УТВЕРЖДЕН

RU.23578167.00001-01-ЛУ

ЦФТ-Технологическое ядро со встроенными средствами защиты

РУКОВОДСТВО АДМИНИСТРАТОРА

RU.23578167.00001-01 36

Листов 86

2021

Подп. и дата

Инв. № дубл.

Взаим. инв. №

Подп. и дата

Инв. № подл.

Оглавление

Аннотация 5

1 Термины и определения 6

2 Назначение и условия применения 7

2.1. Область применения 7

2.2. Краткое описание возможностей 7

2.3. Основные компоненты 7

3 Организационно-распорядительные меры по приемке программного обеспечения 8

4. Установка и настройка серверной части 9

4.1. Установка и настройка базы данных Postgres 9

4.1.1. Создание технических пользователей и ролей 9

4.2. Настройка системы доступа 10

4.2.1. Общие принципы организации доступа 10

4.2.2. Конфигурация файла настроек системы доступа 13

4.2.3. Запуск АРМ «Администратор доступа» 14

4.3. Установка лицензии 15

4.4. Установка и настройка Сервера приложений 15

4.4.1. Системные требования 15

4.4.2. Настройка параметров конфигурационных файлов 16

4.4.3. Настройка опциональных параметров 26

4.4.4. Настройка аутентификации через ADFS + WAP 26

4.4.5. Особенности работы с FIO 29

4.4.6. Настройка Сервера приложений 30

4.4.7. Проверка корректности установки Сервера приложений 32

4.4.8. Шифрование паролей 32

4.4.9. Синхронизация групп пользователя 33

4.4.10. Настройка внешнего пула соединений 38

4.4.11. Создание хранилища с сертификатами 38

4.5. Сервис заданий 39

4.5.1. Настройка сервиса серверов заданий Сервера приложений 40

5. Установка и настройка клиентской части ... 42
5.1. Системные требования ... 42
5.1.1. Поддерживаемые версии операционных систем ... 42
5.1.2. Программное обеспечение, устанавливаемое на рабочие станции ... 43
5.2. Установка Рабочего места Оператора ... 44
5.2.1. Установка и удаление в «тихом» режиме ... 46
5.3. Установка АРМов ... 46
5.3.1. Установка АРМов в каталог файлового сервера ... 47
5.3.2. Установка АРМов на рабочей станции пользователя ... 47
6. Эксплуатация и обслуживание Системы ... 48
6.1. Управление серверными компонентами системы ... 48
6.2. Управление базой данных ... 48
7. Управление учетными записями пользователя ... 50
7.1. Интерфейс АРМ «Администратор доступа» ... 50
7.1.1. Основное меню ... 50
7.1.2. Поиск и сортировка данных ... 53
7.1.3. Выход из АРМа ... 54
7.2. Работа с субъектами доступа ... 55
7.2.1. Создание первого администратора доступа ... 55
7.2.2. Создание первого пользователя-оператора ... 57
7.2.3. Создание операторов ... 57
7.2.4. Свойства пользователя ... 59
7.2.5. Изменение пароля ... 61
7.2.6. Блокирование и разблокирование пользователя ... 61
7.2.7. Создание группы доступа ... 62
7.2.8. Свойства группы доступа ... 64
7.2.9. Удаление группы доступа ... 69
7.2.10. Профили пользователей ... 69
7.2.11. Свойства пользовательских профилей ... 71
7.3. Назначение субъектам прав доступа ... 75
7.3.2. Назначение прав доступа пользователю ... 75
7.3.3. Назначение прав доступа группе пользователей ... 76
7.3.4. Передача прав пользователей ... 77
7.3.5. Отзыв ролей ... 78

8. Порядок работы с прикладным функционалом Системы 80
8.2. Процедуры обновления прикладного функционала 80
9. Действия в случае сбоя 81
9.2. Проверка корректности функционирования Сервера приложений 81
9.3. Включить дополнительное логирование в Сервера приложений 81
9.4. Включение логирования работы АРМов 81
9.5. Получение дампа памяти в АРМ «ЦФТ-Навигатор» 83
10. Сообщения администратору 85
11. Устранение типичных ошибок 86

АННОТАЦИЯ

Настоящий документ представляет собой руководство администратора «ЦФТ-Технологическое ядро со встроенными средствами защиты информации» (далее – Системы) и содержит инструкции по установке и настройке серверной и клиентской частей Системы, основным операциям администратора в процессе эксплуатации и обслуживания Системы, а также пояснения о порядке работы с прикладным функционалом Системы.

Руководство предназначено для специалистов, выполняющих задачи по установке и конфигурированию требуемых параметров Системы, а также по администрированию Системы в процессе ее эксплуатации и обслуживания.

1 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

АРМ – автоматизированное рабочее место

ВМ – виртуальная машина

ОС – операционная система

ПО – программное оборудование

РС – рабочая станция пользователя

Система – «ЦФТ-Технологическое ядро со встроенными средствами защиты информации»

СП – Сервер приложений

СУЛ – список уполномоченных лиц

ЭДО – электронный документооборот

ADFS – программный компонент, предоставляющий пользователям единый вход в системы и приложения, расположенные за пределами организации

FIO (File Import Ouput) - инструмент по импорту данных из файлов и экспорту данных из БД в файл

WAP – протокол для передачи данных

2 НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ

2.1. Область применения

«ЦФТ-Технологическое ядро со встроенными средствами защиты информации» – специализированная информационная система, предназначенная для обеспечения высокоэффективного управления данными организации.

2.2. Краткое описание возможностей

Система реализует следующие функции:

- авторизация пользователей;
- управление учетными данными пользователей;
- реализация ролевого метода разграничения доступа;
- регистрация событий безопасности.

2.3. Основные компоненты

Система состоит из Сервера приложений 2MCA DBI (далее – СП), администрируемого посредством веб-приложения.

Общая структурная схема Системы представлена на рисунке 1.

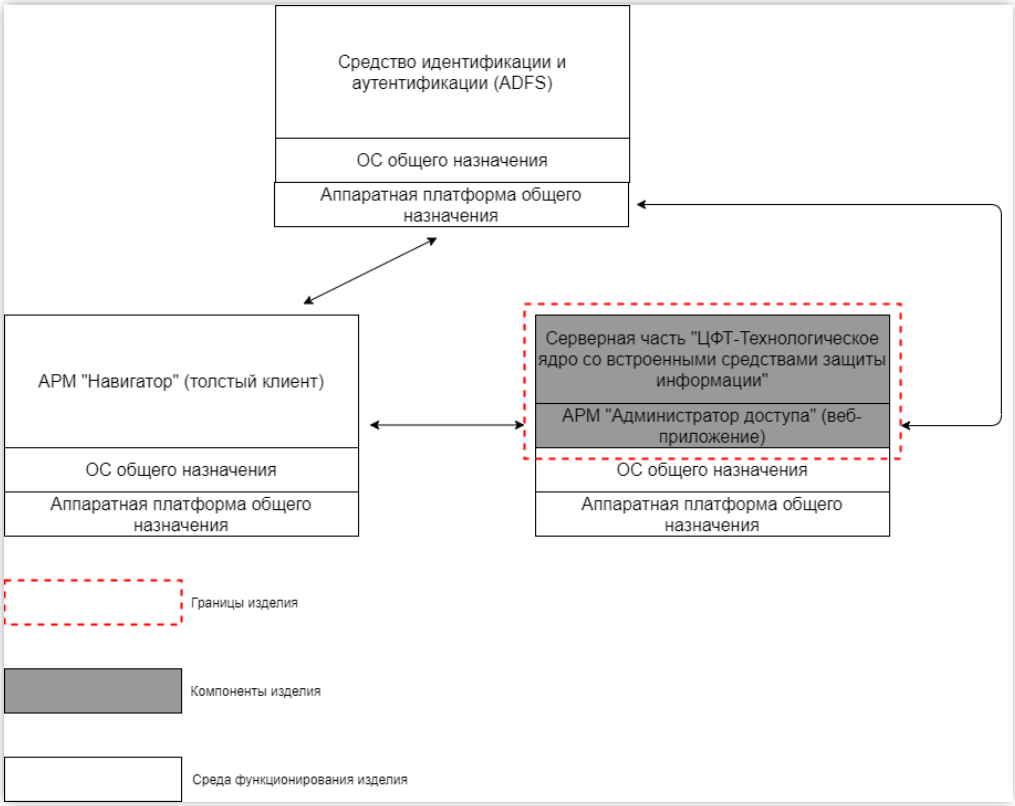


Рисунок 1

3 ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНЫЕ МЕРЫ ПО ПРИЕМКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В целях обеспечения безопасности в процессе приемки ПО рекомендуется соблюдать меры по проверке целостности, комплектности, маркировки и упаковки, указанные в формуляре RU.23578167.00001-01 30.

Также перед установкой дистрибутива рекомендуется произвести контроль целостности неизменяемых файлов дистрибутива на соответствие значениям, приведенным в формуляре RU.23578167.00001-01 30.

4. УСТАНОВКА И НАСТРОЙКА СЕРВЕРНОЙ ЧАСТИ

4.1. Установка и настройка базы данных Postgres

Установка базы данных (далее – БД) Postgres производится согласно официальной документации, размещенной на сайте производителя https://postgrespro.ru/.

Далее на пустой БД Postgres необходимо выполнить настройку скриптов запуска БД. Для этого рекомендуется выполнить следующую последовательность шагов:

- распаковать файл со скриптами initEmptyDBPostgres.zip, расположенный на дистрибутивном диске, поставляемом в комплекте с изделием, в произвольный каталог на рабочей станции (далее – PC) администратора;
- запустить файл initEmptyDBPostgres.bat с параметрами соединения к БД: host, port, database и пользователь postgres. Следует учитывать, что работа скриптов поддерживается только под суперпользователем postgres.

