?time"/>

<module-option name="selectStats" value="select remoteaddr, success, logintime from b_loginstats where loginuuid= ?loginuuid and logintime> ?time order by logintimedesc limit ?count"/>

<module-option name="selectStatsByIp" value="select remoteaddr, success, logintime from b_loginstats where loginuuid= ?loginuuid and remoteaddr = ?remoteaddr and logintime> ?time order by logintimedesc limit ?count"/>

<module-option name="selectUuid" value="select uuid from security_principal where name = ?login"/>

</login-module>

<login-module code="ru.krista.jaas.DataBaseExpiryPolicyLoginModule" flag="requisite">

<module-option name="dsJndiName" value="java:/jdbc/dataaccess"/>

<module-option name="selectQuery" value="select lastchangepassdate, disposable_pass, permanent_pass FROM security_principal where name = ?"/>

</login-module>

<login-module code="DatabaseUsers" flag="optional">

<module-option name="unauthenticatedIdentity" value="guest"/>

<module-option name="hashUserPassword" value="true"/>

<module-option name="hashAlgorithm" value="SHA-256"/>

<module-option name="hashEncoding" value="HEX"/>

<module-option name="hashCharset" value="utf-8"/>

<module-option name="dsJndiName" value="java:/jdbc/dataaccess"/>

<module-option name="principalsQuery" value="SELECT p.password FROM security_principal p WHERE p.name = ?andp.isactive and (p.versionstarttime<= now() and p.versionfinaltime> now()) and (p.employee is null or exists(select * from bud_employee e where e.versioning_key = p.employee and e.versionstarttime<= now() and e.versionfinaltime> now()))"/>

```
        <module-option name="rolesQuery" value="SELECT
DISTINCT role_name,                roles                FROM
(                SELECT                        sp.name as user_name,
'Roles' as roles,                'user' as role_name                FROM
security_principalsp                UNION                SELECT
sp.name as user_name,                    'Roles' as roles,
sr.name as role_name                FROM
security_principalrolespr,                    security_rolesr,
security_principalsp                WHERE                (sr.id =
spr.role) and                (sp.id = spr.principal)                ) as u
WHERE user_name=?"/>
        <module-option name="password-stacking" value="useFirstPass"/>
        </login-module>
        </authentication>
        </security-domain>
```

Словарь запрещенных последовательностей для проверки пароля

```
//Распространенные пароли
secret
ctrhtn
pass
gfhjk
user
comp
admin
master
//Прямыецепочки
1234
2345
3456
4567
5678
6789
7890
qwer
asdf
zxcv
wert
sdfg
xcvb
erty
dfgh
cvbn
rtyu
fghj
vbnm
tyui
ghjk
yuio
hjkl
//Датырождения
195
```

196
197
198
199
200
201
202
january
february
march
april
may
june
july
august
september
october
november
december
//Обратныецепочки
0987
9876
8765
7654
6543
5432
4321
rewq
fdsa
vcxz
trew
gfds
bvcx
ytre
hgfd
nbvc
uytr
jhgf
mnbv

iuyt
kjhg
oiuy
lkjh
//Диагональные1
qaz
wsx
edc
rfv
tgb
yhn
ujm
//Диагональные2
qsc
wdv
efb
rgn
thm
//Змейки
1q2w
2w3e
3e4r
4r5t
5t6y
6y7u
7u8i
8i9o
9o0p
qaws
wsed
edrf
rftg
tgyh
yhuj
ujik
ikol
azsx
sxdc
dcfv

fvgb
gbhn
hnjm

Таблица 0.1 – Перечень и описание функциональных ролей (в соответствии с Законом № 44-ФЗ)

Идентификатор	Наименование	Описание назначения
РКС.АДМ	Администратор подсистемы управления закупками	Роль дает полномочия администратора в под системе.
РКС.КУЗ	Контрактный управляющий подсистемы управления закупками	Роль контрактного управляющего (сотрудника контрактной службы) заказчика, осуществляющего планирование закупок, определение единственного поставщика (подрядчика, исполнителя), формирование и публикацию сведений о контракте в реестре контрактов.
РКС.МСЗ	Осуществляющий мониторинг	Роль сотрудника, осуществляющего мониторинг в сфере закупок.
РКС.НСЗ	Размещающий правила нормирования	Роль сотрудника, осуществляющего нормирование в сфере закупок.
РКС.ПКЗ	Публикация закупок конкурентным способом подсистемы управления закупками	Роль сотрудника уполномоченного органа (уполномоченного учреждения), контрактного управляющего (сотрудника контрактной службы) заказчика, осуществляющего конкурентное определение поставщика (подрядчика, исполнителя).
РКС.ППС	Пользователь подсистемы управления закупками	Роль дает право входа в подсистему. При отсутствии данной роли вход в подсистему будет не возможен.

