

ПРОГРАММА ДЛЯ ЭВМ «СИБИ»
СО ВСТРОЕННЫМИ СРЕДСТВАМИ
ЗАЩИТЫ ИНФОРМАЦИИ

Инструкция пользователя

Листов 16

2019

СОДЕРЖАНИЕ

1. Назначение программы.....	3
1.1 Наименование	3
1.2 Состав ПО «СИБИ».....	3
1.3 Функциональные возможности.....	3
2. Установка программы.....	5
2.1 Программное обеспечение, необходимое для функционирования программы	5
2.2 Установка и настройка ПО.....	5
3. Управление учетными записями в «СИБИ».....	8
3.1 Формирование списка пользователей в «СИБИ»	8
3.2 Активация и назначение ролей пользователям в «СИБИ»	8
4. Выполнение программы	10
4.1 Сценарий взаимодействия пользователя с ПО «СИБИ»	10
4.2 Вход в ПО «СИБИ»	10
4.3 Интерфейс ПО «СИБИ».....	10
4.4 Главная страница.....	11
4.5 Назначение прав пользователю на папку/файл.....	12
4.6 Доступ к файлам и папкам через webDAV.....	14
Перечень сокращений.....	16

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1 Наименование

ПО «СИБИ» предназначено для хранения, обработки (изменения, дополнения, удаления) и обеспечения безопасного удаленного и мобильного доступа к информации конфиденциального характера, обеспечивающей работу с файловыми ресурсами с использованием привычного пользователям представления.

1.2 Состав ПО «СИБИ»

Подсистема управления объектами «СИБИ»;

- Модули формирования файловой структуры;
- Модули работы с объектами «СИБИ».
- Подсистема отчетности;
 - Модули формирования реестров и отчетных форм по заданным параметрам.
- Подсистема уведомлений;
 - Модули формирования и отправки сообщений о событиях;
- Подсистема защиты информации;
- Справочная подсистема;
 - Модули предоставления пользователям базы знаний по работы в «СИБИ».
- Подсистема поиска;
 - Модули реализующие функции полнотекстового поиска.
- Подсистема совместной работы;
 - Модули реализующие функции совместной работы пользователей.

1.3 Функциональные возможности

ПО «СИБИ» представляет собой информационную систему, предназначенную для хранения и обработки информации конфиденциального

характера, в том числе персональных данных (ПДн).

В ПО «СИБИ» определены следующие роли пользователей:

Привилегированные пользователи:

- Администратор прикладного программного обеспечения (далее - Администратор ППО).

Непривилегированные роли пользователей:

- Куратор ФР;
- Пользователь.

На ПО «СИБИ» возложено решение следующих задач:

- Обеспечение возможности хранения и обработки конфиденциальных электронных документов, в том числе ПДн;
- Организация совместной работы с файловыми ресурсами;
- Обработка (изменение, дополнение, удаление) и обеспечение безопасного удаленного и мобильного доступа к информации конфиденциального характера, в том числе ПДн, обеспечивающей работу с файловыми ресурсами с использованием привычного пользователям представления.

2. УСТАНОВКА ПРОГРАММЫ

2.1 Программное обеспечение, необходимое для функционирования программы

Для установки на сервера ПО «СИБИ» под управлением Astra Linux SE, версии 1.6, требуется установка пакетов:

- OpenJRE – среда выполнения кода ПО «СИБИ»;
- Apache2 – web-сервер – обеспечивает работу с сертификатом SSL (HTTPS), распределение запросов между серверами приложений с целью балансировки нагрузки на них;
- Apache Tomcat – web-сервер;
- PostgreSQL – СУБД;

Идентификация и аутентификация пользователей осуществляется по доменным учетным записям средствами Active Directory.

2.2 Установка и настройка ПО

1. Системный администратор выполняет установку ОС Astra Linux Special Edition 1.6 «Смоленск» на сервере. Установка производится в соответствии с Руководством администратора ОССН «Astra Linux Special Edition».

2. Настройка аутентификации в ОС с использованием доменных УЗ и групп. Установка keytab файла для аутентификации в ОС.

3. При прохождении процедуры установки необходимо дополнительно выбрать установку веб-сервера Apache 2.4.25? PostgreSQL 9.6.

4. Системный администратор на сервере приложений указывает настройки сетевых интерфейсов, в файле /etc/resolv.conf указывает адрес DNS сервера в формате <nameserver> <ip_address>.

