2011

ЦЕНТРИНФОРМ

# CRLS

**(Система управления доступом к данным)**

Система CRLS предназначена для осуществления политики разграничения доступа к информации на уровне записей и ячеек защищаемых таблиц, хранящихся в базе данных под управлением MS SQL сервера и предоставления удобных средств администрирования настройки доступа

## Руководство администратора

# Содержание

# 1 ВВЕДЕНИЕ

Настоящий документ содержит руководство администратора системы по управлению доступом к данным (CRLS) (далее – система CRLS или Система). Руководство включает в себя справочную информацию о Системе и сведения о её настройке.

## 1.1 Область применения

Система CRLS предназначена для осуществления политики разграничения доступа к информации на уровне записей и ячеек защищаемых таблиц, хранящихся в базе данных под управлением MS SQL сервера и предоставления удобных средств администрирования настройки доступа.

## 1.2 Краткое описание возможностей

При помощи системы CRLS решается проблема реализации политики разграничения доступа к данным на уровне записей/ячеек, при условии максимального удобства в администрировании.

При этом система имеет возможность:

- предоставления ручного управления доступом на уровне строк (записей) и ячеек таблицы базы данных;
- автоматического разграничения доступа к данным в соответствии с предопределяемыми настройками.

Также система обладает следующими характеристиками:

- поддерживает модель безопасности Microsoft SQL Server;
- интегрируется в приложения, архитектура которых предполагает работу с базой данных через фиксированное соединение;
- для интеграции в системы, построенные на основе WEB, где за разграничение доступа к данным отвечает уровень бизнес логики (WEB сервер), а работа с БД ведется с использованием фиксированного соединения (соединение, ведущееся от встроенной учетной записи, представляющей один из уровней архитектуры, в частности для WEB-ориентированных приложений это будет WEB сервер IIS, Apache…), реализован механизм идентификации и последующей имперсонализации пользователя на уровне БД при использовании фиксированного соединения;
- удовлетворяет требованиям по производительности;
- обеспечивает прозрачный доступ средствами, предоставляемыми Microsoft SQL Server, к данным защищенным системой разграничения;

- имеет средства администрирования независимые от специфики приложений взаимодействующих с базой данных.

### 1.3 Уровень подготовки администратора

Администратор системы CRLS должен обладать знаниями состава и структуры Системы, навыками по сопровождению и настройке Системы, администрированию общесистемного программного обеспечения Системы (ОС, СУБД).

В задачи администратора системы CRLS входит регистрация пользователей и их ролей, построение необходимой иерархии ролей для реализации требуемой политики доступа, а также задание разрешений (в терминах Системы), удовлетворяющих разграничению прав доступа к данным.

### 1.4 Перечень эксплуатационной документации, с которой необходимо ознакомиться пользователю

Администратор системы CRLS должен обладать знаниями настоящего Руководства, а также следующих документов:

- Общее описание Системы;
- Описание контрольного примера.

## 2 ОПИСАНИЕ ОПЕРАЦИЙ

Прежде чем реализовывать политику разграничения доступа к записям/ячейкам объекта (таблицы) с помощью системы CRLS необходимо продумать роли, их иерархию и разрешения на доступ для каждой роли (какие данные каким пользователям будут доступны). Далее (с помощью средства администрирования) осуществляются следующие действия:

- регистрация пользователей в системе CRLS;
- регистрация ролей пользователей и задание их иерархии в системе CRLS;
- включение защищаемых таблиц в систему CRLS;
- создание правил и назначение разрешений;
- контроль произведенных настроек доступа.

### 2.1 Запуск приложения администрирования системы CRLS

Вход в панель администрирования выполняется в несколько этапов:

- запустите приложение администрирования системы CRLS **CRLSWinAdmin.exe**;
- нажмите кнопку меню **«Подключение»**, далее – **«Подключить»**;

- в появившемся окне (рис. 1) заполните необходимые поля и нажмите **«Подключить»**.

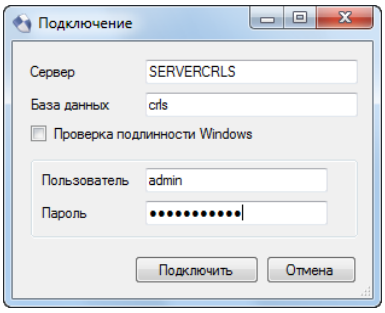


*Рис. 1. Вход в панель администрирования CRLS-системы*

## 2.2 Роли, пользователи, иерархия, поддержка SQL-сервера

В системе CRLS поддерживается построение иерархии ролей и включение в нее пользователей. Также реализована поддержка пользователей, ролей и иерархии ролей, определенных в рамках БД SQL сервера.

### 2.2.1 Регистрация пользователя

Нажмите кнопку меню **«Администрирование»**, далее выберите пункт **«Пользователи»**. На **рис. 2** показана панель работы с пользователями CRLS-системы.

Нажмите кнопку **«Добавить»**, чтобы зарегистрировать нового пользователя.

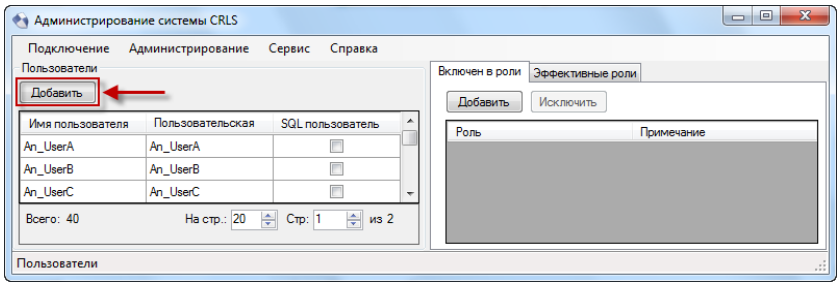


*Рис. 2. Панель работы с пользователя CRLS - системы*

В появившемся окне (рис. 3) заполните необходимые поля и нажмите кнопку **«Ок»**.

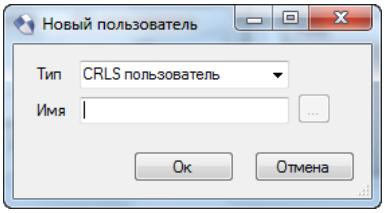


*Рис. 3. Добавление нового CRLS-пользователя*

В случае использования SQL серверной модели безопасности регистрируются существующие SQL – пользователи. Для их автоматического поиска необходимо сменить поле **«Тип»** на **«Пользователь SQL»**, нажать кнопку поиска **«…»** и выбрать пользователя из списка предложенных (рис. 4), затем нажать кнопку **«Ок»**.