1	2	3
РКС.ПСЗ	Публикация совместной закупки подсистемы управления закупками	Роль сотрудника уполномоченного органа (уполномоченного учреждения), контрактного управляющего (сотрудника контрактной службы) заказчика, осуществляющего совместное определение поставщика (подрядчика, исполнителя).
РКС.РЕП	Согласование описания объекта закупки	Роль сотрудника органа власти, реализующего единую политику в соответствующей сфере
РКС.РУК	Полномочия руководителя в подсистеме закупок	Роль даёт права на выполнение операций, для которых требуется роль руководителя организации в подсистеме РКС
РКС.СДЗ	Согласование документацию по закупке подсистемы управления закупками	Роль сотрудника уполномоченного органа (уполномоченного учреждения), осуществляющего формирование/согласование документации по закупкам в соответствии с требованиями законодательства в сфере закупок.
РКС.СКЗ	Секретарь комиссии подсистемы управления закупками	Роль секретаря комиссии по закупкам, осуществляющего формирование и публикацию протоколов по закупкам.
РКС.СОЗ	Описание объекта закупок подсистемы управления закупками	Роль сотрудника уполномоченного органа (уполномоченного учреждения), осуществляющего согласование описания объекта закупок в соответствии с требованиями законодательства в сфере закупок.
РКС.СПЗ	Обоснование плана закупок, плана-графика закупок подсистемы управления закупками	Роль сотрудника органа власти, осуществляющего согласование планов закупок, планов-графиков подведомственных учреждений.

1	2	3
РКС.СПК	Согласование проекта контракта подсистемы управления закупками	Роль сотрудника уполномоченного органа (уполномоченного учреждения), осуществляющего согласование проекта контракта в соответствии с требованиями законодательства в сфере закупок.
РКС.ФКЗ	Финансовый контроль закупок	Финансовый контроль закупок
ОБЩ.НАЧ	Право подписи руководителя структурного подразделения	Роль дает право подписи документов той организации, где пользователь является сотрудником
ОБЩ.ГЛБ	Право подписи главного бухгалтера учреждения (органа власти)	Роль дает право визы (подписи) главного бухгалтера организации, а также право на выполнение других операций, для которых требуется роль главного бухгалтера
ОБЩ.РУК	Право подписи руководителя учреждения (органа власти)	Роль дает право визы (подписи) руководителя (директора) организации, а также право на выполнение других операций, для которых требуется роль руководителя организации
ОБЩ.КСП.ПРОСМОТР	Право на просмотр данных сотрудниками контрольно-счетной палаты	Роль дает права просмотра данных в подсистемах без права редактирования
ОБЩ.РУК_ФЭС	Право подписи руководителя финансово-экономической службы	Роль дает право визы (подписи) руководителя финансово-экономической службы, а также право на выполнение других операций, для которых требуется роль руководителя финансово-экономической службы организации.

Таблица 0.2 – Соответствие функциональных ролей и групп пользователей (в соответствии с Законом № 44-ФЗ)