5. Системный администратор настраивает/проводит:

- а. время на сервере;
- б. сервисные и персонифицированные УЗ, создается также УЗ в БД для приложения и репликации;
- в. установку дополнительных пакетов из дистрибутива Astra Linux SE необходимых для работоспособности приложения (Java OpenJRE 1.8, krb5-user, libapache2-mod-auth-gssapi, at);

- d. установку из файлового архива «СИБИ» командой `tar -zxvf sibi.tar.gz -C /opt/sfolder-app/;`
 - e. установку keytab файла для веб-сервера для функционирования SSO;
 - f. конфигурирование virtualhost и включение модулей apache


```
#sudo a2enmod ssl headers rewrite auth_gssapi proxy proxy_http
proxy_balancer session session_cookie
```
 - g. установку ServerName и SSL сертификата для соответствующего virtualhost на сервере. Установка производится в соответствии с Руководством администратора ОССН «Astra Linux Special Edition» (разделы 6.1 и 17.3 соответственно);
 - h. установку gotp для управления активацией доменных пользователей (распаковка архива gotp.tar.gz в папку /usr/local/gotp);
 - i. ввод сервера в домен с помощью сервиса sssd;
 - j. ldap аутентификацию для доменных УЗ.
6. Администратор ППО проводит настройку «СИБИ», включающую:
- a. настройку gotp для управления активацией доменных пользователей;
 - b. настройку (конфигурационный файл в соответствие со средой, gotp, почта) и запуск приложения через atd.
1. Системный администратор настраивает:
- a. создание БД folders;
 - b. привязку начальной УЗ Администратора БД к привилегированному пользователю `update users set username = 'user' where username = 'admin';`
 - c. проверку доступности БД для локальных подключений `app psql -h localhost -d folders.`

После подключения Администратору ППО отображается web-интерфейс «СИБИ» в соответствии с установленными полномочиями.

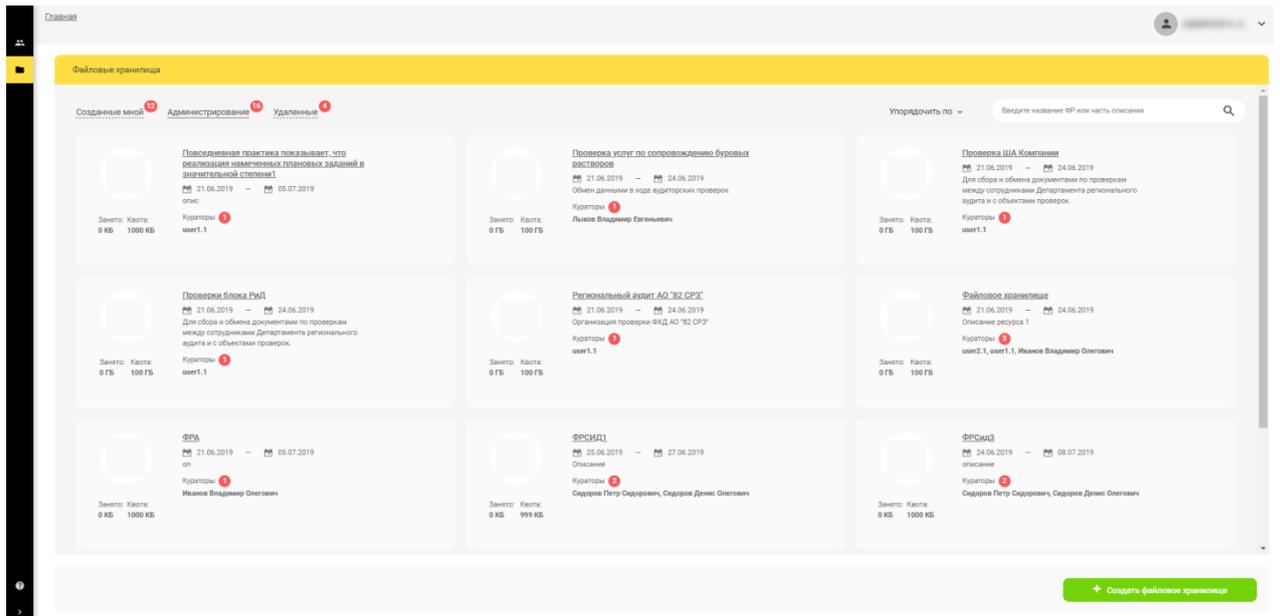
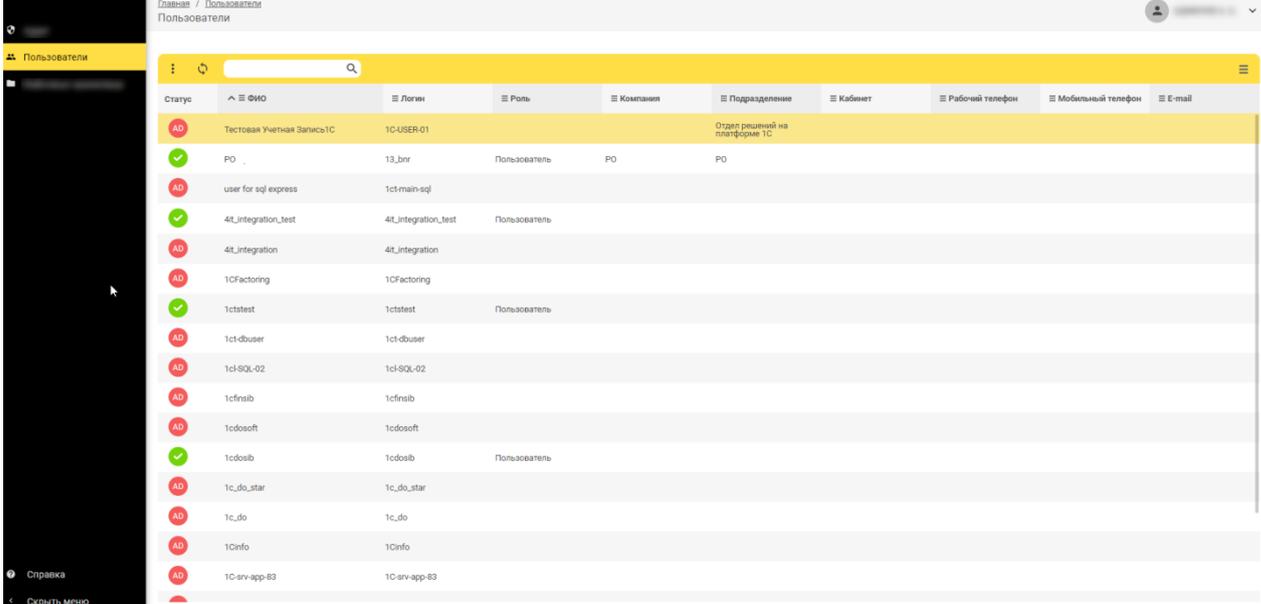