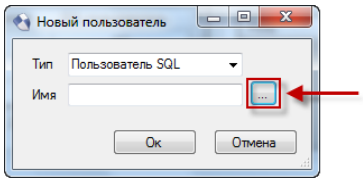


*Рис. 4. Добавление нового SQL-пользователя*

После сохранения новый пользователь отобразится в панели работы с пользователями CRLS-системы (см. рис. 2).

### 2.2.2 **Регистрация ролей**

Роли определяют права и возможности пользователей при работе с таблицами баз данных на основе сформированных правил (паттернов) и разрешений.

Нажмите кнопку меню **«Администрирование»** и выберите пункт **«Роли»**. На **рис. 5** показана панель работы с ролями CRLS-системы.

Нажмите кнопку **«Добавить»**, чтобы добавить новую роль.

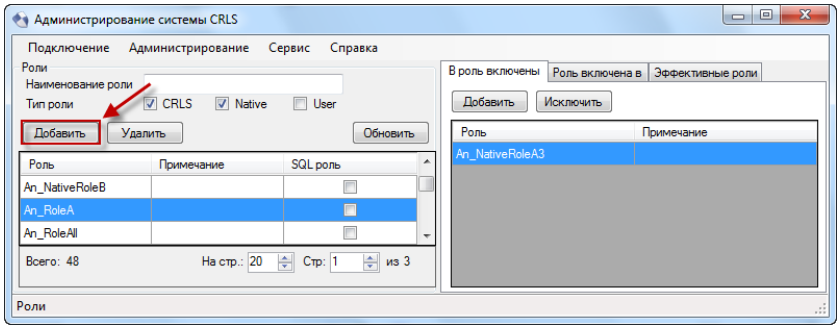


*Рис. 5. Панель работы с ролями CRLS - системы*

В появившемся окне заполните необходимые поля и нажмите кнопку **«Ок»** (рис. 6).

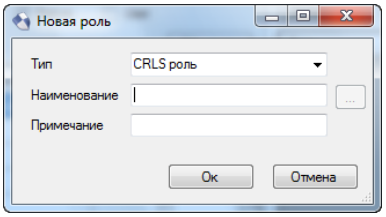


*Рис. 6. Добавление роли*

Новая роль отобразится в панели управления ролями CRLS-системы (см. рис. 5).

#### *2.2.2.1 Регистрация SQL-роли.*

Если предполагается использование ролей, определённых в рамках SQL- сервера, то их необходимо зарегистрировать в системе CRLS.

Чтобы добавить SQL-роль, нажмите **«Добавить»** (см. рис. 5). В появившемся окне (рис. 7) смените поле **«Тип»** на **«Роль SQL»**, нажмите кнопку поиска **«…»,** выберите роль из списка предложенных и нажмите кнопку **«Ок»**.

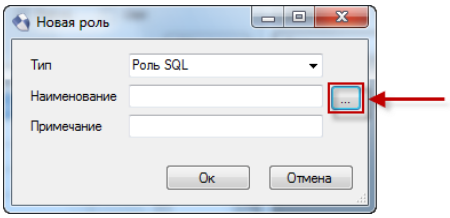


*Рис. 7. Добавление SQL роли*

Новая роль отобразиться в панели управления ролями CRLS-системы (см. рис. 5).

#### 2.2.2.2 *Построение иерархии ролей.*

Зарегистрированные роли можно включать друг в друга для построения их иерархии.

Чтобы связать две и более ролей, в панели управления ролями выберите роль, к которой хотите добавить другие роли, и нажмите кнопку **«Добавить»** (рис. 8)

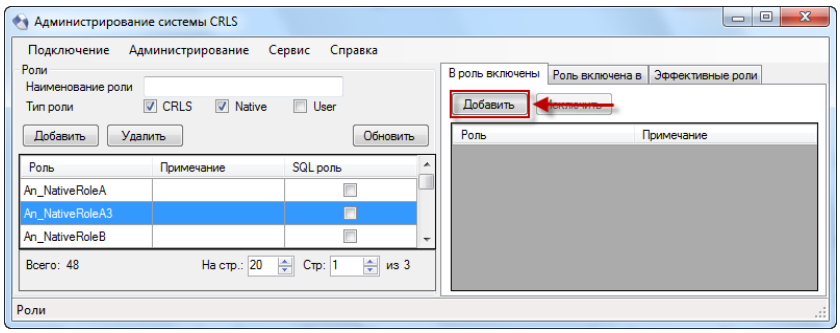


*Рис. 8. Создание иерархии ролей*

В появившемся окне выберите роль, которую нужно добавить, и нажмите кнопку **«Ок»** (рис. 9).

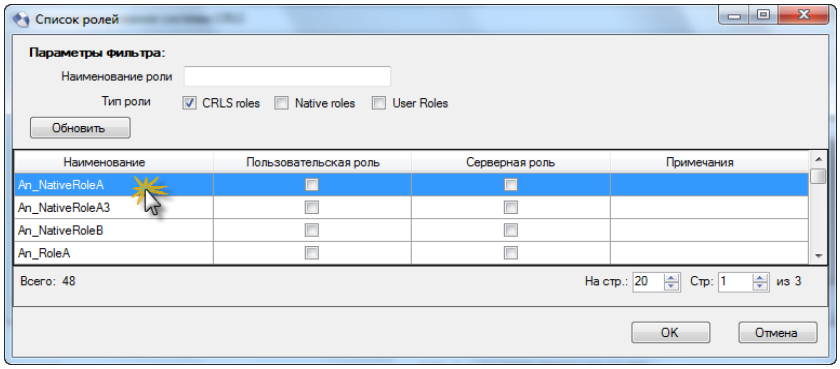


*Рис. 9. Выбор роли для объединения*

Объединённая роль отобразится в правой части панели управления ролями на вкладке **«В роль включены»**, которая открыта по умолчанию (рис. 10).

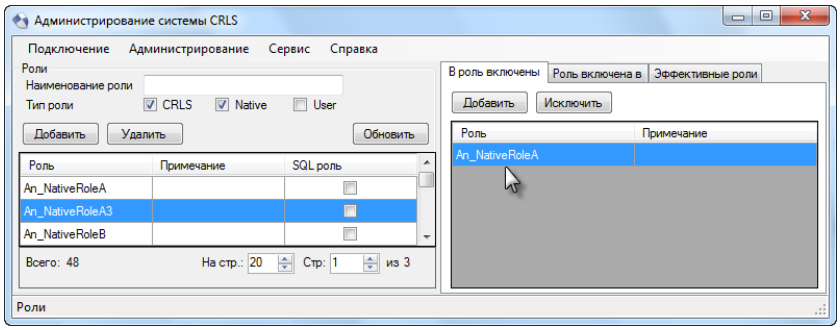


*Рис. 10. Отображение связанных ролей*

На вкладке **«Роль включена в»** отображаются роли, в состав которых включена выделенная роль. На вкладке **«Эффективные роли»** отображаются все роли, с которым связана выделенная роль.

