Настройка безопасности

# Общие положения

## Структура системы безопасности

Структура системы безопасности состоит из следующих элементов:

1. Пользователи (Users)
2. Группы (Groups)
3. Роли (Roles)
4. Объекты безопасности (Security objects или SecObjects)
5. Типы доступа (AccessTypes)
6. Разрешения (Grants)

Все элементы позволяют хранить в себе следующую информацию:

### Пользователи

1. Логин (обязательно, должно быть уникальным)
2. Пароль (не обязательно для пользователей Active Directory)
3. Адрес электронной почты
4. Отображаемое имя

### Группы

1. Имя группы (обязательно, должно быть уникальным)
2. Описание

### Роли

1. Имя роли (обязательно, должно быть уникальным)
2. Описание

### Объект безопасности

1. Имя объекта (обязательно, должно быть уникальным)
2. Описание

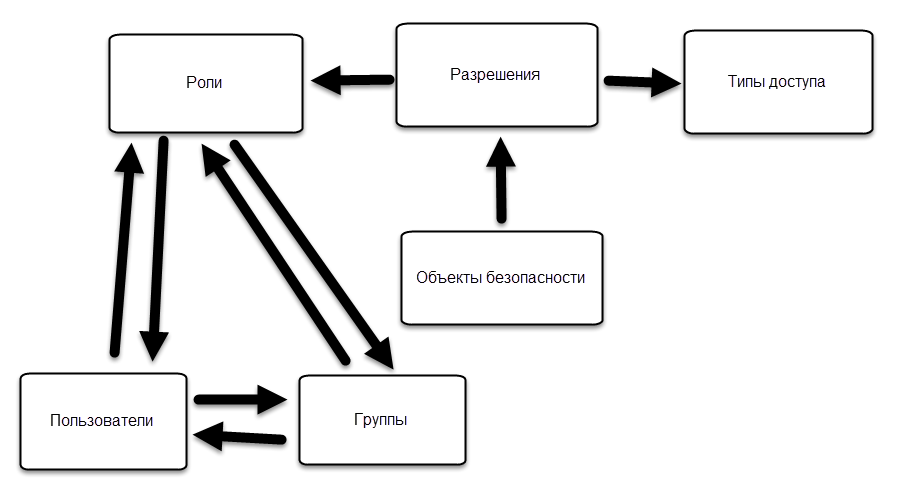
### Типы доступа

1. Имя типа доступа (Этот элемент недоступен для редактирования и предназначен исключительно для внутреннего использования системой)

### Разрешения

1. Ссылка на объект безопасности
2. Ссылка на роль
3. Ссылка на тип доступа

## Схема информационных потоков



## Принцип работы системы

Для настройки системы безопасности в первую очередь нужно определить список ролей. К примеру, с информационной системой (ИС) работают три типа пользователей: пользователи, которые вводят данные, пользователи, которым нужен только контроль и просмотр данных, пользователи, которые отвечают за настройку ИС. Таким образом, можно создать три роли, соответственно: «Оператор ввода», «Руководитель», «Администратор системы». Для каждой из ролей необходимо настроить свой список доступа с указанием типов доступа и объектов безопасности.

Далее можно приступить к назначению пользователям и группам соответствующих ролей.

# Общий вид интерфейса

рис. 1.

Основным элементом управления на странице «Настройки безопасности» (рисунок 1) является командная строка. Настройка безопасности системы производится путем ввода в командной строке соответствующих команд и отправке их на сервер.

Для облегчения ввода команд в командной строке реализована интуитивно понятная и интерактивная система подсказок, облегчающая ввод команды, таким образом, что необязательно знать синтаксис всех команд.