Рисунок 1 - Web-интерфейс «СИБИ»

3. УПРАВЛЕНИЕ УЧЕТНЫМИ ЗАПИСЯМИ В «СИБИ»

3.1 Формирование списка пользователей в «СИБИ»

1. Активные пользователи «СИБИ» (элемент  во вкладке «Пользователи»).
2. Неактивные пользователи «СИБИ» (элемент  во вкладке «Пользователи»).



Статус	ФИО	Логин	Роль	Компания	Подразделение	Кабинет	Рабочий телефон	Мобильный телефон	E-mail
	Тестовая Учетная Запись 1С	1C-USER-01			Отдел решений на платформе 1С				
	PO .	13_bnr	Пользователь	PO	PO				
	user for sqj express	1ctmain-sqj							
	4it_integration_test	4it_integration_test	Пользователь						
	4it_integration	4it_integration							
	1CFactoring	1CFactoring							
	1ctstest	1ctstest	Пользователь						
	1ctdbuser	1ctdbuser							
	1cSQL-02	1cSQL-02							
	1cfnalb	1cfnalb							
	1cdosoft	1cdosoft							
	1cdosib	1cdosib	Пользователь						
	1c_do_star	1c_do_star							
	1c_do	1c_do							
	1Cinfo	1Cinfo							
	1C-avr-app-83	1C-avr-app-83							

Рисунок 2 – Список пользователей «СИБИ»

3.2 Активация и назначение ролей пользователям в «СИБИ»

Для активации пользователя в «СИБИ» пользователю с ролью «Администратор ППО» необходимо:

1. На вкладке «Пользователи» выбрать пользователя.
2. В столбце «Статус» нажать левой кнопкой мыши (далее - ЛКМ) на элемент  .
3. Выбрать роль пользователя из выпадающего списка и нажать кнопку «Подтвердить».
4. Пользователь становится активным в «СИБИ». При нажатии цвет элемента  меняется на  и в Системе выводится всплывающее окно «Пользователь успешно создан».