Дальнейшие действия по инициализации БД следует выполнять в соответствии с инструкциями, изложенными в файле initEmptyDBPostgres/README.txt, который находится в установочном каталоге скриптов БД.

4.1.1. Создание технических пользователей и ролей

При успешном запуске БД будут созданы следующие схемы:

- APP – схема владельца данных приложения (таблицы с бизнес-данными),
- RTL – схема с объектами CoreServices (системная схема для временного хранения сессии),
- UADM – схема данных доступа (таблица с данными доступа пользователей),
- AUD – схема аудита (журналирование событий безопасности),

Также при успешном запуске БД будут созданы служебные (технические) пользователи и роли для БД Postgres:

- Суперпользователь app_srv:
  - с правами на бизнес-данные (владелец схемы, где находятся бизнес данные). Используется для добавления, модификации, удаления и чтения бизнес данных.
  - с правами аудита (владелец схемы, где находятся данные аудита). Используется для добавления и чтения данных аудита.
  - доступ к данным контроля доступа отсутствует.
- Суперпользователь app_adm:

– с правами на вспомогательные таблицы ТЯ (владелец схемы, где находятся таблицы состояния пользовательских сессий)
– с правами аудита (владелец схемы, где находятся данные аудита). Используется для добавления и чтения данных аудита.
– доступ к бизнес-данным и данным контроля доступа отсутствует.

- Суперпользователь uadmin_usr:
  – с правами на данные системы доступа (владелец схемы, где находятся данные о системе доступа). Используется для управления пользователями и правами доступа.
  – с правами аудита (владелец схемы, где находятся данные аудита). Используется для добавления и чтения данных аудита.
  – доступ к бизнес-данным отсутствует.
- Суперпользователь ibs. Имеет права на все перечисленное выше.

При этом на схему доступа будет внесена информация о пользователе IBS и группе ADMIN_GRP, а также будут выданы права администратора для пользователя IBS. Для того чтобы права пользователя были проинициализированы, необходимо в настройках СП задать параметру enable-user-groups-transfer-to-model значение true. Подробнее см. в разделе settings.xml.

По умолчанию пароли технических пользователей совпадают с названием роли. Сразу после создания технических пользователей рекомендуется сменить пароли средствами БД на соответствующие требованиям безопасности, согласно принятым в организации регламентам.

Примечание

Для обеспечения информационной безопасности Системы и запрета несанкционированного доступа к ней непривилегированных пользователей рекомендуется разделить пароль администратора IBS на несколько частей и обеспечить распределенное хранение каждой части разными сотрудниками.

4.2. Настройка системы доступа

4.2.1. Общие принципы организации доступа

Система является объектно-ориентированной и состоит СП, администрируемого посредством АРМ «Администратор доступа», и толстого клиента – АРМ «ЦФТ-Навигатор», взаимодействующего с СП.

Система включает в себя следующие основные подсистемы:

1. Подсистема функций безопасности (посредством которой происходит подключение и авторизация на СП, идентификация субъектов доступа;

предоставление доступа к данным БД, а также регистрация событий безопасности).

2. Подсистема взаимодействия с клиентом (предоставляет API для взаимодействия толстого клиента «ЦФТ-Навигатор» с СП, а также среду выполнения программного кода, реализующего бизнес-функции).

Толстый клиент в свою очередь представляет собой совокупность нижеследующих элементов, автоматизирующих решение какой-либо задачи, выполняемой пользователем-оператором:

1. Типы базовых понятий (ТБП) – хранение данных (экземпляров ТПБ), агрегация функций.
2. Представлений ТБП – пользователь-оператор может просмотреть список экземпляров ТБП только через доступные ему Представления.
3. Операций ТБП – пользователь-оператор может менять данные Приложения, только выполняя доступные ему Операции.
4. Переходов ТБП – специализированные операции ТБП.
5. Экземпляров ТБП – пользователь-оператор может просмотреть список экземпляров ТБП только согласно назначенным ему правам доступа.

Создание подсистемы контроля доступа базируется на следующих принципах:

1. Обеспечить необходимый уровень гибкости и детализации контроля доступа пользователей к информационным ресурсам Приложения по матрице субъект доступа (пользователь) – объект доступа (элемент Приложения).
2. Реализация контроля доступа на стороне сервера таким образом, чтобы пользователь не смог получить доступ к информационным ресурсам Системы «в обход» системы контроля доступа, используя программное обеспечение, отличное от клиентских АРМов.

Все пользователи Системы с точки зрения системы доступа делятся на две категории.

1. Операторы

Это основная категория, к которой относятся пользователи, имеющие доступ к функционалу Приложения.

Основные права операторов:

- Подключение к СП по определенному протоколу;
- Право на выборку данных из представлений ТБП;
- Запуск операций ТБП.

При взаимодействии пользователя с определенной ролью с СП система контроля доступа «проверяет» права конкретного пользователя на доступ к данному

информационному ресурсу. Подробнее о назначении субъектам прав доступа см. раздел Назначение субъектам прав доступа.

Так, система доступа регламентирует доступ пользователей к следующим информационным ресурсам системы:

А) Доступ к ТБП. Все доступные пользователю ТБП отображаются в меню АРМ «ЦФТ-Навигатор».
Б) Доступ к представлениям ТБП. Пользователь может просмотреть список экземпляров ТБП только через доступные ему представления
В) Доступ к операциям. Пользователь может выполнить только доступные ему операции.
Г) Доступ к переходам. Пользователь может сменить состояние экземпляра ТБП, только через доступный ему метод перехода.
Д) Доступ к экземплярам. Можно определить доступ пользователя к отдельным экземплярам ТБП.

Примечание

Доступно если поддержан при в представлениях и операциях Приложения. В этом случае Оператор сможет просматривать только те экземпляры ТБП, которые ему доступны и выполнять операции также только над доступными экземплярами.

Доступ определяется Администратором доступа.

2. Администраторы доступа

Это категория пользователей, которые могут создавать, модифицировать и удалять пользователей системы доступа, определять права доступа к информационным ресурсам.

Данная роль может иметь доступ к некоторые данным Приложения, чтобы обеспечить функции разграничения прав на эти объекты.

Данной роли не дается никаких прав на изменение как прикладных данных (запуск операций).

После создания и первичной настройки пользователей Системы администрирование и работа с данными осуществляется только через зарегистрированные в системе доступа учетные записи (далее – УЗ) (субъекты доступа).

Соединение с системой осуществляется в два этапа:

1. Сначала посредством механизмов внешней аутентификации (ADFS);
2. Затем (в случае успешной аутентификации) – по аутентификационным данным пользователя производится его идентификации как субъекта системы доступа и инициализация окружения, необходимого для его дальнейшей работы. Информация о подключении пользователя заносится в журнал регистрации сессий.

Без такой инициализации пользователь не может выполнять свои функции даже при наличии формальных прав на объекты системы.

4.2.2. Конфигурация файла настроек системы доступа

Настройка системы доступа предполагает выполнение следующих шагов:

1. Установить JRE 11 версии (для 64-битных ОС), следуя инструкции, размещенной на официальном сайте производителя https://adoptium.net/releases.html .
2. Подготовить файл настроек веб-приложения АРМ «Администратор доступа» application.properties по инструкции, описанной в разделе Конфигурация файла настроек системы доступа.
3. Запустить АРМ «Администратор доступа».

Создать файл настроек системы доступа application.properties в отдельном каталоге на РС администратора. Извлечь файл useradmin.jar из архива useradmin.zip, расположенного на дистрибутивном диске, в каталог с файлом application.properties.

В файле application.properties необходимо внести следующие параметры:

А) Включить возможность аутентификации средствами БД

Пример:

useradmin.security.authorization=ANY

Примечание:

Аутентификация по паролю используется только при первом входе в АРМ «Администратор доступа». Далее она должна быть отключена для обеспечения функций безопасности. Подробнее см. раздел Запуск АРМ «Администратор доступа». Создание первого администратора доступа.

Б) Добавить настройки авторизации по ADFS

Пример:

# Использовать oauth2 аутентификацию
spring.security.oauth2.enable=true

spring.security.oauth2.client.registration.adfs.client-id=2145-46bc-4233-a481-4ddd05e1b8e8
spring.security.oauth2.client.registration.adfs.client-secret=dyDrOxoSmNKuDEhAoKRVdxH6_iEkuj9Esw0SBdU_
spring.security.oauth2.client.registration.adfs.authorized-grant-type=authorization_code
#spring.security.oauth2.client.registration.adfs.token-

uri=https://abc.ru/adfs/oauth2/token
#spring.security.oauth2.client.registration.adfs.userAuthorizationUri=https://abc.ru/adfs/oauth2/authorize
spring.security.oauth2.client.registration.adfs.redirect-uri={baseUrl}/login/oauth2/code/{registrationId}
spring.security.oauth2.client.registration.adfs.scope=openid
spring.security.oauth2.client.provider.adfs.issuer-uri=https://abc.ru/adfs

В) Добавить настройки пула соединения с пользовательскими данными

Пример:

orm.data.dialect=org.hibernate.dialect.PostgreSQL10Dialect
orm.data.driver=org.postgresql.Driver
orm.data.url=jdbc:postgresql://localhost:0000/postgres?currentSchema=uadm,aud,app,public
orm.data.username=uadmin_usr
orm.data.password=uadmin_usr

Г) Добавить настройки пула соединения с метаданными.