Код	Наименование	Включить в группу	Правило
1	2	3	4
20.00	Планы-графики закупок. Создатель	Да	Функциональная роль = "РКС.КУЗ", Полномочие организации "ОДНО ИЗ":
			"Заказчик" (Код="201", "2CU"), "Заказчик, осуществляющий закупки в соответствии с частью 5 статьи 15 Закона № 44-ФЗ (27н)" (Код="212", "2CS"), "Организация, осуществляющая полномочия заказчика на осуществление закупок на основании соглашения в соответствии с частью 6 статьи 15 Закона № 44-ФЗ (27н)" (Код="213", "2OA")
20.10	Планы-графики закупок. Согласующий	Да	Функциональная роль = "РКС.СПЗ", Полномочие организации "ОДНО ИЗ": "Главного распорядителя бюджетных средств" (Код="101"), "Распорядителя бюджетных средств" (Код="102")
20.11	Планы-графики закупок. Согласующий финансовое обеспечение	Да	Функциональная роль = "ОБЩ.ГЛБ"
20.12	Планы-графики. Согласующий описания объекта закупки	Да	Функциональная роль = "РКС.СПЗ" Полномочие организации "ОДНО ИЗ": "Уполномоченный орган" (Код="202"), "Уполномоченное учреждение" (Код="203")
20.20	Планы-графики закупок. Утверждающий	Да	Функциональная роль = "ОБЩ.РУК" Полномочие организации "ОДНО ИЗ": "Заказчик" (Код="201", "2CU"), "Заказчик, осуществляющий закупки в соответствии с частью 5 статьи 15 Закона № 44-ФЗ (27н)" (Код="212", "2CS"), "Организация, осуществляющая полномочия заказчика на осуществление закупок на основании соглашения в соответствии с частью 6 статьи 15 Закона № 44-ФЗ (27н)" (Код="213", "2OA")
20.30	Планы-графики закупок. Публикующий	Да	Функциональная роль = "РКС.КУЗ", Полномочие организации "ОДНО ИЗ": "Заказчик" (Код="201", "2CU"), "Заказчик, осуществляющий закупки в соответствии с частью 5 статьи 15 Закона № 44-ФЗ (27н)" (Код="212", "2CS"),

Приложение 2

к приказу департамента по
регулированию контрактной системы
Краснодарского края

от 25.08.2023 № 91

«Приложение 3

к Регламенту работы региональной
информационной системы
Краснодарского края,
используемой в сфере
закупок для обеспечения
государственных и муниципальных нужд

ПОРЯДОК
формирования и размещения запроса о предоставлении ценовой информации в региональной информационной системе Краснодарского края, используемой в сфере закупок для обеспечения государственных и муниципальных нужд, в целях определения цены контракта, заключаемого с единственным поставщиком (подрядчиком, исполнителем)

1. Перечень терминов и сокращений

В настоящем документе применены следующие термины и сокращения с соответствующими определениями, представленные в Таблице 1.

Таблица 1

Перечень терминов и сокращений

Термин	Определение
Заказчик	государственный орган (в том числе орган государственной власти), орган управления государственным внебюджетным фондом либо государственное казенное учреждение, действующие от имени субъекта Российской Федерации, уполномоченные принимать бюджетные обязательства в соответствии с бюджетным законодательством Российской Федерации от имени субъекта Российской Федерации и осуществляющие закупки, а также бюджетное учреждение, автономное учреждение или государственное унитарное предприятие, осуществляющее закупки;

Термин	Определение
	муниципальный орган или муниципальное казенное учреждение, действующие от имени муниципального образования, уполномоченные принимать бюджетные обязательства в соответствии с бюджетным законодательством Российской Федерации от имени муниципального образования и осуществляющие закупки, а также бюджетное учреждение, автономное учреждение или муниципальное унитарное предприятие, осуществляющее закупки.
Поставщик	участник закупки малого объема, подавший заявку, соответствующую условиям закупки малого объема, с которым заключается контракт по итогам закупки малого объема
Участник закупки малого объема	любое юридическое лицо независимо от его организационно-правовой формы, формы собственности, места нахождения и места происхождения капитала, за исключением юридического лица, местом регистрации которого является государство или территория, включенные в утверждаемый в соответствии с пунктом 15 статьи 241 Бюджетного кодекса Российской Федерации перечень государств и территорий, используемых для промежуточного (офшорного) владения активами в Российской Федерации (далее - офшорная компания), либо юридического лица, являющегося иностранным агентом в соответствии с Федеральным законом от 14 июля 2022 г. № 255-ФЗ «О контроле за деятельностью лиц, находящихся под иностранным влиянием», или любое физическое лицо, в том числе зарегистрированное в качестве индивидуального предпринимателя, за исключением физического лица, являющегося иностранным агентом в соответствии с Федеральным законом от 14 июля 2022 г. № 255-ФЗ «О контроле за деятельностью лиц, находящихся под иностранным влиянием»
Закон № 44-ФЗ	Федеральный закон от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»
Порядок	порядок формирования и размещения запроса о предоставлении ценовой информации в Системе с целью последующего заключения контракта с единственным поставщиком (подрядчиком, исполнителем)