# Синтаксис командной строки

Настройка безопасности осуществляется с помощью четырех команд:

1. Grant
2. Add
3. Set
4. Remove

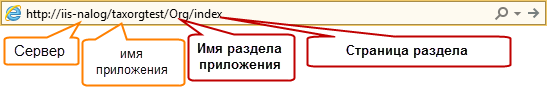
***Примечание****. В дальнейшем этот список может быть дополнен.*

## Grant

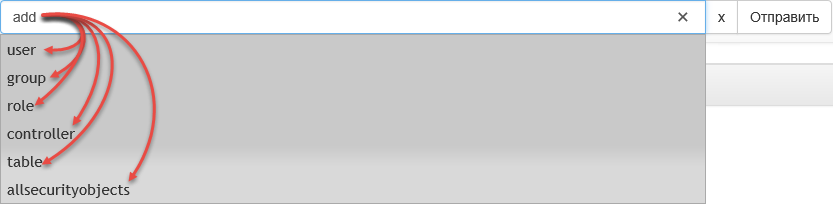
Предоставляет разрешения для роли по определенному типу доступа на выбранный объект безопасности

1. grant exec to <Имя роли> on <Имя раздела+Имя страницы раздела (КонтроллерДействие)>
2. grant <Команды доступа к хранилищам БД> to <Имя роли> on <Имя хранилища БД или псевдоним хранилища>

* <Имя роли> - Имя роли
* <Имя раздела+Имя страницы (КонтроллерДействие)> - Это сочетание двух последних команд адреса URL



## Add



1. add user <Логин пользователя> [Пароль] [email] [Отображаемое имя]

Если ИС настроена на работу с Windows пользователями необходимо ввести только имя пользователя в формате domain\login, пример:

*Пример добавления пользователя Windows*

**add user slv\admin**

*Пример добавления простого пользователя с паролем*

**add user login $trongP@$$w0rd** [**login@gmail.com**](mailto:login@gmail.com) **«Иванов Василий Петрович»**

***Примечание****. В данном примере отображаемое имя закрыто в кавычках, т.к. состоит из нескольких слов*

1. add group <Имя группы> [Описание]

***Примечание****. Если описание состоит из нескольких слов необходимо закрывать его в кавычки.*

Примеры:

*Пример добавления группы:*

**add group Users**

*Пример добавления группы с описанием:*

**add group Администраторы «Группа администрирования»**

1. add role <Имя роли> [Описание]

***Примечание****. Если описание состоит из нескольких слов необходимо закрывать его в кавычки.*

Примеры:

*Пример добавления роли*

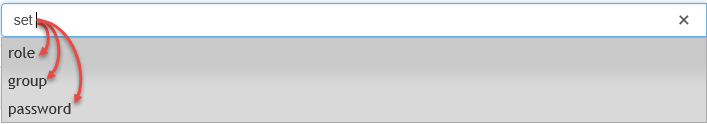
**add group Оператор**

*Пример добавления роли с описанием*

**add group Администраторы «Роль администрирования»**

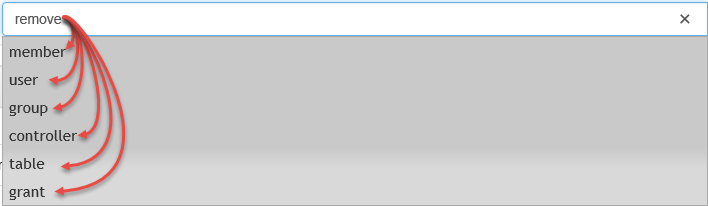
1. ~~add table <Имя хранилища>, add controller <Имя контроллера>~~ - не рекомендуется использовать эти команды, вместо это рекомендуется использовать команду **add allsecurityobjects** - эта команда добавляет в хранилище информацию по всем используемым в ИС объектам безопасности

## Set



1. set role <Имя роли> to <Логин пользователя>
2. set group <Имя группы> to <Логин пользователя>
3. set password <Пароль> for user <Логин пользователя>

## Remove



1. remove member <Логин пользователя> from <Имя роли>
2. remove user <Логин пользователя> from <Имя группы>

***Примечание****. Если после слова* ***from,*** *в подсказке, ничего не появляется, то это означает, что для данного пользователя не назначено ни одной роли (группы).*

1. remove group <Имя группы>
2. remove controller <Имя КонтроллерДействие>
3. remove table <Имя хранилища>
4. remove grant …

***Примечание****. Для команды* ***remove grant*** *смотрите синтаксис команды* ***grant****.*