Пример:

orm.metamodel.dialect=org.hibernate.dialect.H2Dialect
orm.metamodel.driver=org.apache.ignite.IgniteJdbcThinDriver
orm.metamodel.url=jdbc:ignite:thin://127.0.0.1:0000;schema=dbi_project
orm.metamodel.username=
orm.metamodel.password=

4.2.3. Запуск АРМ «Администратор доступа»

После корректной настройки конфигурационных файлов системы доступа необходимо запустить АРМ «Администратор доступа». Для этого требуется, находясь в каталоге расположения файла useradmin.jar, выполнить команду:

%JAVA_HOME%/java -jar -Duser.language=ru -Duser.country=RU useradmin.jar >./uadmin.log 2>&1 &

После этого следует открыть веб-приложение АРМ «Администратор доступа» в браузере по адресу сервера, на котором запущен АРМ «Администратор доступа».

Примечание:

Команда для запуска АРМ «Администратор доступа» для ОС семейства Unix:

nohup [ПУТЬ ДО JRE]/java -jar -Duser.language=ru -Duser.country=RU [ПУТЬ ДО useradmin]/useradmin.jar>./uadmin.log 2>&1 &

Для дальнейшей работы Системы рекомендуется создать первого администратора доступа – пользователя с правом создавать дальнейших пользователей-операторов. Подробнее об этом см. раздел Создание первого администратора доступа.

4.3. Установка лицензии

Для работы пользователей через СП необходима установка лицензии. Коды приложений в лицензии - 2MCA.APP, 2MCA_DBI.

Функциональность лицензируется в запретительном режиме, т.е. без явно выданной лицензии работа пользователей через СП невозможна.

Примечание:

Лицензионный ключ выдается каждому именованному пользователю на одну PC. Каждый пользователь должен быть одновременно лицензирован в качестве пользователя Системы.

4.4. Установка и настройка Сервера приложений

Для обеспечения работы СП необходимо выполнить следующие шаги:

- Установить OpenJDK 8 версии (для 64-битных ОС), следуя инструкции, размещенной на официальном сайте производителя;
- Установить СП из списка поддерживаемых (см. раздел Системные требования);
- Подготовить конфигурационные файлы;
- Подготовить архив 2mca.war, согласно инструкции readme.txt, размещенной на дистрибутивном диске;
- Настроить СП и установить приложение;
- Проверить корректность установки приложения.

4.4.1. Системные требования

Требования к аппаратному обеспечению

Для оценки требований к аппаратному обеспечению рекомендуется обратиться к экспертам ЦФТ, для индивидуального расчета параметров оборудования.

Требования к программному обеспечению

Указанные ниже требования к программному обеспечению необходимы для бесперебойной работы СП 2MCA. Они зависят от предполагаемой нагрузки.

- Операционная система: «РЕД ОС 7.2 Муром»;
- OpenJDK Runtime Environment (build 1.8.0_242-b08);
- Apache Tomcat 9.0.45

Требования к окружению

- Время на сервере СУБД и СП должно быть синхронизировано.
- В профиле пользователя, под которым запускается контейнер СП, необходимо указать следующую кодировку:

  LANG=ru_RU.CP1251; export LANG

- Для использования пароля в кодировке Cp1251, необходимо в JVM передать параметр:

  -Dfile.encoding=Cp1251

4.4.2. Настройка параметров конфигурационных файлов

Для обеспечения работы СП необходимо наличие следующих конфигурационных файлов:

- settings.xml;
- pool-settings.xml;
- jaas-settings.xml;
- cda-settings.xml;
- log4j.properties;
- auth-settings.xml.

Путь до конфигурационных файлов указывается в настройках запуска сервера (подробнее см. раздел Настройка сервера Tomcat).

4.4.2.1. settings.xml

Файл содержит настройки работы СП.

Синтаксис:

```
<?xml version="1.0" encoding="windows-1251"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<entry key="[Название параметра]">[Значение параметра]</entry>
</properties>
```

Описание общих параметров:

- log4j.properties – файл настроек службы журналирования, обязательный параметр. Необходимо указывать полный путь до файла log4j.properties.
- edoc.installed=0 – признак инсталляции дистрибутива ЭДО на схеме (по умолчанию равен 1).
- core.jaas.config.name – установка режима аутентификации. Устанавливает один из режимов аутентификации:

- session.nls.init – признак установки NLS-параметров профиля пользователя при инициализации сессии из лёгкой в тяжёлую. По умолчанию равен false.
- server.uid – настройка задаётся в случае запуска нескольких СП на одной машине. Или если имя машины, на которой запускается СП, превышает 30 символов. Это же значение следует указать в job-setting.xml в поле job.machine вместо <название компьютера> (см. раздел Настройка сервиса серверов заданий Сервера приложений).

Для того чтобы права пользователя были проинициализированы, параметру enable-user-groups-transfer-to-model необходимо задать значение true.

Пример:

файл settings.xml

<entry key="enable-user-groups-transfer-to-model">true</entry>.

Описание параметров, специфичных для СП:

- stdio.home_path – корневой каталог FIO, обязательный параметр;
- stdio.temp_path – каталог для загрузки временных файлов, обязательный параметр;
- session.check.interval - интервал (в секундах) проверки состояния пользовательских сессий. 0 - проверка выключена;
- enable-java-dbmslob-convert – признак исполнения функций dbms_lob.converttoblob, dbms_lob.converttoclob на стороне СП 2МСА. По умолчанию равен false, означает исполнение на стороне БД.
- enable-java-dbmsxmlgen-convert - признак исполнения функции dbms_xmlgen.convert на стороне СП 2МСА. По умолчанию равен false, означает исполнение на стороне БД.
- enable-java-xmltype-transform - признак исполнения функции xmltype.transform на стороне СП 2МСА. По умолчанию равен false, означает исполнение на стороне БД.
- enable-light-sessions - признак включения режима лёгкой инициализации пользовательских сессий. По умолчанию равен false, означает что режим выключен.
- enable-migration-service - признак включения очистки «зависших» прикладных сессий между клиентом и СП. По умолчанию равен false, означает что очистка сессий выключена.
- core.web.auth.chain.names - список ключей сервисов аутентификации, разделяются запятой «,».

Параметр указывается только при настройке аутентификации через внешние службы. Подробнее см. в разделе auth-settings.xml.

Подробнее о работе с FIO через СП – см. раздел Особенности работы с FIO.

Примечание

Если один из параметров (session.check.interval, enable-light-sessions или enable-migration-service) не задан, или имеет пустое значение, то режим контроля активных пользовательских сессий отключается.

Примеры:

СП 2 МСА

```
<?xml version="1.0" encoding="windows-1251"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<entry key="stdio.home_path">~/FIO/schema_name</entry>
<entry key="stdio.temp_path">~/FIO/schema_name/ibs/tmp</entry>
<entry key="log4j.properties">log4j.properties</entry>
<entry key="edoc.installed">0</entry>
<entry key="core.jaas.config.name">CoreNTLMLoginModule</entry>
<entry key="enable-java-dbmslob-convert">false</entry>
</properties>
```

Описание параметров, специфичных для СП 2МСА DBI:

- lic.installation – полный путь до файла лицензии инсталляции;
- lic.sul – полный путь до файла СУЛ;
- lic.applications – полный путь до файла с описание приложения CORE.

Пример:

```
<entry key="lic.installation">/usr/share/apache-tomcat-9.0.45/webapps/lic/lic.lic</entry>
<entry key="lic.sul">/usr/share/apache-tomcat-9.0.45/webapps/lic/sul.lic</entry>
<entry key="lic.applications">/usr/share/apache-tomcat-9.0.45/webapps/lic/cft_corp_rosatom.xsap</entry>
```

4.4.2.2. pool-settings.xml

Файл, в котором содержится информация о соединении с сервером БД. Он должен содержать настройки двух пулов соединений: для инициализации пользовательских запросов и для открытия/закрытия сессий.

Синтаксис:

<?xml version="1.0" encoding="windows-1251"?>

<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">

<properties>

<entry key="[Название параметра]">[Значение параметра]</entry>

</properties>

Описание параметров:

- <prefix>-<poolNumber>.alias – имя пула, обязательный параметр.
- <prefix>-<poolNumber>.factory-class – фабрика для открытия соединений, может быть драйвером или источником данных, обязательный параметр.

Например: oracle.jdbcftc.CoreConnectionDriver – драйвер, подготавливающий соединение перед передачей его в пул; oracle.jdbc.pool.OracleDataSource – источник SQL-соединений; oracle.jdbc.xa.client.OracleXADataSource – источник XA-соединений.

- <prefix>-<poolNumber>.driver-url – строка соединения с базой данных, обязательный параметр. Если в качестве фабрики указан драйвер oracle.jdbcftc.CoreConnectionDriver, то строка соединения должна начинаться с core:<имя пула>.

Строка соединения с базой данных может задаваться тремя способами:

@<server>:<port>:<database SID>

@//<server>:<port>/<service name>

@<tns-name>

- <prefix>-<poolNumber>.user – пользователь, от имени которого устанавливается соединение с БД, обязательный параметр.

Примечание

Для запуска СП в настройке Имя пользователя необходимо указать имя владельца схемы.

Для пула, отвечающего за открытие/закрытие сессий, необходимо указать пользователя с ролью СП (создание сессий).

- <prefix>-<poolNumber>.password – пароль пользователя, обязательный параметр.

Примечание

Пароль может быть указан в зашифрованном виде, подробнее о шифровании паролей см. в разделе «Шифрование паролей».