Термин	Определение
Закупка малого объема	комплекс мероприятий, проводимых заказчиком в целях получения ценовой информации в отношении товара, работы, услуги для определения цены контракта, заключаемого с единственным поставщиком (подрядчиком, исполнителем) в соответствии с пунктами 4 или 5 части 1 статьи 93 Закона № 44-ФЗ
Заявка	Предложение участника закупки малого объема, содержащее ценовую и иную информацию, необходимую для определения цены контракта, заключаемого с единственным поставщиком (подрядчиком, исполнителем) в соответствии с пунктами 4 или 5 части 1 статьи 93 Закона № 44-ФЗ
Система	региональная информационная система Краснодарского края, используемая в сфере закупок для обеспечения государственных и муниципальных нужд
Электронный ресурс	информационная система, обеспечивающая проведение закупок малого объема, являющаяся модулем Системы, или внешний ресурс, интегрированный с Системой
ОКПД 2	ОК 034-2014 (КПЕС 2008). Общероссийский классификатор продукции по видам экономической деятельности
КТРУ	Каталог товаров работ, услуг для обеспечения государственных и муниципальных нужд

2. Описание порядка формирования и размещения запроса о предоставлении ценовой информации в Системе

2.1 Порядок разработан в целях реализации распоряжения главы администрации (губернатора) Краснодарского края от 11 октября 2019 г. № 376-р «Об утверждении методических рекомендаций по применению методов определения цены контракта, заключаемого с единственным поставщиком (подрядчиком, исполнителем)» и применяется заказчиками в дополнение к методическим рекомендациям по применению методов определения начальной (максимальной) цены контракта, цены контракта, заключаемого с единственным поставщиком (подрядчиком, исполнителем), утвержденным приказом Министерства экономического развития Российской Федерации от 2 октября 2013 г. № 567.

2.2. Порядок определяет процесс сбора ценовых предложений с использованием Системы для определения и обоснования методом сопоставимых рыночных цен (анализа рынка) цены контракта, заключаемого с единственным поставщиком (подрядчиком, исполнителем) в соответствии с пунктами 4 или 5 части 1 статьи 93 Закона № 44-ФЗ.

3. Определение цены контракта с использованием Системы

3.1. Для определения и обоснования цены контракта с использованием электронного ресурса заказчики формируют информацию о закупке малого объема в Системе в соответствии с Инструкцией для закупок малого объема, расположенной в разделе «Инструкции» интерфейса «Закупки».

3.2. Информация о закупке малого объема, формируемая в Системе, должна содержать:

код ОКПД 2;

код КТРУ (при наличии);

наименование объекта закупки;

описание объекта закупки, сформированное заказчиком в соответствии со статьей 33 Закона № 44-ФЗ, с указанием единицы измерения, количества товара, объема работы или услуги, в том числе в соответствии с КТРУ (при наличии), а также иных условий, необходимых для заключения контракта;

объем финансового обеспечения на закупку малого объема, определенный с учетом норм статей 19, 22 Закона № 44-ФЗ;

срок подачи заявок;

проект контракта;

инструкцию для участника закупки малого объема по форме согласно приложению 1 к Порядку, которая должна содержать:

информацию о применении национального режима в части установления запрета на допуск товаров, происходящих из иностранных государств, работ, услуг, соответственно выполняемых, оказываемых иностранными лицами, и предоставлении подтверждающих документов и (или) информации в соответствии с требованиями, предусмотренными соответствующими нормативными правовыми актами, если в отношении закупаемых товаров (работ, услуг) установлены соответствующие требования;

информацию об установлении единых требований к участникам закупки малого объема в соответствии с частью 1 статьи 31 Закона № 44-ФЗ и документах, подтверждающих соответствие требованиям, установленным в рамках пункта 1 части 1 статьи 31 Закона № 44-ФЗ (при необходимости), если в отношении лиц, поставляющих товары, выполняющих работы, оказывающих услуги, устанавливаются соответствующие требования.

3.3. Заказчик вправе установить срок подачи заявок самостоятельно, но он должен составлять не менее одного рабочего дня с даты размещения информации о закупке малого объема. В случае, если заказчик оставляет поле «Дата и время окончания подачи заявок» пустым Система проставляет такой срок автоматически – один рабочий день с даты размещения информации о закупке малого объема.

