

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ
программного комплекса «ОКиДОКи»
версия 2.4

Модуль «Администратор»

Ярославль

2020

Оглавление

1	Общие сведения.....	3
1.1	Что такое «ОКиДОКи».....	3
1.2	Учетная запись суперпользователя.....	3
2	Управление доступом.....	4
2.1	Подраздел «Роли».....	4
2.2	Подраздел «Учетные записи».....	4
3	Справочники.....	6
4	Официальная информация о продукте.....	7

1 Общие сведения

1.1 Что такое «ОКиДОКи»

«ОКиДОКи» — модульная система автоматизированного создания и управления документами в области информационной безопасности.

Модуль «Администратор» позволяет:

- управлять правами доступа к модулям программного комплекса «ОКиДОКи» и их разделам;
- редактировать справочники, общие для всех организаций, работающих с системой.

1.2 Учетная запись суперпользователя

После установки программного комплекса «ОКиДОКи» вход в систему возможен от имени учетной записи суперпользователя с логином `admin` и паролем `admin`.

2 Управление доступом

2.1 Подраздел «Роли»

Управление доступом реализовано на основе ролевой модели.

Права доступа можно разграничить по модулям, их разделам (верхнее меню) и подразделам (левое меню).

Кроме того, можно разрешить доступ только к конкретным организациям (в случае, если с программным комплексом «ОКиДОКи» работают сразу несколько различных организаций), а в пределах организации — только к конкретным территориальным подразделениям. Последнее может быть удобно, когда нужно дать пользователю право ведения журнала по конкретному территориальному подразделению. Следует иметь в виду, что ограничение прав доступа пользователя конкретными территориальными подразделениями не ограничивает его в доступе к разделу «Документы» и разделу «Ввод данных».

Скриншот интерфейса «ОКиДОКи» в разделе «Роли». В таблице перечислены роли и их права доступа к различным модулям и объектам. В строке «Разрешить доступ только к следующим объектам:» выделено красным кругом.

Роли	Полный список	✓	✓
Учетные записи	Модуль "Документы"	✓	✓
	Сводные данные	✓	✓
	Основные документы	✓	✓
	Уведомление в Роскомнадзор	✓	✓
	Классификация информационных систем	✓	✓
	План внутренних проверок	✓	✓
	Назначение ответственных	✓	✓
	Информационные системы персональных данных	✓	✓
	Системы, классифицируемые по приказу ФСТЭК России № 17	✓	✓
	Готовность к проверкам	✓	✓
	Сводные данные	✓	✓
	Роскомнадзор (персональные данные)	✓	✓
	ФСТЭК России (техническая защита информации)	✓	✓
	ФСБ России (применение криптосредств)	✓	✓

! Если не указан ни один конкретный разрешенный объект, данная роль будет иметь право доступа ко всей базе данных

Разрешить доступ только к следующим объектам:

Организация	Разрешенные объекты

Готово Отмена Для сохранения данных нажмите "Готово" "Отмена" вернет все значения к исходным

2.2 Подраздел «Учетные записи»

После того, как роли будут созданы, каждой учетной записи пользователя системы должна быть сопоставлена одна или несколько ролей. Считается, что пользователь имеет право доступа, если хотя бы одна из назначенных ему ролей

имеет соответствующее право доступа.

Рекомендуется связывать учетные записи с сотрудниками, информация о которых введена в базу данных. Если база данных еще не заполнена, можно сразу добавлять новых сотрудников в базу данных при создании учетных записей.

3 Справочники

В этом разделе можно редактировать некоторые справочники в части значений, общих для всех организаций, работающих с системой.

4 Официальная информация о продукте

Правообладатель: общество с ограниченной ответственностью «Стандарт безопасности» (подтверждено свидетельством о государственной регистрации программы для ЭВМ № 2018665012).

Адрес правообладателя: 150047, г. Ярославль, ул. Угличская, д. 39В.

Официальный сайт: www.yarsec.ru.

Телефон для связи по вопросам приобретения продукта: (4852) 587-300.

Электронный адрес службы технической поддержки и консультирования по работе с продуктом: oki@yarsec.ru.

Телефон службы технической поддержки и консультирования по работе с продуктом: (4852) 587-300 (доб. 181).