### 2.2.3 Назначение ролей пользователю

Чтобы включить пользователя в роли, в панели управления пользователями нажмите кнопку **«Добавить»** (рис. 11).

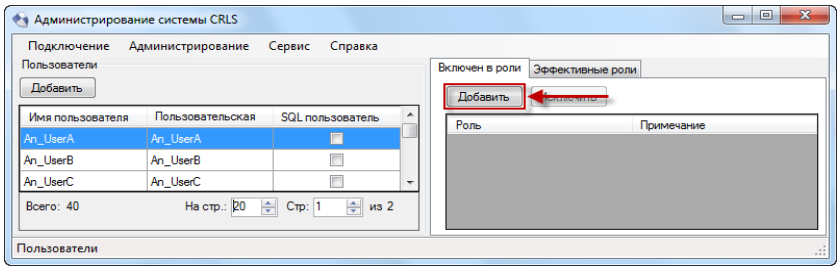


*Рис. 11. Включение пользователя в роль*

В появившемся окне выберите нужную роль и нажмите кнопку **«Ок»** (рис. 12)

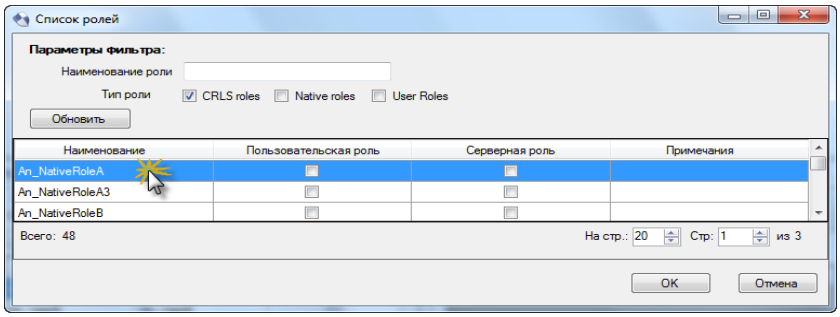


*Рис. 12. Выбор роли для пользователя*

Список ролей, в которые включен пользователь, отобразится в правой части панели управления пользователями на вкладке **«Включен в роли»** (рис. 13).

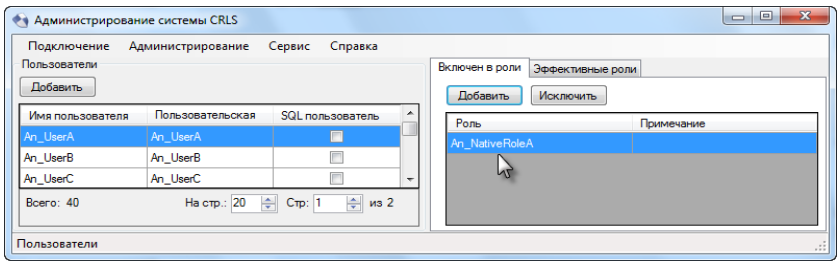


*Рис. 13. Список ролей пользователя*

На вкладке **«Эффективные роли»** отображаются все роли, с которыми связан пользователь.

## 2.3 Включение/исключение таблиц в систему/из системы CRLS

### 2.3.1 Общие сведения

Для реализации политики разграничения доступа к записям/ячейкам объекта (таблицы) с помощью системы CRLS необходимо произвести включение выбранной таблицы в систему. При выполнении данной операции происходит создание инфраструктуры, необходимой для функционирования механизмов системы CRLS по разграничению доступа. К этой инфраструктуре относится отображение (представление, полностью повторяющее структуру таблицы, в том числе значения по умолчанию, вычисляемые поля, и т.д.), через которое субъект может осуществить доступ к объекту (таблице), ключи шифрования и прочее.

После включения таблицы в систему CRLS появляется возможность реализации политики разграничения доступа путем создания правил и назначения разрешений.

### 2.3.2 Включение таблицы в систему

Включение таблицы в систему происходит в три этапа:

1) Выбор необходимой таблицы, для которой необходимо разграничение доступа системой CRLS;
2) Настройка параметров включения для выбранной таблицы, включение;
3) Просмотр отчета о ходе выполнения операции.

#### *2.3.2.1 Добавление таблицы в систему CRLS*

Нажмите кнопку меню **«Администрирование»** и выберите пункт **«Таблицы»**. На рис. 14 показана панель работы с таблицами системы CRLS.

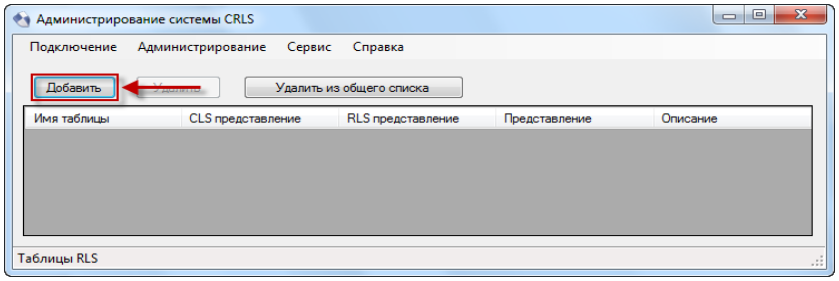


*Рис. 14. Добавление таблицы в систему CRLS*

В появившемся окне выберите таблицу, доступ к данным которой требуется разграничить, и нажмите кнопку **«Далее»** (Рис. 15).

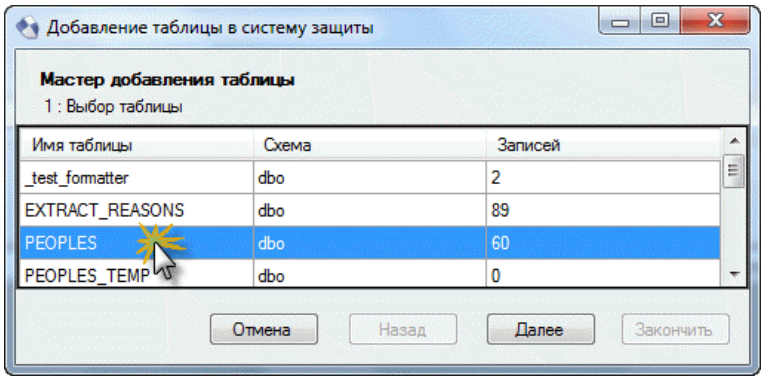


*Рис. 15. Выбор таблицы*

На следующем шаге (рис. 16) можно осуществить настройку параметров включения таблицы в систему CRLS:

- CLS-представление - имя представления уровня CLS, отвечающего за разграничение на уровне ячеек (генерируется автоматически);
- RLS-представление - имя представления уровня RLS, отвечающего за разграничение на уровне записей (генерируется автоматически);
- Главное представление - имя представления, через которое будет осуществляться доступ к данным защищаемой таблицы. Данное представление должно быть доступно конечному потребителю взамен защищаемой таблицы (генерируется автоматически);
- Имя публичного ключа - имя симметричного ключа (генерируется автоматически).
- Заполните необходимые поля и нажмите кнопку **«Далее»**.