В случае если заявки на закупку малого объема не поступили, срок окончания подачи заявок продлевается на два рабочих дня.

Если с учетом продления срока подачи заявок на закупку малого объема заявки не поступили, заказчик вправе заключить контракт без использования Системы. При этом сведения о таком контракте формируются в Системе из несостоявшейся закупки малого объема.

Если на закупку малого объема поступила одна или более заявок, заказчик вправе заключить контракт с учетом положений пункта 3.5 Порядка.

Если по результатам рассмотрения заявок все заявки отклонены, заказчик вправе провести новую закупку.

3.4. Подача заявок осуществляется с момента размещения информации о закупке малого объема и прекращается по истечении срока, указанного заказчиком в соответствии с требованиями пункта 3.3 Порядка.

3.5. Заказчик в течение трех рабочих дней после окончания срока подачи заявок:

рассматривает заявки на соответствие установленным требованиям закупки малого объема;

при наличии заявок, соответствующих установленным требованиям закупки малого объема, определяет цену контракта на основании минимального предложения цены;

формирует в Системе протокол рассмотрения заявок на закупку малого объема по форме согласно приложению 2 к Порядку;

направляет посредством Системы на электронный ресурс поставщику для подписания проект контракта.

При подаче минимального ценового предложения несколькими участниками закупки малого объема поставщиком признается участник, заявка которого поступила ранее других заявок.

Заказчик при направлении поставщику проекта контракта для подписания вправе самостоятельно установить предельный срок направления заказчику подписанного проекта контракта, изменив значение, установленное в Системе по умолчанию (3 рабочих дня), в большую или меньшую сторону, но не менее 1 рабочего дня с даты отправки поставщику проекта контракта. В случае если по истечении данного срока заказчику не поступит в Системе подписанный контракт, заказчик вправе направить проект контракта участнику, заявка которого соответствует требованиям закупки малого объема и содержит следующее минимальное ценовое предложение, при этом предельный срок подписания контракта должен составлять не менее 1 рабочего дня.

3.6. Протокол рассмотрения заявок на закупку малого объема может содержать следующие основания для отказа от заключения контракта с участником закупки малого объема и (или) признания заявки несоответствующей установленным требованиям закупки малого объема:

ценовое предложение в заявке участника закупки малого объема превышает объем финансового обеспечения на закупку малого объема, установленный заказчиком;

заявка и (или) участник не соответствует условиям и требованиям, установленным в закупке малого объема;

установление недостоверности информации, содержащейся в документах и информации, представленных участником закупки малого объема.

Начальник отдела
информационно-аналитического
сопровождения  В.С. Лабунец

Приложение 1
к Порядку формирования и
размещения запроса о
предоставлении ценовой
информации в Региональной
информационной системе
Краснодарского края, используемой
в сфере закупок для обеспечения
государственных и муниципальных
нужд, в целях определения цены
контракта, заключаемого с
единственным поставщиком
(подрядчиком, исполнителем)

ИНСТРУКЦИЯ
для участника закупки малого объема

Предложение участника закупки малого объема, содержащее ценовую и иную информацию, необходимую для определения цены контракта, заключаемого с единственным поставщиком (подрядчиком, исполнителем) в соответствии с пунктами 4 или 5 части 1 статьи 93 Закона № 44-ФЗ (далее – заявка), направляемое с использованием региональной информационной системы, используемой в сфере закупок для обеспечения государственных и муниципальных нужд (далее – система), или внешнего ресурса, интегрированного с Системой, должно соответствовать условиям и требованиям закупки малого объема и содержать следующую информацию:

1) наименование товара, товарном знаке (его словесном обозначении) (при наличии), конкретной модели (при наличии), знаке обслуживания (при наличии), фирменном наименовании (при наличии), патенте (при наличии), полезной модели (при наличии), промышленном образце (при наличии), наименовании производителя и страны происхождения товара;

2) функциональные, технические и качественные характеристики, эксплуатационные характеристики объекта закупки;

3) документы, подтверждающие соответствие требованиям пункта 1 части 1 статьи 31 Федерального закона от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» (далее – Закон № 44-ФЗ) (при наличии таких требований);

4) подтверждающие документы и (или) информацию в соответствии с требованиями, установленными нормативными правовыми актами о запрете на допуск товаров, происходящих из иностранных государств работ, услуг, соответственно выполняемых, оказываемых иностранными лицами (при установлении заказчиком таких требований в информации о закупке малого объема в соответствии с нормами статьи 14 Закона № 44-ФЗ (применение национального режима при осуществлении закупок));

5) расчет цены товара (работы, услуги).