- <prefix>-<poolNumber>.initial-connection-count – количество соединений, создаваемых при запуске, обязательный параметр.
- <prefix>-<poolNumber>.minimum-connection-count – минимальное количество соединений с БД, обязательный параметр.
- <prefix>-<poolNumber>.maximum-connection-count – максимальное количество соединений с БД, обязательный параметр.
- <prefix>-<poolNumber>.inactive-connection-timeout – тайм-аут для неактивных соединений в пуле (в секундах). По истечении этого времени неактивное соединение удаляется из пула. Обязательный параметр.
- <prefix>-<poolNumber>.timeout-check-interval – время, через которое будет производиться проверка соединений, обязательный параметр.
- <poolNumber> – номер пула. Отсчет ведется с нуля.
- <prefix> – префикс, указывающий какой именно пул используется для работы с БД. Возможные значения:
  - tomcat – если источником данных выступает БД Postgres.

Значение зависит от выбранного класса источника данных в файле cda-settings.xml.

Пример:

```
<?xml version="1.0" encoding="windows-1251"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<entry key="ucp-0.alias">main</entry>
<entry key="ucp-0.driver-
url">core:main:jdbc:oracle:thin:@server:1541:db_sid</entry>
<entry key="ucp-0.factory-class">oracle.jdbcftc.CoreConnectionDriver</entry>
<entry key="ucp-0.user">usr</entry>
<entry key="ucp-0.password">pwd</entry>
<entry key="ucp-0.initial-connection-count">1</entry>
<entry key="ucp-0.minimum-connection-count">1</entry>
<entry key="ucp-0.maximum-connection-count">150</entry>
<entry key="ucp-0.inactive-connection-timeout">60</entry>
<entry key="ucp-0.timeout-check-interval">1</antry>
<entry key="ucp-1.alias">adm</entry>
```

```
<entry key="ucp-1.driver-
url">core:adm:jdbc:oracle:thin:@server:1541:db_sid</entry>
<entry key="ucp-1.factory-class">oracle.jdbcftc.CoreConnectionDriver</entry>
<entry key="ucp-1.user">usr</entry>
<entry key="ucp-1.password">pwd</entry>
<entry key="ucp-1.initial-connection-count">1</entry>
<entry key="ucp-1.minimum-connection-count">0</entry>
<entry key="ucp-1.maximum-connection-count">150</entry>
<entry key="ucp-1.inactive-connection-timeout">60</entry>
<entry key="ucp-1.timeout-check-interval">1</entry>
    </properties>
```

4.4.2.3. jaas-settings.xml

Файл содержит настройки аутентификации.

Синтаксис:

```
<?xml version="1.0" encoding="windows-1251"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
    <properties>
<entry key="[Название параметра]">[Значение параметра]</entry>
    </properties>
```

Сообщения о попытках соединения можно просмотреть в логах СП.

4.4.2.4. cda-settings.xml

Файл содержит настройки доступа к данным.

Синтаксис:

```
<?xml version="1.0" encoding="windows-1251"?>
<!DOCTYPE cda-configuration SYSTEM "cda-settings.dtd">
<cda-configuration>
<transaction-manager-lookup-class>[Имя класса]</transaction-manager-lookup-
class>
<data-source-lookup-class>[Имя класса]</data-source-lookup-class>
<connection-factory-class>[Имя класса]</connection-factory-class>
<database-units defaultDatabaseType="main">
  <database-unit alias="DB_UNIT_NAME">
```

```
        <database type="main">
            <data-source-srv>[Название пула]</data-source-srv>
                <data-source-adm>[Название пула]</data-source-adm>
        </database>
    </database-unit>
</database-units>
</cda-configuration>
```

Описание параметров:

- transaction-manager-lookup-class – имя класса, который отвечает за передачу данных, обязательный параметр.

Возможные варианты:

- ru.cft.platform.core.dao.datasource.impl.XATransactionManagerLookup
- data-source-lookup-class – имя класса, который отвечает за поиск источника данных, обязательный параметр.

Возможные варианты:

- ru.cft.platform.core.dao.datasource.impl.UCPDataSourceLookup – устаревшее значение.

Если указан этот класс, то на самом деле используется ru.cft.platform.core.dao.datasource.ucp.UCPDataSourceLookup. Рекомендуется указать один из классов, перечисленных ниже.

- ru.cft.platform.core.dao.datasource.ucp.UCPDataSourceLookup – класс, который указывается для использования пула Oracle Universal Connection Pool. Это значение следует указывать в случае использования БД Oracle.
- ru.cft.platform.core.dao.datasource.tomcat.TomcatPoolDataSourceLookup – класс, который указывается для использования пула Apache Tomcat. Это значение следует указывать в случае использования БД Postgres.
- ru.cft.platform.core.dao.datasource.impl.xa.JNDIDataSourceLookup – класс, который указывается для использования внешнего, по отношению к СП, пула.

В зависимости от указываемого класса, в pool-settings.xml надо будет указать соответствующий префикс для настройки пулов соединений с БД.

- connection-factory-class – имя класса, который отвечает за соединение с источником данных, обязательный параметр.
- <database-units defaultDatabaseType="main"> – тип базы данных, используемый по умолчанию там, где не указано явно, обязательный параметр.

- <database-unit alias="DB_UNIT_NAME"> – имя блока баз данных, обязательный параметр.
- <database type="main"> – тип базы данных, состоящий из произвольного набора символов, характеризующих назначение базы данных. Один из указанных типов должен быть выделен в качестве типа по умолчанию. Обязательный параметр.
- data-source-srv – название пула, который отвечает за инициализацию/завершение соединений, обязательный параметр.
- data-source-adm – название пула, который отвечает за открытие/закрытие соединений, обязательный параметр.

Пример:

```
<?xml version="1.0" encoding="windows-1251"?>

<!DOCTYPE cda-configuration SYSTEM "cda-settings.dtd">

<cda-configuration>

    <transaction-manager-lookup-class>ru.cft.platform.core.dao.datasource.impl.XATransactionManagerLookup</transaction-manager-lookup-class>

    <data-source-lookup-class>ru.cft.platform.core.dao.datasource.impl.UCPDataSourceLookup</data-source-lookup-class>

    <connection-factory-class>ru.cft.platform.core.container.connection.ConnectionFactory</connection-factory-class>

    <database-units defaultDatabaseType="main">

        <database-unit alias="DB_UNIT_NAME">

            <database type="main">

                <data-source-srv>main</data-source-srv>

                <data-source-adm>adm</data-source-adm>

            </database>

        </database-unit>

    </database-units>

</cda-configuration>
```

4.4.2.5. log4j.properties

log4j – библиотека для журналирования информационных сообщений. Файл log4j.properties содержит настройки журнала информационных сообщений. Для настройки файла log4j.properties рекомендуется ознакомиться с документацией, размещенной по адресу http://logging.apache.org/log4j/1.2/ .

Синтаксис:

log4j.rootCategory=<WARN_LEVEL>, <APPENDER_NAME1>

log4j.appender.<APPENDER_NAME1>=org.apache.log4j.ConsoleAppender

log4j.appender.<APPENDER_NAME1>.layout=org.apache.log4j.PatternLayout

log4j.appender.<APPENDER_NAME1>.layout.ConversionPattern=%-5p [%x] %c{2}:%m%n

Описание параметров:

<WARN_LEVEL> – уровень информативности сообщений.

<APPENDER_NAME1> – имя аппендера.

- log4j.rootCategory – строка определяет уровень информативности сообщений в журнале, а также определяет имя аппендера. Аппендер – объект, который определяет, что нужно делать с журналируемыми сообщениями.
- log4j.appender.<APPENDER_NAME1> – строка задаёт вывод сообщений в консоль. Формат выводимых сообщений определяется шаблоном.
- log4j.appender.<APPENDER_NAME1>.layout – в строке указывается, что для аппендера используется класс org.apache.log4j.PatternLayout, который отвечает за простой вывод в консоль.
- log4j.appender.<APPENDER_NAME1>.layout.ConversionPattern – в строке задаётся шаблон вывода журнала.

Пример рекомендованной настройки параметров журналирования:

```
log4j.rootCategory=INFO, Console

# uncomment to log just the SQL

#log4j.logger.org.hibernate.SQL=DEBUG

# uncomment to JDBC bind parameters

#log4j.logger.org.hibernate.type=TRACE

#log4j.logger.org.hibernate.type.descriptor.sql.BasicExtractor=ERROR

#log4j.logger.org.hibernate.type.NullableType=ERROR

# uncomment to log cache activity

#log4j.logger.org.hibernate.cache=DEBUG

# uncomment to log requests and responses verbatim

#log4j.logger.ru.cft.platform.web.api.WebAPIServlet=TRACE
```

```
# uncomment to log methods validation, implementation
#log4j.logger.ru.cft.platform.business.runtime.method.MethodAdapter=DEBUG

# uncomment to log MT steps
#log4j.logger.ru.cft.platform.sat.player.Player =DEBUG

# uncomment to log dynamic PLP
#log4j.logger.ru.cft.platform.business.runtime.dynamic.DynamicPLPImpl=DEBUG

log4j.logger.org.apache.tapestry5 = WARN
log4j.logger.org.hibernate.cache.ehcache.AbstractEhcacheRegionFactory = ERROR
log4j.logger.org.hibernate.cache.ehcache.internal.strategy.
                    EhcacheAccessStrategyFactoryImpl = ERROR
log4j.logger.org.hibernate.engine.internal.StatefulPersistenceContext = ERROR
log4j.logger.org.hibernate.engine.jdbc.spi.SqlExceptionHelper = OFF
log4j.logger.org.hibernate.proxy.pojo.javassist.JavassistLazyInitializer = OFF
log4j.logger.ru.cft.platform.web.ui.tapestry = WARN

log4j.appender.Console=org.apache.log4j.ConsoleAppender
log4j.appender.Console.layout=org.apache.log4j.PatternLayout
log4j.appender.Console.layout.ConversionPattern=%-5p [%x] %c{2}: %m%n
```

4.4.2.6. auth-settings.xml

Файл предназначен для настройки аутентификации через сторонние службы каталогов.