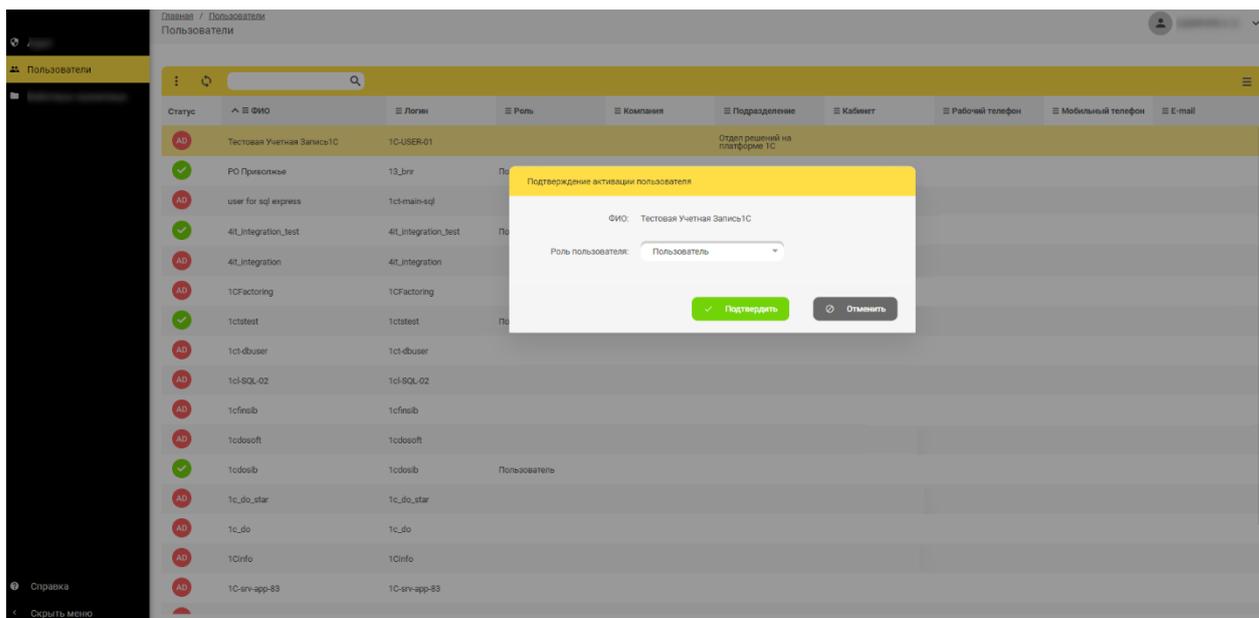


Рисунок 3 – Добавление пользователей «СИБИ»

4. ВЫПОЛНЕНИЕ ПРОГРАММЫ

4.1 Сценарий взаимодействия пользователя с ПО «СИБИ»

К работе с Системой допускаются пользователи, ознакомленные с настоящей Инструкцией пользователя.

ПО «СИБИ» предназначена для хранения, обработки информации конфиденциального характера, в том числе ПДн, обеспечивающей работу с файловыми ресурсами с использованием привычного пользователям представления.

Пользователю запрещено распечатывание файлов любым способом, отличным от печати выгруженного файла.

В ПО «СИБИ» пользователю доступно выполнение операций только в соответствии с назначенной ролью.

При необходимости временно покинуть рабочее место пользователь обязан заблокировать свой сеанс работы средствами операционной системы. При завершении работы в ПО «СИБИ» пользователь обязан закрыть все вкладки браузера, отображающие страницы сайта ПО «СИБИ».

4.2 Вход в ПО «СИБИ»

С целью начала работы с ПО «СИБИ» пользователь должен выполнить следующие действия:

Доступ пользователей к Системе осуществляется в следующем порядке:

- аутентификация пользователя на своей рабочей станции с использованием своей доменной учетной записи;
- Пользователь автоматически идентифицируется в Системе на основе доменных учетных записей (механизм Single Sign-On (SSO)).

После перехода по адресу ресурса пользователю отображается web-интерфейс ПО «СИБИ» в соответствии с установленными полномочиями.

4.3 Интерфейс ПО «СИБИ»

Интерфейс ИС «СИБИ» интуитивно понятен для пользователя.

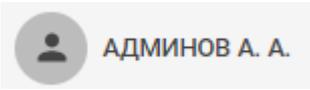
4.4 Главная страница

Главная страница ПО «СИБИ» содержит следующие элементы:

- «Рабочий стол» - для перехода к прочим функциям Системы с минимальным числом шагов;
- «Верхняя сервисная панель» - содержит информацию о Пользователе, вошедшем в Систему.

4.4.1 Верхняя сервисная панель

Верхняя сервисная панель содержит следующие элементы:

-  - кнопка «Вызов меню пользователя».