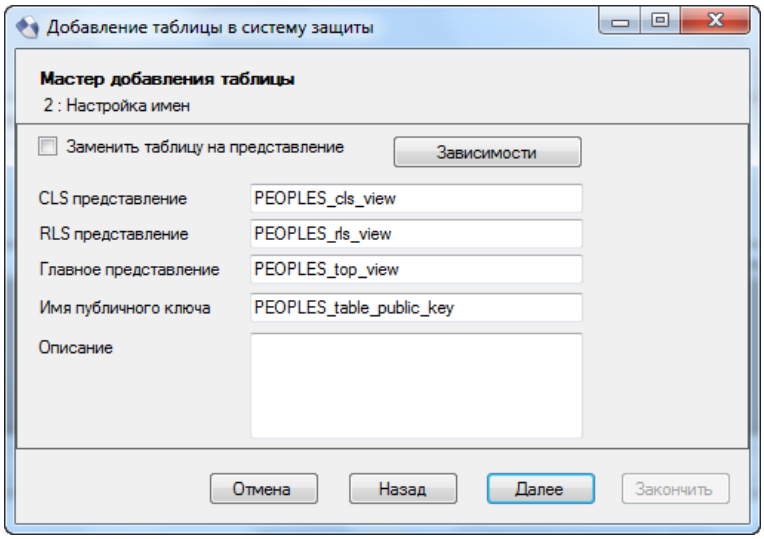


*Рис. 16. Настройка представлений для таблицы*

При необходимости переноса или копирования разрешений SQL-сервера, отметьте галочкой соответствующее поле, выберите **«Разрешения»** и нажмите кнопку **«Далее»** (рис. 17).

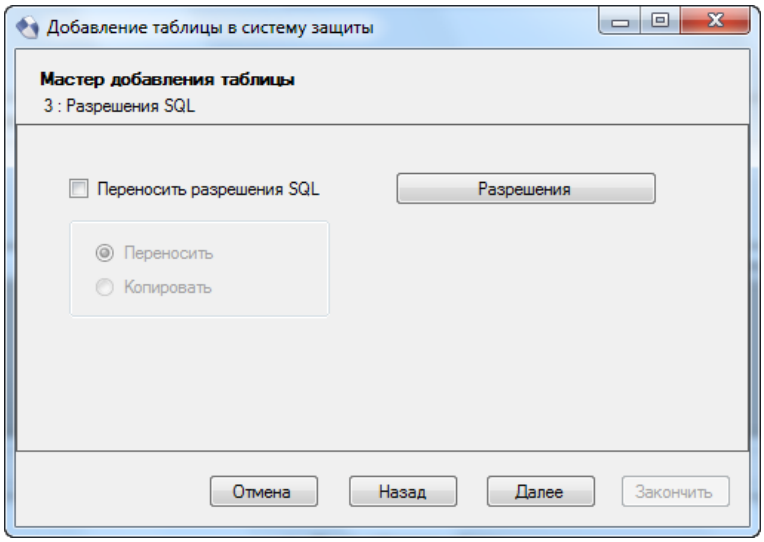


*Рис. 17. Разрешения SQL*

На следующем шаге необходимо указать, для каких колонок таблицы будет осуществляться разграничение на уровне ячеек. Список доступных колонок формируется из всех колонок выбранной таблицы, тип данных которых позволяет сохранение шифрограмм (рис. 18). Выберите нужные колонки и нажмите кнопку **«Закончить»**.

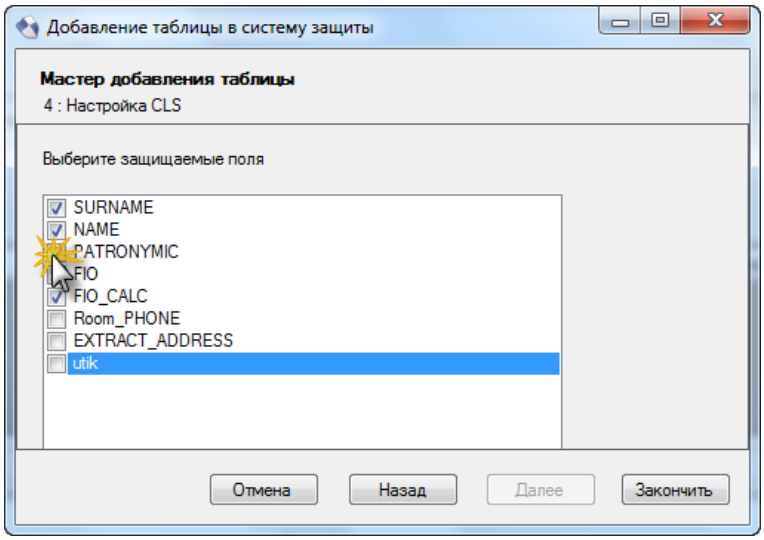


*Рис. 18. Выбор защищаемых колонок таблицы*

### 2.3.2.2 *Просмотр отчета о ходе выполнения операции*

В данном отчете содержится описание всех шагов, осуществляемых системой при переводе таблицы в режим защищаемой, и статус их выполнения (рис. 19).

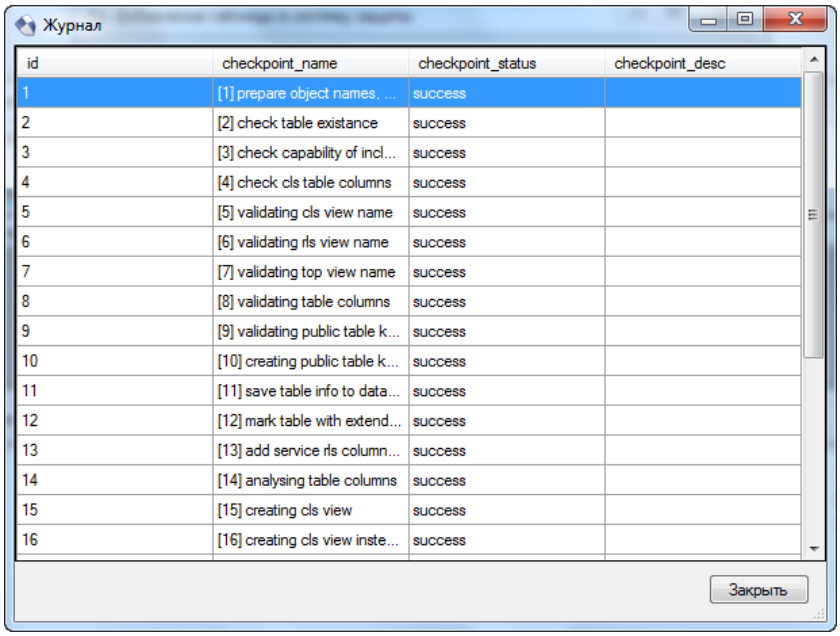


*Рис. 19. Отчет о ходе выполнения операции включения*

### 2.3.3 Исключение таблицы из системы

Исключение таблицы из системы происходит в два этапа:

1) Выбор необходимой таблицы, исключаемой из системы CRLS;
2) Просмотр отчета о ходе выполнения операции.