Шаблон файла:

```
<?xml version="1.0" encoding="windows-1251"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
    <properties>
<entry key="КЛЮЧ">ЗНАЧЕНИЕ</entry>
    </properties>
```

КЛЮЧ представляет собой связку названия модуля аутентификации и параметра. Разделяются символом точки ".".

Пример:

<entry key="Oracle.driver-url">jdbc:oracle:thin:@any.host.com:anyport:dbsid</entry>

где:

1. Oracle – название модуля аутентификации. Название может быть любым, но без пробелов и английскими буквами.
2. driver-url – параметр. Параметры для каждого модуля аутентификации задаются свои.

Название/-я модуля/-ей аутентификации указываются в файле settings.xml в параметре core.web.auth.chain.names.

4.4.3. Настройка опциональных параметров

Краткое описание стартовых настроек сервера:

-Dnet.sf.ehcache.skipUpdateCheck=true

Отключает проверку последней версии библиотеки Ehcache.

4.4.4. Настройка аутентификации через ADFS + WAP

Описание параметров приведено в таблице 1.

Таблица 1

Название параметра	Значение параметра	Комментарий
class	ru.cft.platform.web.auth.filter.ADFSOAuth20Filter	Название класса, который занимается аутентификацией
authentication_url	URL сервера аутентификации	Адрес сервера аутентификации
token_url	URL для получения access-токена	Адрес для получения access-токена по протоколу OAuth2.0
client_id	уникальный идентификатор клиента аутентификации	Уникальный идентификатор клиента аутентификации. Этот идентификатор можно получить после регистрации приложения в ADFS. Идентификатор клиента представляет собой публично доступную строку, которая используется ADFS для идентификации приложения, а также используется для создания авторизационных URL для пользователей
client_secret	секрет клиента	Секрет клиента. Его можно получить после регистрации приложения в ADFS. Секрет клиента используется для аутентификации подлинности приложения для ADFS, когда приложение запрашивает доступ к аккаунту

		пользователя. Секрет клиента должен быть известен только приложению и ADFS
cert_path полный	путь до сертификата	Сертификат, которым подписан токен. Нужен для проверки токена
scope	openid	Область данных, которая запрашивается о пользователе. Настройка для поддержания спецификации OAuth2.0. Регистр значения важен, следует указывать в нижнем регистре

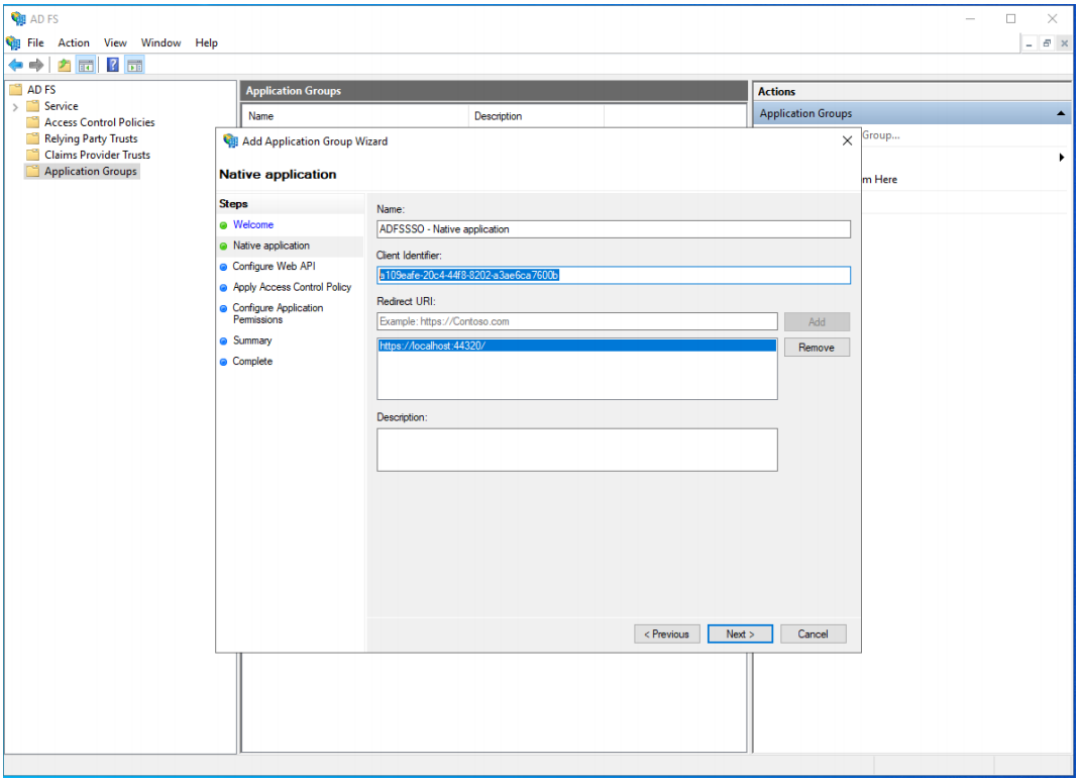
Токен, присылаемый от ADFS к СП, должен быть подписан алгоритмом RSA256.

Обязательные поля, которые ADFS должно передавать приложению в составе токена OpenID:

1. os_user – имя пользователя;
2. os_domain – название домена.

Настраивать получение этих полей следует по документации, но ниже даны вспомогательные комментарии:

При создании новой группы приложений (Application groups) на шаге настройки приложения важно запомнить значение поля Client Identifier и указать его же на странице настройки Web API (рисунок 2).



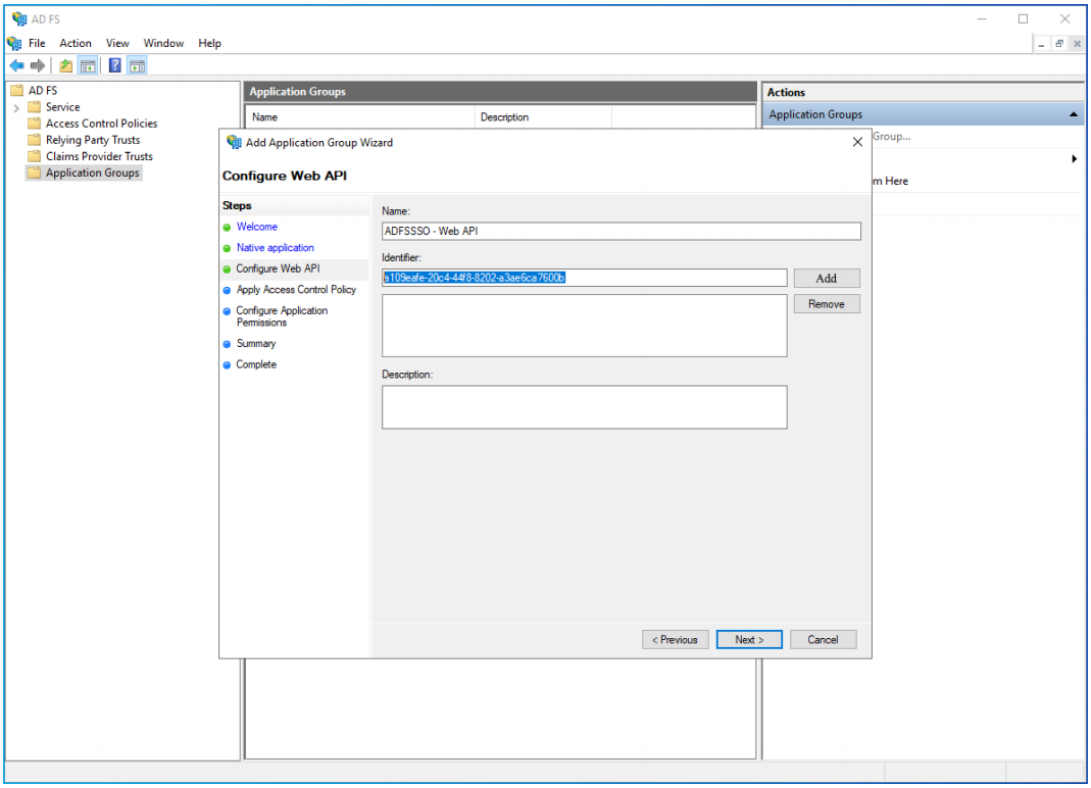


Рисунок 2

Требования (Claims) настраиваются в другом диалоге. Исходно доступны требования, изложенные в документации Microsoft (https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/technical-reference/the-role-of-claims#what-are-claim-types). Для получения значений os_user, os_domain необходимо использовать Windows account name.