Наименование страны происхождения товаров рекомендуется указывать в соответствии с Общероссийским классификатором стран мира ОК (МК (ИСО 3166) 004-97) 025-2001. Ответственность за достоверность сведений о стране происхождения товара, указанного в предложении, несет участник закупки.

Заявка и документы и (или) информация к заявке участника закупки малого объема в отношении объекта закупки должны содержать конкретные значения показателей. Не допускается наличие неопределенности в значениях или множественность значений, свойственных модельному ряду закупаемых (используемых) товаров. Значения показателей, предоставляемых участником закупки малого объема, не должны допускать разночтений или иметь двусмысленное толкование.

Заявка и документы и (или) информация к заявке участника закупки малого объема в отношении поставляемых товаров, товаров, используемых при выполнении работ, оказании услуг, с любыми товарными знаками не должно сопровождаться словами «или эквивалент».

Заявка и документы и (или) информация к заявке участника закупки малого объема в отношении объекта закупки должно соответствовать требованиям к такому объекту, установленным заказчиком в описании объекта закупки.

Начальник отдела
информационно-аналитического
сопровождения  В.С. Лабунец

Приложение 2
к Порядку формирования и размещения запроса о предоставлении ценовой информации в Региональной информационной системе Краснодарского края, используемой в сфере закупок для обеспечения государственных и муниципальных нужд, в целях определения цены контракта, заключаемого с единственным поставщиком (подрядчиком, исполнителем)

ФОРМА
протокола рассмотрения заявок на закупку малого объема

Наименование заказчика	
Объект закупки	
Предельная цена контракта, руб.	
Адрес электронного ресурса (площадки)	
Идентификационный код закупки	
Номер закупки	

По результатам сбора предложений для заключения государственного (муниципального) контракта для обеспечения государственных (муниципальных) нужд заказчика на основании пункта 4 (5) части 1 статьи 93 Федерального закона от 5 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» поступили следующие предложения:

№ п/п	Номер заявки участника	Дата и время подачи предложения	Предложение о цене, руб.	Решение заказчика	Обоснование принятия решения
1					
2					
3					

Решение заказчика по итогу рассмотрения заявок на закупку малого объема:

_____

Контрактный управляющий (руководитель контрактной службы)

_____

Инициатор закупки _____

Иные должностные лица (при необходимости)».

Начальник отдела
информационно-аналитического сопровождения  В.С. Лабунец

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
к проекту приказа «О внесении изменений в приказ департамента по регулированию контрактной системы Краснодарского края от 3 февраля 2020 г. № 11 «Об утверждении Регламента работы региональной информационной системы Краснодарского края, используемой в сфере закупок для обеспечения государственных и муниципальных нужд»

В соответствии с изменением функциональных ролей пользователей региональной информационной системе Краснодарского края, используемой в сфере закупок для обеспечения государственных и муниципальных нужд (далее – РИССЗ КК), приложение 2 к Регламенту работы региональной информационной системы Краснодарского края, используемой в сфере закупок для обеспечения государственных и муниципальных нужд (далее – Регламент), изложено в новой редакции.

Пункты 2-4 Регламента изложены с учетом добавленного функционала осуществления закупок по Федеральному закону от 18 июля 2011 г. № 223-ФЗ «О закупках товаров, работ, услуг отдельными видами юридических лиц».

В связи с изменением алгоритма осуществления закупок малого объема, добавлением возможности автоматической установки даты и времени окончания подачи заявок и добавления новой функции автоматического продления срока подачи заявок приложение, изменением требований к срокам приема ценовых предложений участников закупки малого объема и исключением формулировок, позволяющих заказчику учитывать ценовые предложения, поступившие не через РИССЗ КК, приложение 3 к Регламенту изложено в новой редакции.

Начальник отдела
информационно-аналитического
сопровождения  В.С. Лабунец