#### *2.3.3.1 Выбор необходимой таблицы*

Нажмите кнопку меню **«Администрирование»** и выберите пункт **«Таблицы»**. Отметьте таблицу, которую необходимо удалить, и нажмите кнопку **«Удалить»** (рис. 20).

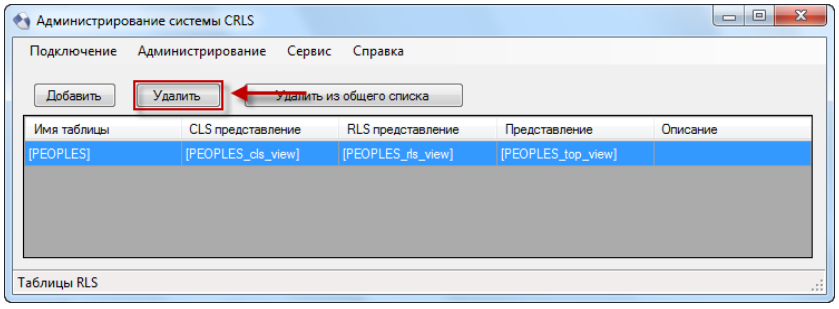


*Рис. 20 Удаление таблицы из системы CRLS*

Данная опция позволяет деинсталлировать инфраструктуру системы в случае неудачного завершения операции включения в систему.

#### *2.3.3.2 Просмотр отчета о ходе выполнения операции.*

В данном отчете содержится описание всех шагов, осуществляемых системой при выводе таблицы из режима защищаемой, и статус их выполнения (рис. 21).

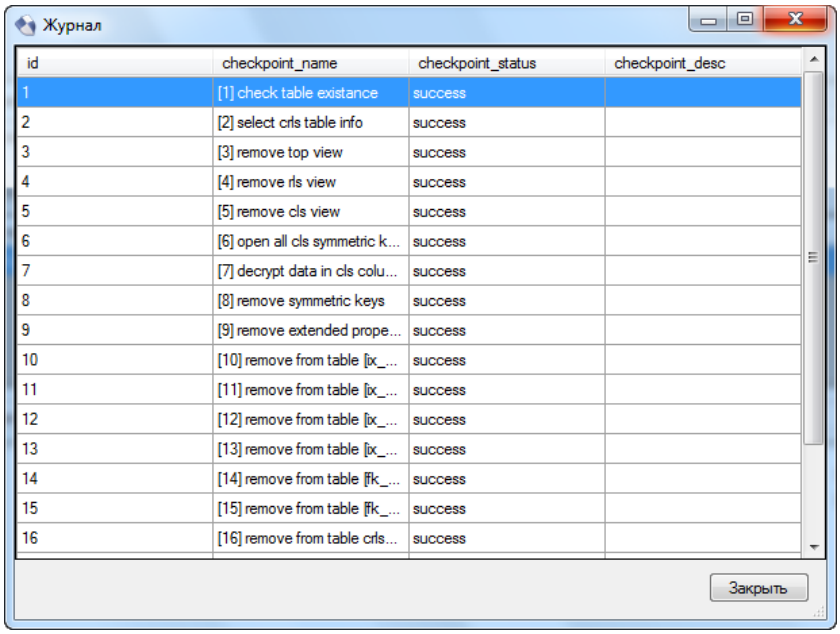


*Рис. 21. Отчет о ходе выполнения операции исключения*

## 2.4 Настройка логики (паттерны, разрешения)

### 2.4.1 Паттерны

Паттерны представляют собой условие (выражение), формируемое ответственным за разграничение доступа лицом, с помощью модуля администрирования системы CRLS. Основная задача правил - классифицировать контекст, при котором осуществляется доступ.

С помощью паттернов можно классифицировать:

- операцию:
  - выборка;
  - добавление;
  - удаление;
  - изменение.
- объект:
  - запись;
  - ячейка, удовлетворяющая необходимым условиям.
- субъект:
  - пользователь;
  - пользователь, входящий в роль, и т. д.
- все перечисленные выше комбинации.

Паттерны позволяют увеличить масштаб, при котором администратору необходимо осуществить настройку разграничения доступа. Разграничение доступа сводится не к ручной привязке разрешений к конкретным объектам, а к привязке разрешений к

правилам, классифицирующим контекст доступа, согласно требованиям безопасности. Система CRLS автоматически применяет правила и вычисляет разрешения в момент работы (доступа) с данными защищаемой таблицы.

Паттерны доступа CRLS-системы делятся на паттерны RLS, которые классифицируют строки таблицы и паттерны CLS, которые классифицируют ячейки таблицы.

#### 2.4.1.1 *Формирование паттерна RLS*

Нажмите кнопку меню **«Администрирование»** и выберите пункт **«Паттерны RLS»**. На **рис. 22** показана панель работы с паттернами RLS.

Напротив поля **«Таблица»** нажмите значок поиска **«…»**, чтобы выбрать таблицу, для которой будет сформирован паттерн RLS.

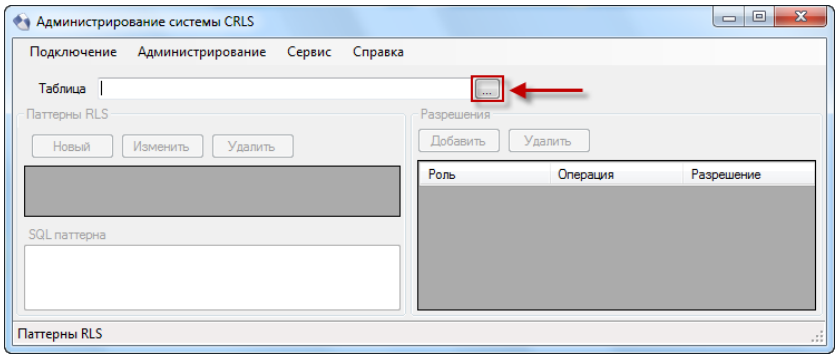


*Рис. 22. Добавление таблицы для формирования паттерна RLS*

В появившемся окне выберите таблицу и нажмите **«Ок»** (рис. 23).