Чтобы добавить в токен поля os_user, os_domain, необходимые для успешной аутентификации, нужно создать два дополнительных Claim Custom Rules:

c:[type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"] => issue(type = "os_domain", value = RegExReplace(c.value, "(?<os_domain>[-_A-Za-z0-9]+)\\(?<os_user>[-_A-Za-z0-9]+)", "${os_domain}"));

c:[type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname"] => issue(type = "os_user", value = RegExReplace(c.value, "(?<os_domain>[-_A-Za-z0-9]+)\\(?<os_user>[-_A-Za-z0-9]+)", "${os_user}")) (рисунок 3);

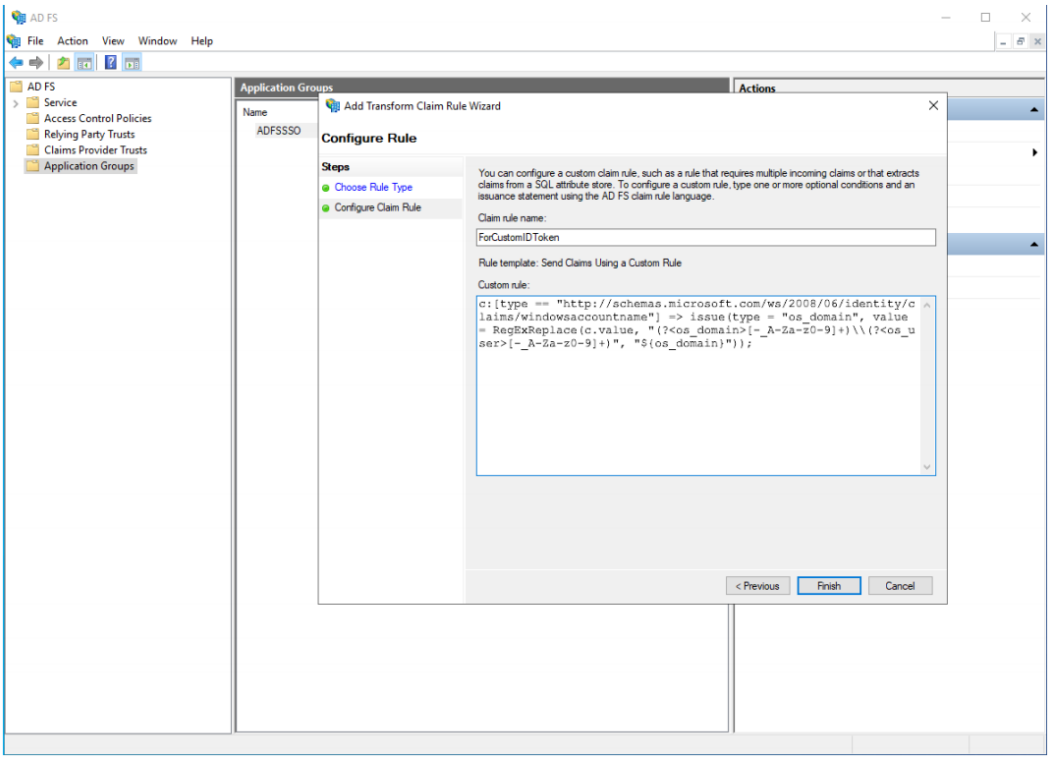


Рисунок 3

Пример настройки auth-settings.xml:

```
<?xml version="1.0" encoding="windows-1251"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
    <properties>
<entry key="ADFS.class">ru.cft.platform.web.auth.filter.ADFSOAuth20Filter</entry>
<entry key="ADFS.authentication_url">https://fsa.cft.ru/adfs/oauth2/authorize</entry>
<entry key="ADFS.token_url">https://fsa.cft.ru/adfs/oauth2/token</entry>
<entry key="ADFS.client_id">sfsdf89hfs-sfdfsafsd67asfdsa-dfsa</entry>
<entry key="ADFS.client_secret">DFlkgshHJKffdsYUi0FDsd_fdsfsFDsFFDsf</entry>
<entry key="ADFS.cert_path">/full/path/to/cert.pem</entry>
<entry key="ADFS.scope">openid</entry>
    </properties>
```

4.4.5. Особенности работы с FIO

При подключении через СП работа с файлами осуществляется на самом СП, а не на сервере БД.

Поэтому для корректной работы с FIO при подключении через СП необходимо настроить файл settings.xml, указав следующие параметры:

- stdio.home_path – корневой каталог FIO, обязательный параметр;

- stdio.temp_path – каталог для загрузки временных файлов, обязательный параметр.

4.4.6. Настройка Сервера приложений

Внимание!

В промышленной эксплуатации при соединении с СП строго рекомендуется использовать протокол HTTPS.

СП поставляется на дистрибутивном диске в виде набора каталогов. Для запуска СП и дальнейшей установки СП в Tomcat необходимо получить СП в виде архива с расширением .war. Для этого рекомендуется выполнить следующую последовательность действий:

1. С дистрибутивного диска распаковать архив platform2mca.zip в произвольный каталог на PC администратора;
2. Запустить файл make_war.bat, расположенный в каталоге platform2mca.

Готовый (собранный) файл 2mca.war будет находиться в том же каталоге, что и make_war.bat.

4.4.6.1. Настройка сервера Tomcat

Здесь и далее <TOMCAT_HOME> – путь до каталога, в который установлен сервер Tomcat.

4.4.6.1.1. Настройка порта доступа

В файле <TOMCAT_HOME>\conf\server.xml должна присутствовать секция:

<Connector port="8080" protocol="HTTP/1.1" connectionTimeout="20000"/>,

где port – порт, по которому доступен СП.

4.4.6.1.2. Указание файла настроек Сервера приложений

В случае использования Windows запустите tomcat7w.exe, находящийся в каталоге <TOMCAT_HOME>\bin\. В открывшемся окне на вкладке Java в поле Java Options добавьте новые аргументы:

-Dibso.container.settings=<PATH_TO_SETTINGS.XML>,

где <PATH_TO_SETTINGS.XML> – полный путь до файла конфигурации settings.xml.

-Djavax.net.ssl.trustStore=<PATH_TO_KEYSTORE>,

где <PATH_TO_KEYSTORE> – полный путь до хранилища с сертификатами. Указывать следует в том случае, если настраивается аутентификация через LDAPs. Подробнее см. разделы jaas-settings.xml и Создание хранилища с сертификатами.

В случае использования Linux добавьте переменную CATALINA_OPTS в ~/.bash_profile:

CATALINA_OPTS="-server -Xms2g -Xmx6g -Dibso.container.settings=<PATH_TO_SETTINGS.XML> -Djavax.net.ssl.trustStore=<PATH_TO_KEYSTORE>",

где:

- server - специальный параметр для JVM, чтобы применялись серверные оптимизации во время исполнен ия java-кода;
- Xms2g - количество памяти, выделяемой на старте приложения;
- Xmx6g - максимальное количество памяти, которое может быть выделено для приложения. Значение этого параметра варьируется в зависимости от нагрузки на СП;

<PATH_TO_SETTINGS.XML> – полный путь до файла конфигурации settings.xml;

<PATH_TO_KEYSTORE> – полный путь до хранилища с сертификатами. Указывать следует в том случае, если настраивается аутентификация через LDAPs. Подробнее см. разделы jaas-settings.xml и «Создание хранилища с сертификатами».

После добавления .bash_profile необходимо «перечитать», чтобы добавленная переменная оказалась в окружении. Для этого, находясь в домашнем каталоге, следует выполнить команду:

. .bash_profile

4.4.6.2. Установка СП на Tomcat

Установка СП состоит из следующих шагов:

1. Скопировать war-файл 2mca.war в каталог <TOMCAT_HOME>\webapps\.

2. Поместить все перечисленные ниже конфигурационные файлы в каталог, в котором расположены файлы:

- settings.xml;
- pool-settings.xml;
- jaas-settings.xml;
- cda-settings.xml;
- log4j.properties.

Примечание

Подробнее с описанием конфигурационных файлов можно ознакомиться в разделе [Настройка параметров конфигурационных файлов](#).

4.4.7. Проверка корректности установки Сервера приложений

Проверить корректность установки СП можно, указав в адресной строке браузера (например, Internet Explorer) строку вида:

<ServerName>:<port>/<ContextName>/diag,

где:

- <ServerName> – доменное имя сервера, на котором установлен СП;
- <ContextName> – контекст СП, обычно совпадает с именем war-файла;
- <port> – порт, который использует сервер.

Если приложение установлено корректно, то в окне браузера появится информация об используемой схеме и описание web-архива, а также время выполнения диагностики.

Следует обратить внимание на значения JDBC OCI и JDBC. У JDBC OCI должно быть значение SUCCESS (рисунок 4):

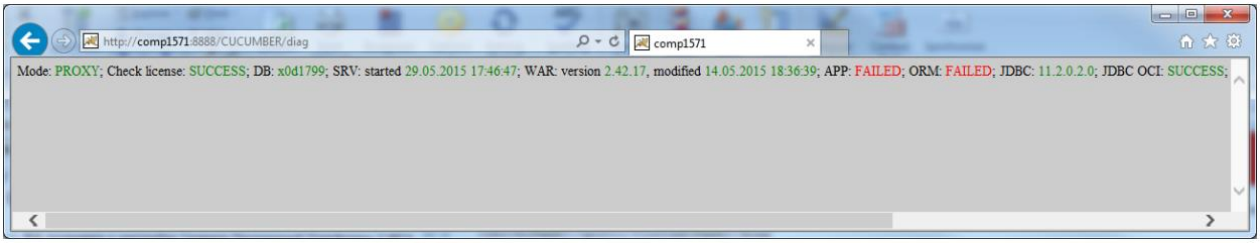


Рисунок 4

4.4.8. Шифрование паролей

Для шифрования паролей необходимо использовать утилиту crpwd.exe (для работы программы требуется установленная JRE ver.1.6. и выше). При запуске утилиты двойным щелчком левой кнопки мыши откроется окно Шифрование пароля (рисунок 5).

Последовательность по шифрованию пароля состоит из следующих шагов:

- В поле Пароль ввести пароль.
- Нажать кнопку **Зашифровать**.
- В поле Результат появится зашифрованный пароль.