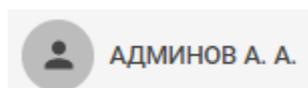


Рисунок 4 - Верхняя сервисная панель

4.4.2 Кнопка «Вызов меню пользователя»

Кнопка «Вызов меню пользователя» отображает имя пользователя, обеспечивает разворачивание/сворачивание пользовательского меню.

Настройки уведомлений

Настройки рабочего стола

Последний вход в систему

Выйти

Рисунок 5 - Пользовательское меню

Пользовательское меню содержит элементы:

- **Настройки уведомлений** - кнопка «Настройки уведомлений». Обеспечивает переход в настройки профиля пользователя;
- **Настройки рабочего стола** - кнопка для настройки отображения рабочего

стола;

- **Последний вход в систему** - кнопка для вывода информации о последнем входе в Систему пользователя;
- **Выйти** - кнопка «Выйти». Обеспечивает переход на страницу с сообщением о завершении сеанса работы.

4.5 Назначение прав пользователю на папку/файл

Для назначения прав пользователю на какую-либо папку/файл, пользователю с ролью «Куратор», необходимо:

- 1) Перейти на страницу «Файловые хранилища».
- 2) Открыть файловый ресурс, в котором необходимо назначать права пользователю на папку/файл.
- 3) В файловом ресурсе перейти во вкладку «Управление доступом» (см. рисунок 6).
- 4) В левой части экрана выбрать папку, на которую необходимо задать права.
- 5) В правой части экрана, в окне «Настройка прав доступа» нажать кнопку «Добавить» (см. рисунок 7).
- 6) В открывшемся окне «Добавление пользователя в группу», с помощью строки поиска, найти необходимого пользователя или группу пользователей.
- 7) Добавить пользователей или группу пользователей и нажать кнопку «Создать» (см. рисунок 8).
- 8) В окне «Настройка прав доступа» нажать на запись пользователя с правами и нажать на «красный круг» напротив права «Чтение» (см. рисунок 9).