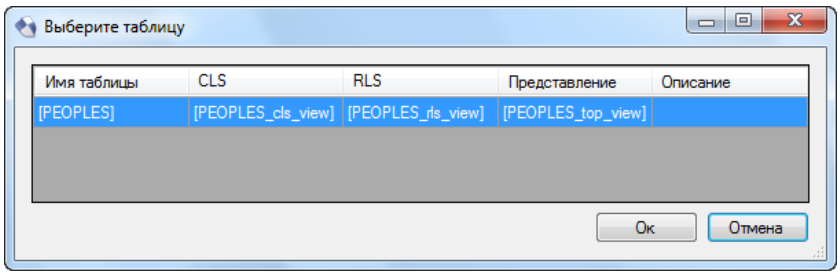


*Рис. 23. Выбор таблицы*

Затем в панели управления паттернами RLS нажмите **«Новый»** для создания нового паттерна, присвойте ему наименование и нажмите кнопку **«Ок»** (рис. 24).

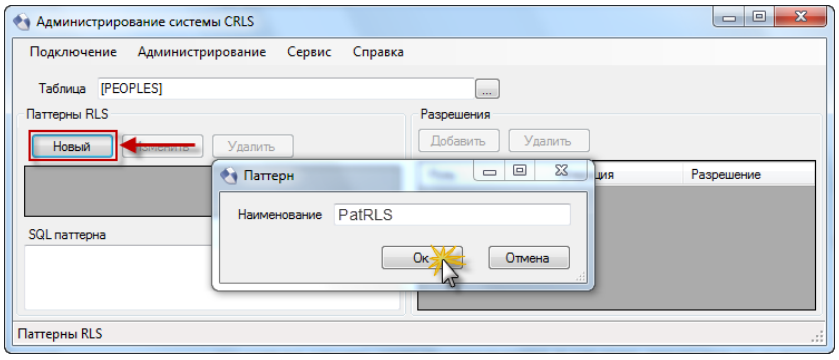


*Рис. 24. Создание нового паттерна RLS*

На **рис. 25** показана панель формирования выражения паттерна.

Формирование происходит в 3 этапа:

1) Выбор группы выражения;
2) Выбор условия операнда:
3) Добавление условия в выражение.

Выражение создаётся с целью классификации контекстов:

- контекст субъекта (пользователь, осуществляющий операцию);
- контекст данных (для классификации записей).
- контекст операции (insert, update);

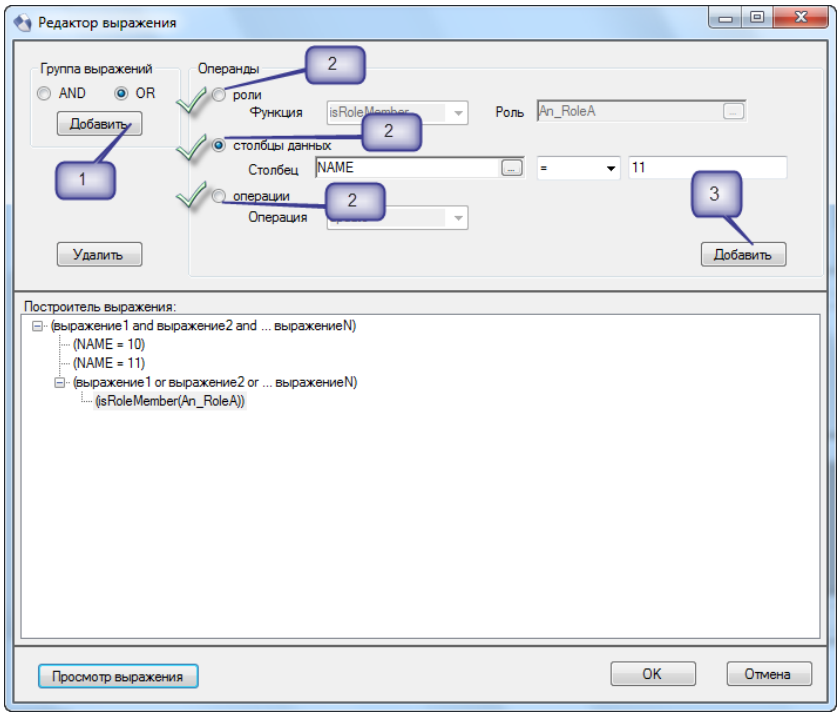


*Рис. 25. Формирование выражения паттерна RLS*

После формирования выражения нажмите кнопку **«Ок»**. Новый паттерн отобразится в панели управления паттернами RLS (рис. 26).

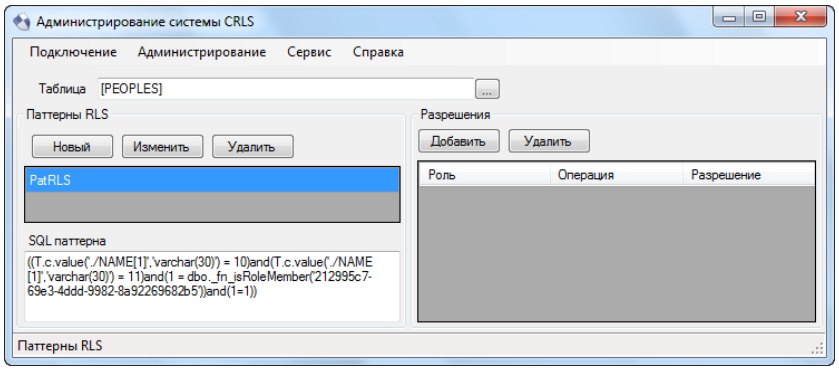


*Рис. 26. Просмотр паттернов RLS*

Зарегистрированные паттерны можно изменять и удалять.

### *2.4.1.2 Формирование паттерна CLS*

Нажмите кнопку меню **«Администрирование»** и выберите пункт **«Паттерны CLS»**.

На **рис. 27** показана панель работы с паттернами CLS. Чтобы добавить новый паттерн, нажмите кнопку **«Новый»** и заполните следующие поля:

- Наименование – наименование паттерна;
- Колонка – выбор колонки для паттерна;
- Ключ - ключ шифрования в момент создания правила (генерируется автоматически);
- Приоритет - приоритет паттерна (на одну ячейку может быть создано несколько паттернов; для шифрования / дешифрования будет выбран ключ из правила с наибольшим приоритетом).