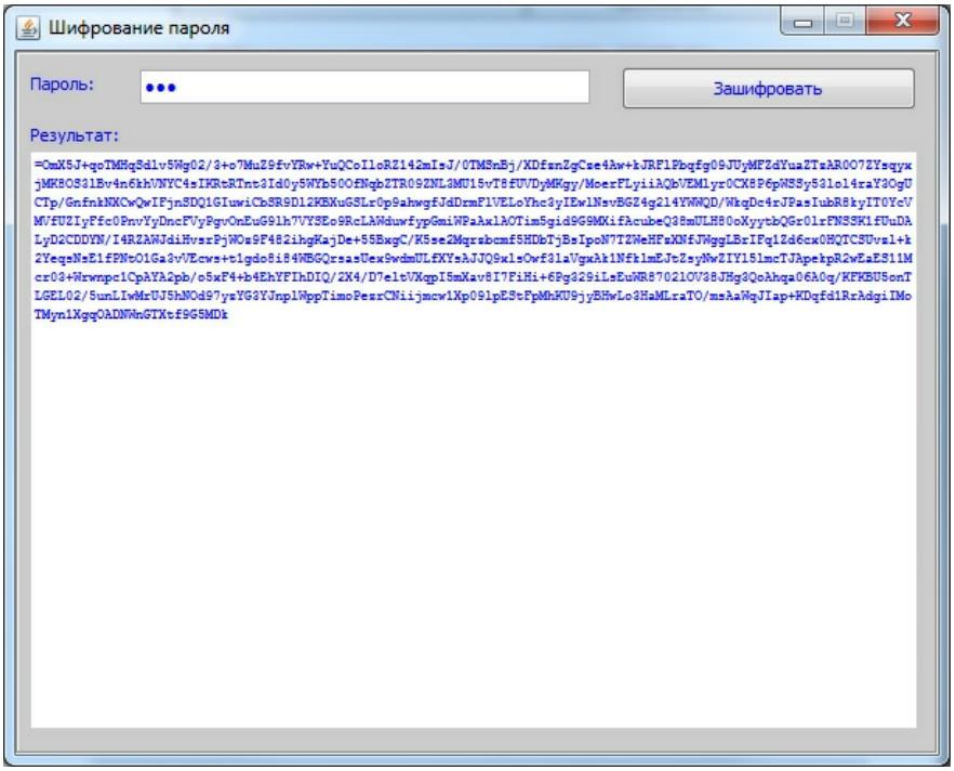


Рисунок 5

4.4.9. Синхронизация групп пользователя

При соединении пользователя через СП в подсистеме доступа происходит синхронизация групп пользователя с группами доступа этого пользователя в Active Directory. В результате синхронизации группы пользователя в подсистеме доступа и Active Directory будут совпадать.

Для настройки синхронизации групп пользователя необходимо добавить соответствующие параметры в следующие конфигурационные файлы (подробнее о настройке конфигурационных файлов см. раздел Настройка конфигурационных файлов):

- settings.xml;
- active-directory-settings.xml;
- cda-settings.xml;
- pool-settings.xm.

4.4.9.1. settings.xml

В файл settings.xml необходимо добавить параметр enable-user-group-synchronization (признак включения синхронизации групп пользователя) со значением true.

Пример:

<?xml version="1.0" encoding="windows-1251"?>

<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">

```
<properties>
    <entry key="stdio.home_path">~/FIO/schema_name</entry>
    <entry key="stdio.temp_path">~/FIO/schema_name/ibs/tmp</entry>
    <entry key="log4j.properties">log4j.properties</entry>
    <entry key="edoc.installed">0</entry>
    <entry key="core.jaas.config.name">CoreNTLMLoginModule</entry>
    <entry key="enable-user-group-synchronization">true</entry>
</properties>
```

4.4.9.2. active-directory-settings.xml

Файл содержит настройки доступа к Active Directory.

Синтаксис:

```
<?xml version="1.0" encoding="windows-1251"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
    <properties>
        <entry key="[Название параметра]">[Значение параметра]</entry>
    </properties>
```

Описание параметров:

- <serverId>.active-directory.server – адрес LDAP сервера, обязательный параметр.
- <serverId>.active-directory.search-base – базовая строка для поиска по Active Directory, обязательный параметр.
- <serverId>.active-directory.default-domain – домен, информация о пользователях которого находится на данном сервере, обязательный параметр.
- <serverId>.active-directory.username – имя пользователя, имеющего права на чтение дерева каталогов LDAP, обязательный параметр.

Значение параметра должно быть вида: <имя_пользователя>@<домен>. В некоторых случаях, значение параметра может не содержать @<домен>, необходимость определяется настройками Active Directory.

В качестве значения <имя_пользователя> может быть задан тот же пользователь, который указывается в конфигурационном файле jaas-settings.xml при аутентификации через Active Directory.

Значение <домен> должно совпадать со значением параметра <serverId>.active-directory.default-domain.

- <serverId>.active-directory.password – пароль пользователя, обязательный параметр.

Пароль, который задается в качестве значения параметра <serverId>.active-directory.password, может быть указан в зашифрованном виде. Подробнее о шифровании паролей см. в разделе Шифрование паролей.

- <serverId> - произвольный идентификатор сервера.

Особенности настройки двух и более серверов:

Если необходимо настроить основной и резервный сервера Active Directory, то указываются 2 набора параметров с разными <serverId>.

Если пользователи принадлежат двум разным доменам, то нужно указать 2 набора параметров с разными <serverId> и соответствующими значениями параметра <serverId>.active-directory.default-domain для каждого домена.

Пример:

```
<?xml version="1.0" encoding="windows-1251"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<entry key="server1.active-directory.server">ldap://example.of.domain:port</entry>
<entry key="server1.active-directory.search-base">dc=example,dc=of,dc=domain</entry>
<entry key="server1.active-directory.username">SECURITY@example.of.domain</entry>
<entry key="server1.active-directory.password">psw</entry>
<entry key="server1.active-directory.default-domain">example.of.domain</entry>
<entry key="server2.active-directory.server">ldap://example2.of.domain:port</entry>
<entry key="server2.active-directory.search-base">dc=example2,dc=of,dc=domain</entry>
<entry key="server2.active-directory.username">SECURITY2@example2.of.domain</entry>
<entry key="server2.active-directory.password">psw2</entry>
<entry key="server2.active-directory.default-domain">example2.of.domain</entry>
</properties>
```

4.4.9.3. cda-settings.xml

В файл cda-settings.xml необходимо добавить параметр data-source-sec – название пула, который отвечает за открытие/закрытие соединений, используемых для синхронизации групп пользователя.

Примечание

Имена пулов должны соответствовать именам, которые заданы в файле pool-settings.xml.

Пример:

```
<?xml version="1.0" encoding="windows-1251"?>
<!DOCTYPE cda-configuration SYSTEM "cda-settings.dtd">
<cda-configuration>
    <transaction-manager-lookup-class>ru.cft.platform.core.dao.datasource.impl.XATransactionManagerLookup</transaction-manager-lookup-class>
    <data-source-lookup-class>ru.cft.platform.core.dao.datasource.impl.UCPDataSourceLookup</data-source-lookup-class>
    <connection-factory-class>ru.cft.platform.core.container.connection.ConnectionFactory</connection-factory-class>
    <database-units defaultDatabaseType="main">
        <database-unit alias="DB_UNIT_NAME">
            <database type="main">
                <data-source-srv>main</data-source-srv>
                <data-source-adm>adm</data-source-adm>
                <data-source-sec>security</data-source-sec>
            </database>
        </database-unit>
    </database-units>
</cda-configuration>
```

4.4.9.4. pool-settings.xml

В файл pool-settings.xml нужно добавить настройки пула соединений, имя которого задается в файле cda_settings.xml.

В качестве пользователя, от имени которого устанавливается соединение с БД, необходимое для синхронизации групп пользователя, можно указать:

- владельца схемы;
- пользователя с ролью Администратор доступа;

Пример:

```
<?xml version="1.0" encoding="windows-1251"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
    <entry key="ucp-0.alias">main</entry>
    <entry key="ucp-0.driver-
    url">core:main:jdbc:oracle:thin:@server:1541:db_sid</entry>
    <entry key="ucp-0.factory-class">oracle.jdbcftc.CoreConnectionDriver</entry>
    <entry key="ucp-0.user">usr</entry>
    <entry key="ucp-0.password">pwd</entry>
    <entry key="ucp-0.initial-connection-count">1</entry>
    <entry key="ucp-0.minimum-connection-count">1</entry>
    <entry key="ucp-0.maximum-connection-count">150</entry>
    <entry key="ucp-0.inactive-connection-timeout">60</entry>
    <entry key="ucp-0.timeout-check-interval">1</entry>
    <entry key="ucp-1.alias">adm</entry>
    <entry key="ucp-1.driver-
    url">core:adm:jdbc:oracle:thin:@server:1541:db_sid</entry>
    <entry key="ucp-1.factory-class">oracle.jdbcftc.CoreConnectionDriver</entry>
    <entry key="ucp-1.user">usr</entry>
    <entry key="ucp-1.password">pwd</entry>
    <entry key="ucp-1.initial-connection-count">1</entry>
    <entry key="ucp-1.minimum-connection-count">0</entry>
    <entry key="ucp-1.maximum-connection-count">150</entry>
    <entry key="ucp-1.inactive-connection-timeout">60</entry>
    <entry key="ucp-1.timeout-check-interval">1</entry>
    <entry key="ucp-2.alias">security</entry>
    <entry key="ucp-
    2.driverurl">core:adm:jdbc:oracle:thin:@server:1541:db_sid</entry>
    <entry key="ucp-2.factory-class">oracle.jdbcftc.CoreConnectionDriver</antry>
    <entry key="ucp-2.user">usr</entry>
    <entry key="ucp-2.password">pwd</entry>
    <entry key="ucp-2.initial-connection-count">1</entry>
```

```
    <entry key="ucp-2.minimum-connection-count">0</entry>
    <entry key="ucp-2.maximum-connection-count">150</entry>
    <entry key="ucp-2.inactive-connection-timeout">60</entry>
    <entry key="ucp-2.timeout-check-interval">1</entry>
</properties>
```

4.4.10. Настройка внешнего пула соединений

Необходимо настроить два пула соединений: для инициализации пользовательских запросов и для открытия/закрытия сессий.