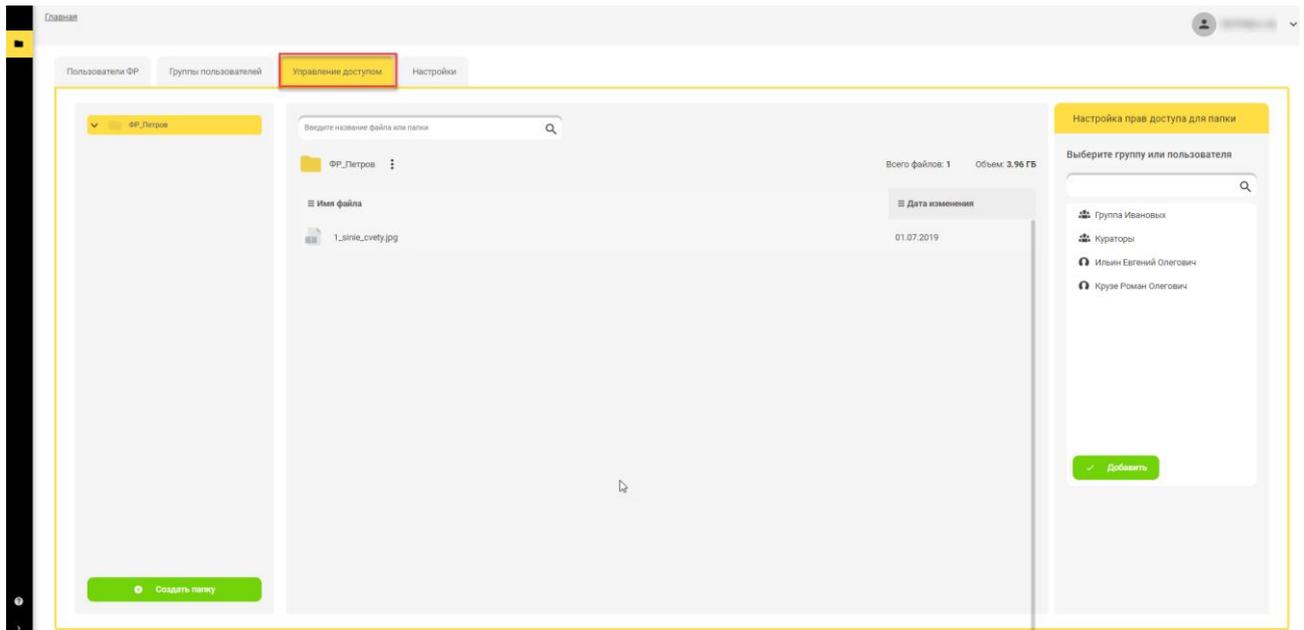


Рисунок 6 – Управление доступом

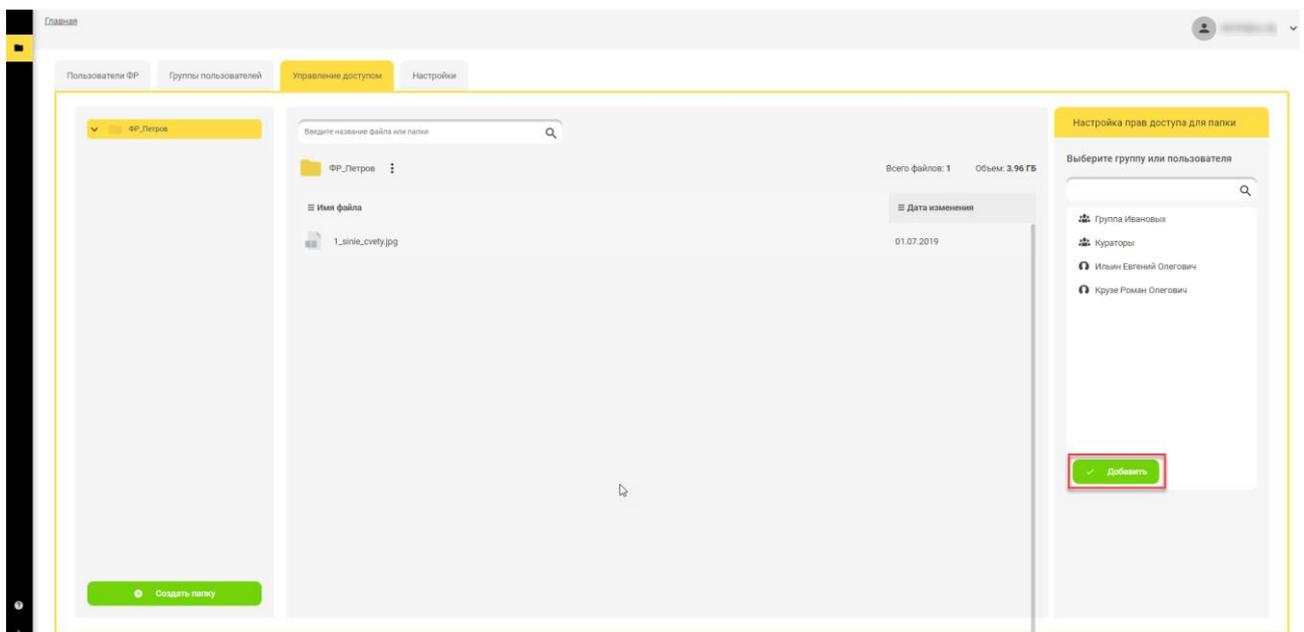


Рисунок 7 – Настройка прав доступа

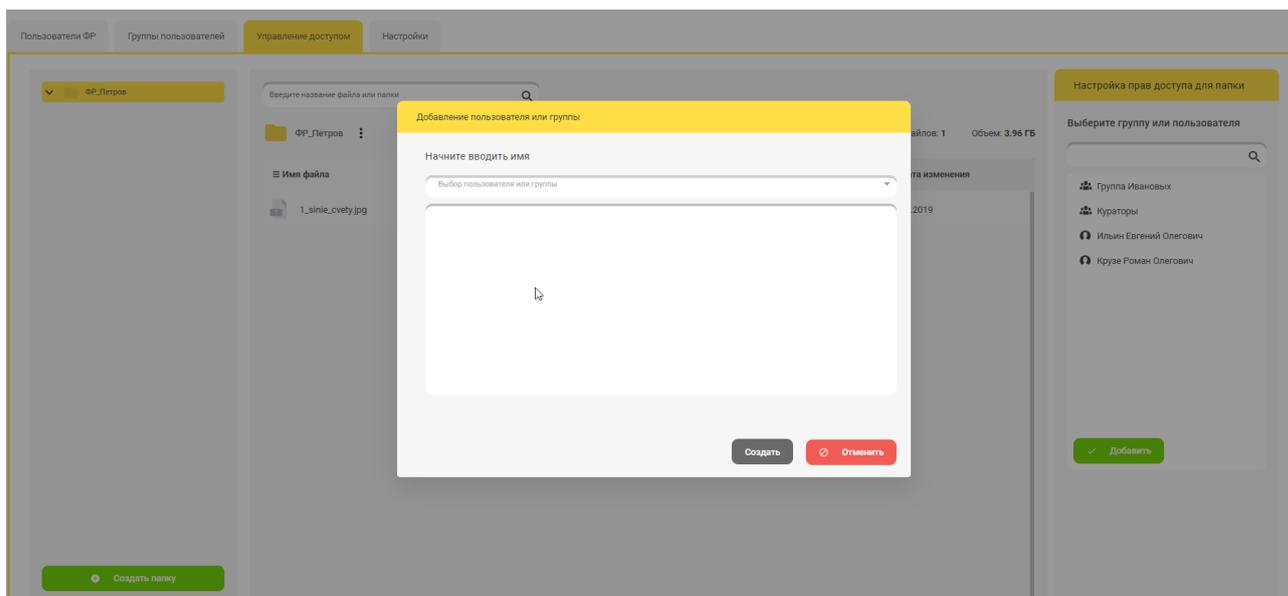


Рисунок 8 – Добавление пользователя или группы

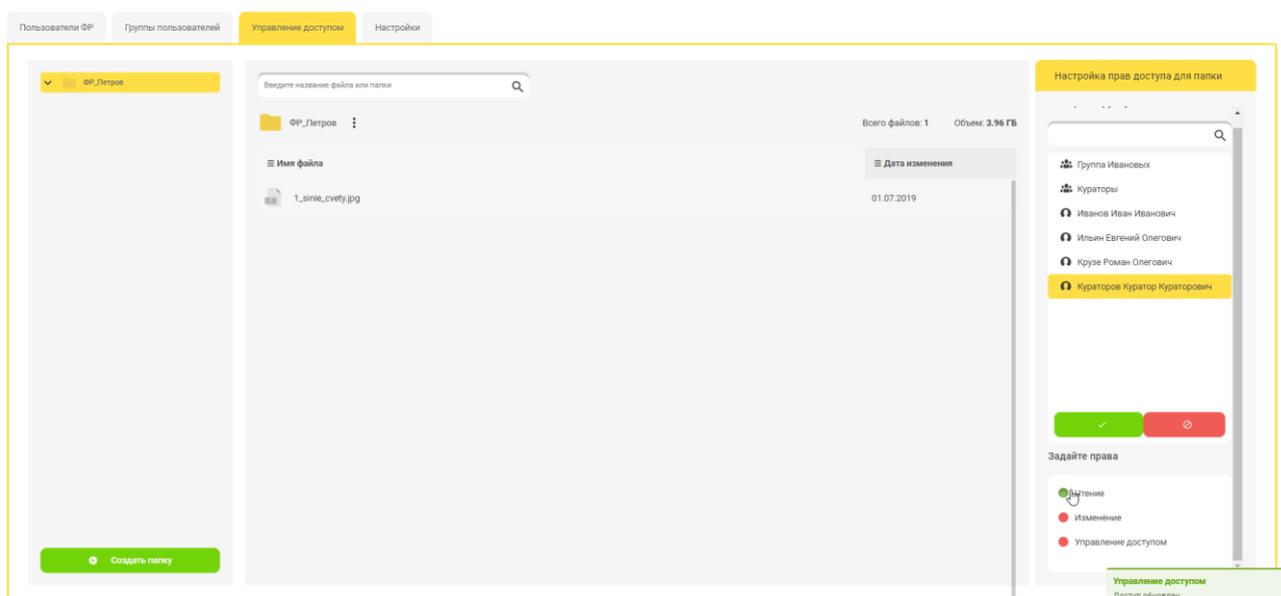


Рисунок 9 – Назначение прав пользователю

4.6 Доступ к файлам и папкам через webDAV

Для доступа к папкам и файлам файлового ресурса через webDAV, к которому есть доступ, пользователю с ролью «Куратор» необходимо:

- 1) Перейти в корневую папку ФР, к которому имеется доступ (изменение).
- 2) Ввести логин и пароль¹ пользователя.
- 3) Добавить новый элемент в ФР (см. рисунок 10).

¹ Поле «Логин» чувствительно к регистру. Вводить логин следует в строгом соответствии с записью в AD

- 4) На Главной странице ПО «СИБИ» открыть навигационное меню.
- 5) Перейти на страницу «Файловые хранилища».
- 6) Открыть ФР, в которое был добавлен новый элемент.
- 7) Открыть вкладку «Управление доступом». В левом окне, открыть корневую папку. Созданная папка из шага 3 отображается в интерфейсе ПО «СИБИ» (см. рисунок 11).