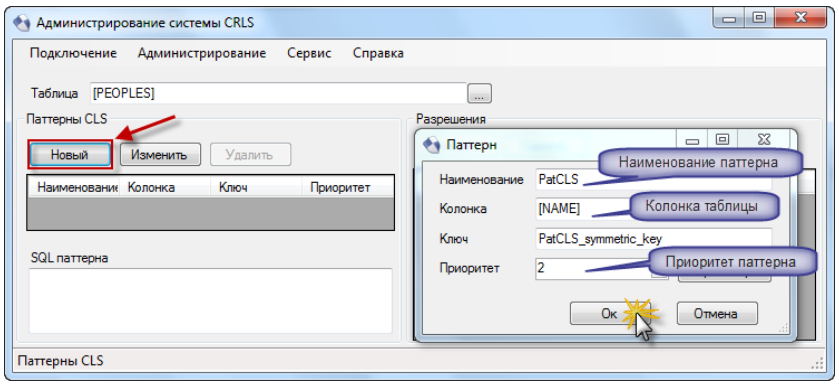


*Рис. 27. Создание паттерна CLS*

После заполнения необходимых полей нажмите кнопку **«Ок»**.

Формирование выражения паттерна CLS происходит аналогично формированию выражения паттерна RLS.

Зарегистрированные паттерны можно изменять и удалять.

## 2.4.2 **Разрешения**

Разрешения бывают двух типов:

- на уровне записи (уровень RLS):
  - роль (пользователь);
  - операция;
  - разрешено/запрещено.
- на уровне ячейки (уровень CLS):
  - роль (пользователь);
  - разрешено/запрещено.

Назначение разрешений осуществляется в панели управления паттернами.

Возможности пользователей при работе с таблицами баз данных будут определены тем, какие разрешения в итоге будут выставлены сформированным паттернам.

Для создания разрешения нужно выполнить следующие действия (рис. 28):

- добавить паттерн в роль;
- выбрать операцию (select, insert, delete, update) (для паттерна CLS операцию выбирать не нужно);
- установить разрешение.

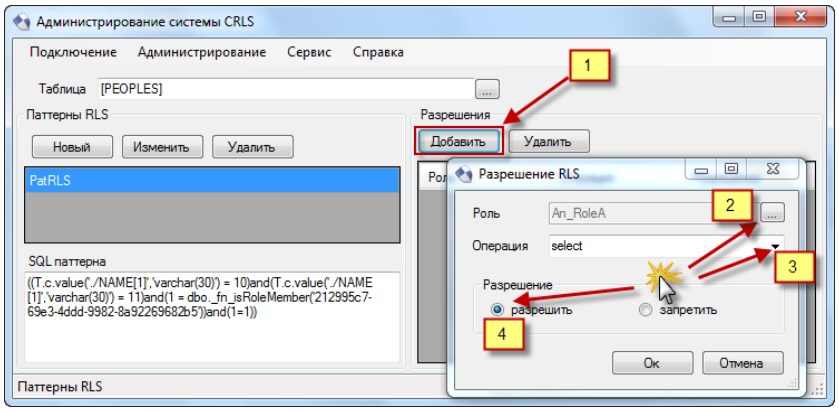


*Рис. 28. Добавление разрешения*

Созданное разрешение отобразится в правой части панели управления паттернами (рис. 29). Разрешения можно удалять.

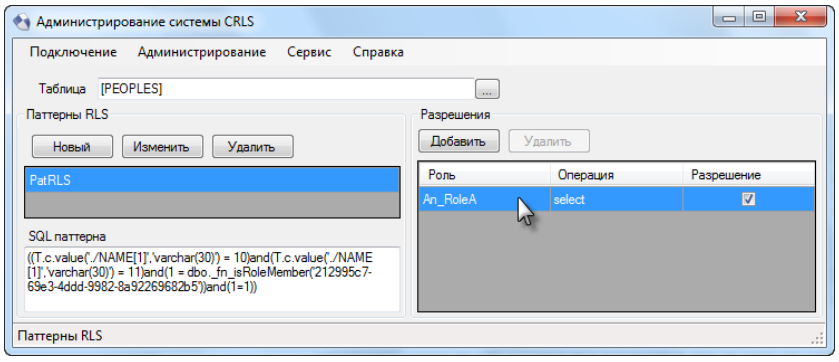


*Рис. 29. Добавление разрешения*

## 2.5 Дополнительные возможности

### 2.5.1 Меню «Сервис»

Меню «Сервис» предоставляет администратору Системы возможность проверить в режиме реального времени работоспособность настроенной политики разграничения доступа, а также сохранить текущие настройки и загрузить в систему сохранённые ранее настройки.

#### *2.5.1.1 Управление записями*

Данная опция позволяет администратору Системы посмотреть результаты настройки разрешений в Системе (рис. 30).

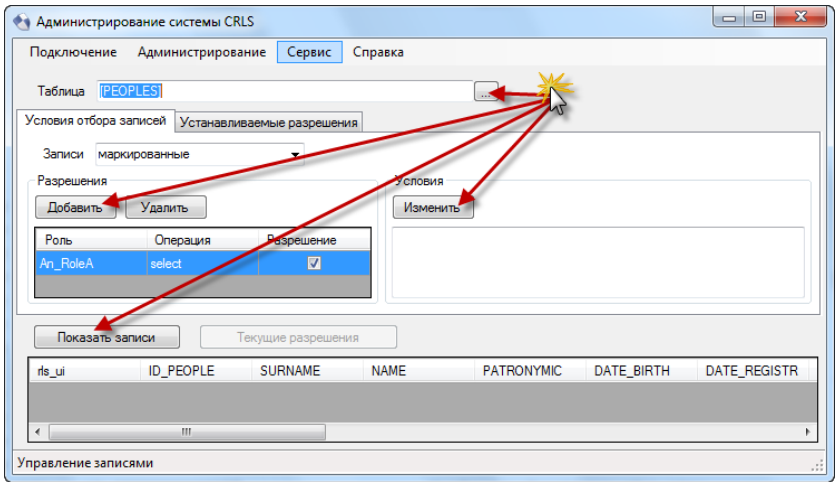


*Рис. 30. Управление записями*

Нажмите кнопку меню **«Сервис»** и выберите пункт **«Управление записями»**.

Чтобы посмотреть, как работает разрешение, выберите таблицу, нажав кнопку **«…»** напротив поля **«Таблица»**. Затем нажмите кнопку **«Добавить»** и выберите роль и её разрешение. Если требуется изменить условия выражения, нажмите кнопку **«Изменить»**. Чтобы посмотреть доступные записи таблицы для созданного разрешения, нажмите кнопку **«Показать записи»**.

#### *2.5.1.2 Динамический запрос*

Данная опция позволяет администратору Системы посмотреть записи, которые видны пользователям Системы (рис. 31).