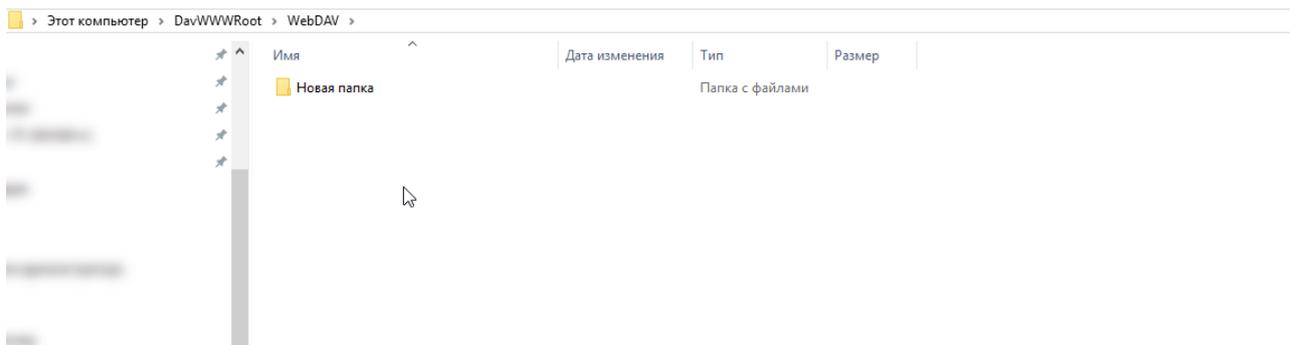


Рисунок 10 – Создание новой папки в ФР

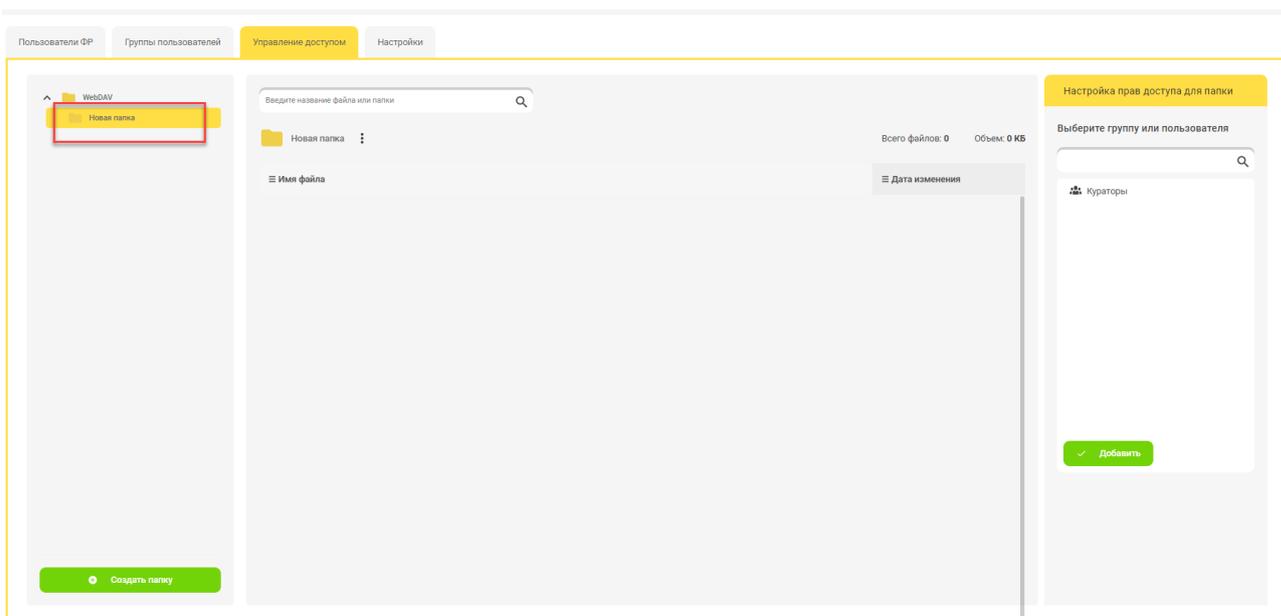


Рисунок 11 – Созданная папка в ФР

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Расшифровка
АРМ	Автоматизированное рабочее место
ИБ	Информационная безопасность
ИТ	Информационные технологии
ОС	Операционная система
ОГ	Общество Группы
ПО «СИБИ»	Программа для ЭВМ «СИБИ».
ПК	Персональный компьютер
УЗ	Учетная запись
ФИО	Фамилия, имя, отчество
AD	Active Directory (Активный каталог)
eToken	Персональное средство аутентификации в виде USB-ключей и смарткарт