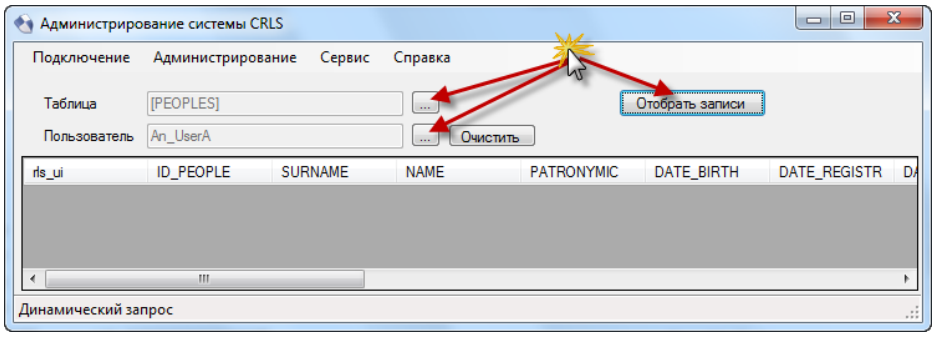


*Рис. 31. Динамический запрос*

Нажмите кнопку **«…»** напротив поля **«Таблица»** и выберите таблицу для работы. Затем нажмите кнопку **«…»** напротив поля **«Пользователь»** и выберите пользователя, от имени которого нужно посмотреть таблицу. Далее нажмите кнопку **«Отобрать записи»**, чтобы посмотреть доступные записи для пользователя.

### *2.5.1.3 Сериализация настроек*

Данная опция позволяет сохранять настройки политики разграничения доступа, сформированные для Системы, а также загружать в Систему сохранённые ранее настройки.

Чтобы сохранить текущие настройки, нажмите кнопку меню **«Сервис»** и выберите пункт **«Сериализация настроек»**.

В появившемся окне (рис. 32) поставьте маркер на **«Выгрузка»**, напротив поля **«Сохранить в файл»** нажмите значок **«…»** и укажите каталог, в который требуется сохранить файл настроек (предварительно присвоив ему наименование).

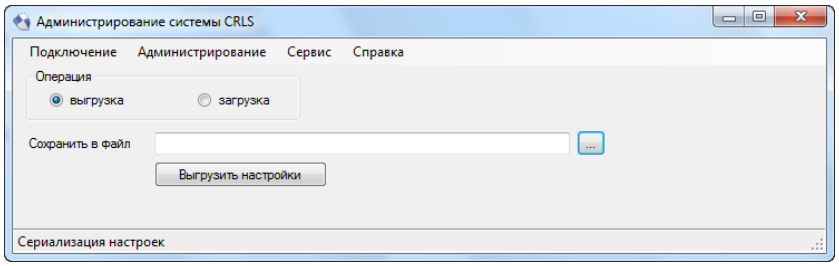


*Рис. 32. Сохранение настроек*

После выбора каталога для сохранения в панели Сериализации настроек нажмите кнопку **«Выгрузить настройки»**. На экране появится окно об успешном сохранении (рис. 33).

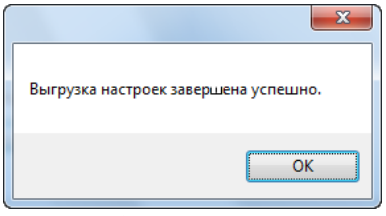


*Рис. 33. Сохранение настроек*

Чтобы загрузить в Систему сохранённый ранее файл настроек, нажмите кнопку меню **«Сервис»** и выберите пункт **«Сериализация настроек»**.

В появившемся окне (рис. 34) поставьте маркер на **«Загрузка»**, выберите каталог, откуда будет произведена загрузка файла настроек, выберите таблицу, для которой требуется применить настройки, и нажмите **«Загрузить для таблицы»**.

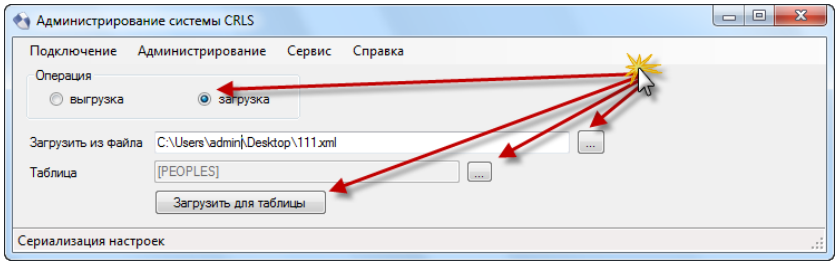


*Рис. 34. Загрузка настроек*

Далее появится окно (рис. 35) с отчётом о ходе выполнения процедуры сохранения настроек для таблицы.

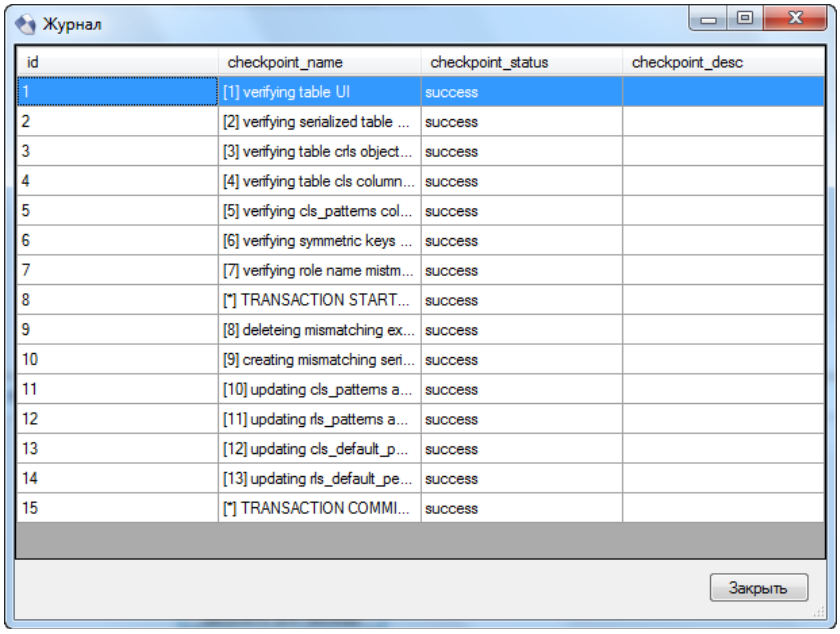


*Рис. 35. Отчёт о сохранении настроек*

# 3 РЕКОМЕНДАЦИИ ПО ОСВОЕНИЮ

## 3.1 Общие рекомендации

Для успешного освоения представленной в «Руководстве администратора» системы рекомендуется ознакомиться с документами:

- общее описание системы;
- описание контрольного примера.

## 3.2 Описание контрольного примера

База данных, содержащая контрольный пример предоставляется Заказчику на компакт-диске вместе с документацией.

# 4 ЗАКЛЮЧЕНИЕ

Политика безопасности определяется администратором данных и зависит от бизнес-логики, реализуемых функций и требований к безопасности. Система CRLS имеет механизмы, расширяющие возможности по управлению доступом к данным и их защите, обеспечивая гибкость настройки доступа к информации для разных пользователей.