4.4.10.1. Настройка параметров

В конфигурационном файле cda-settings.xml следует:

1. Установить значение ru.cft.platform.core.dao.datasource.impl.xa.JNDIDataSourceLookup параметру data-source-lookup-class.
2. Установить параметрам data-source-srv и data-source-adm значения имен пулов (JNDI name), созданных при настройке сервера.

Примечание:

Создание пулов соединений выполняется по инструкции соответствующего СП.

4.4.11. Создание хранилища с сертификатами

Используемая утилита keytool входит в состав JVM. Обо всех доступных опциях этой утилиты можно узнать на официальном сайте Oracle.

Хранилище формируется командой:

keytool -genkey -keystore server.jks -dname "CN=commonName, OU=organizationUnit, O=organizationName, L=localityName, ST=stateName, C=RU" -storepass storepass -alias selfGeneratedCert -keypass serverpass

По итогу в каталоге, из которого команда была запущена, сформируется хранилище с именем server.jks, паролем к хранилищу storepass, сгенерированным самоподписанным сертификатом с алиасом selfGeneratedCert и паролем к этому сертификату serverpass. Делается это так потому, что нельзя сформировать пустое хранилище без сертификатов. Этот сертификат в дальнейшем не понадобится.

Рекомендуется в keystore не использовать alias-ы, отличающиеся только регистром.

Если требуется, чтобы хранилище сформировалось по определённому пути, то в качестве имени хранилища следует указать этот путь, включающий и название хранилища.

Опция keystore задает имя файла-хранилища. Если её не указать, тогда keytool создаст файл с именем .keystore в домашнем каталоге пользователя.

Доступ к keystore защищается паролем. Опция -storepass указывает пароль для доступа к keystore целиком. Этот пароль необходим для возможности модификации keystore.

Второй пароль необходим для доступа к отдельному алиасу внутри keystore. Указывается с помощью опции -keypass.

По умолчанию хранилище создастся в формате JKS. Для тех целей, для которых создаётся это хранилище этого формата достаточно. О других форматах хранилища и способах конвертации с помощью keytool можно узнать на официальном сайте Oracle.

Для добавления существующих сертификатов следует воспользоваться командой:

keytool -import -keystore server.jks -file cert.cer -storepass storepass - alias myCert

По итогу в хранилище server.jks окажется сертификат server.cer с паролем доступа у нему storepass и алиасом myCert.

Для просмотра содержимого и типа хранилища следует воспользоваться командой:

keytool -list -keystore server.jks -storepass storepass

Для удаления сертификата из хранилища следует воспользоваться командой:

keytool -delete -alias keyAlias -keystore keystore-name -storepass password,

где:

- keyAlias – алиас удаляемого сертификата,
- keystore-name – путь до хранилища,
- password – пароль к хранилищу.

4.5. Сервис заданий

Механизм выполнения заданий по расписанию предназначен для автоматического запуска заданий (операций ТБП или произвольных исполняемых блоков) по расписанию в указанное время или с заданной периодичностью без непосредственного участия пользователя. Подсистема позволяет настроить выполнение определённых длительных операций, работающих с большими объёмами данных, в вечернее или ночное время при низкой активности работы системы.

Примечание:

Настройка сервиса заданий производится только при необходимости для бизнес-задач.

4.5.1. Настройка сервиса серверов заданий Сервера приложений

Для работы СП необходимо сконфигурировать файл job-settings.xml.

Файл следует расположить в том же каталоге, в котором находятся другие конфигурационные файлы.

Описание содержимого файла:

- Имя узла СП или нескольких узлов, использующихся для запуска сервиса обработки заданий. Настройка обязательная.

<entry key="job.machine"><название компьютера>,<название компьютера></entry>

Если в settings.xml задано значение настройки server.uid, то это же значение следует указать вместо <название компьютера> (см. раздел settings.xml).

- Индекс сервера, который будет выполнять задания, соответствующие этому индексу. Соответствует колонке c_srv в заданиях по расписанию. По умолчанию в СП значение 0. Настройка необязательная.

<entry key="job.server"><число></entry>

- Максимальное количество заданий, которое может выполняться на СП. По умолчанию значение -1 (неограниченно). Настройка необязательная.

<entry key="job.max-tasks"><число></entry>

- Максимальное количество выполняемых заданий с заданными кодами [код задания 1]: [количество выполняемых заданий с этим кодом 1];...;[код задания N]:[количество выполняемых заданий с этим кодом N]. Настройка необязательная.

<entry key="job.mask-tasks"><маска>:<ограничение></entry>

- Количество заданий, которое СП может обрабатывать одновременно. По умолчанию в СП значение 2. Настройка необязательная.

<entry key="job.maxRunInOnce"><число></entry>

- Параметр, позволяющий выполнять на СП только задания с маской. Если маски не указаны и параметр равен true, то обработчик заданий будет работать как будто параметра нет. Настройка необязательная, по умолчанию false.

<entry key="job.runOnlyMask">true/false</entry>

Пример:

```
<?xml version="1.0" encoding="windows-1251"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
    <entry key="job.machine">machine_1,machine_2</entry>
    <entry key="job.server">4</entry>
    <entry key="job.max-tasks">5</entry>
<entry key="job.maxRunInOnce">5</entry>
<entry key="job.mask-tasks">qa:2;q:1</entry>
<entry key="job.runOnlyMask">false</entry>
</properties>
```

5. УСТАНОВКА И НАСТРОЙКА КЛИЕНТСКОЙ ЧАСТИ

Для корректной работы пользователей требуется установка АРМ «ЦФТ-Навигатор».

5.1. Системные требования

5.1.1. Поддерживаемые версии операционных систем

В качестве PC рекомендуется использовать персональные компьютеры конфигурации, удовлетворяющей требованиям следующих версий операционной системы (далее – ОС), приведённых в таблице 2.

Таблица 2

АРМ «ЦФТ-Навигатор»	Windows 10 (x32, X64)	Windows Server 2012 R2	Windows Server 2016	Windows Server 2019	Windows Server 2008 R2 SP1	Windows 8.1 (x32, X64)	Windows 7 SP (x32, X64)	Windows Vista SP1 (x32)
	✓	✓	✓	✓	✓	✓	✓	✓

Работа с ОС Windows Server

Следует иметь в виду, при удалённой работе с АРМ «ЦФТ-Навигатор» на Windows Server 2012 R2 в режиме RemoteApp возможно появление проблем, связанных с особенностями работы RemoteApp, которые не зависят от конкретного приложения и могут проявляться для любого приложения системы.

Работа с ОС Windows 7

Для работы в АРМе «ЦФТ-Навигатор» в ОС Windows 7 следует использовать персональные компьютеры с 2 ГБ оперативной памяти и более, а также с индексом производительности не менее 3.

Примечание

Рекомендуется использовать русские редакции ОС Microsoft Windows. Возможно использование интернациональных или панъевропейских редакций при условии их корректной русификации.

Важно!

При настройке клиентского места на 64-разрядных ОС следует иметь в виду следующее:

- программа Рабочее место Оператора «ЦФТ – Платформа развития» устанавливается в каталог C:\Program Files (x86)\;

- 32-разрядные библиотеки регистрируются в каталоге C:\Windows\SysWOW64\;
- в реестре используются ветки ...\Software\Wow6432Node\....;
- формат даты в ОС должен соответствовать формату DD/MM/YYYY.

5.1.2. Программное обеспечение, устанавливаемое на рабочие станции

Дополнительное ПО, устанавливаемое на РС пользователя	АРМ «Навигатор»
Рабочее место Оператора «ЦФТ–Платформа развития»	
Компонент безопасности SKSB версии 1.10.0.3 Примечание Перед установкой необходимо установить 32 разрядный распространяемый пакет Microsoft Visual C++ 2010 (x86)	**Примечание:** 1) если для входа в АРМ запрашивается наличие сертификата; 2) если необходимо предъявлять лицензию с уровнем доступа
Microsoft .Net Framework 4.5.2	
32 разрядный распространяемый пакет Microsoft Visual C++ 2010 (x86)	
32 разрядный распространяемый пакет Microsoft Visual C++ 2013 (x86)	

Дополнительные условия

Перед установкой необходимого ПО следует убедиться, что на персональных компьютерах с поддерживаемыми версиями ОС Windows установлен MSXML 6.0 SP2. При необходимости данные компоненты можно загрузить с официального сайта Microsoft.

Примечание

Хотя в подавляющем большинстве случаев проблем совместимости ПО «ЦФТ – Платформа Развития» с ПО третьих фирм не возникает, корректная работа системы гарантируется только при выполнении вышеописанной процедуры инсталляции и отсутствии любого ПО, установленного на компьютере и не описанного выше. При необходимости использовать на рабочем месте какое-либо иное ПО следует проконсультироваться со службой

технической поддержки на предмет совместимости данного ПО с ПО «ЦФТ – Платформа Развития».

5.2. Установка Рабочего места Оператора

Для работы с АРМ «ЦФТ – Навигатор» требуется установить программу Рабочее место Оператора. Установка производится для всех пользователей Windows на PC.

Для установки **Рабочего места Оператора** следует:

1. Находясь в личном кабинете клиента на сайте сопровождения https://support.cft.ru скачать архив с установочными файлами.
2. Распаковать их в произвольный установочный каталог, следуя инструкциям.
3. В установочном каталоге выбрать файл вида InstallNovo {версия} .msi
4. Однократным щелчком правой кнопки мыши вызвать контекстное меню и выбрать в нем команду **Установить**. Запустится программа установки **Рабочее место Оператора** (рисунок 6).

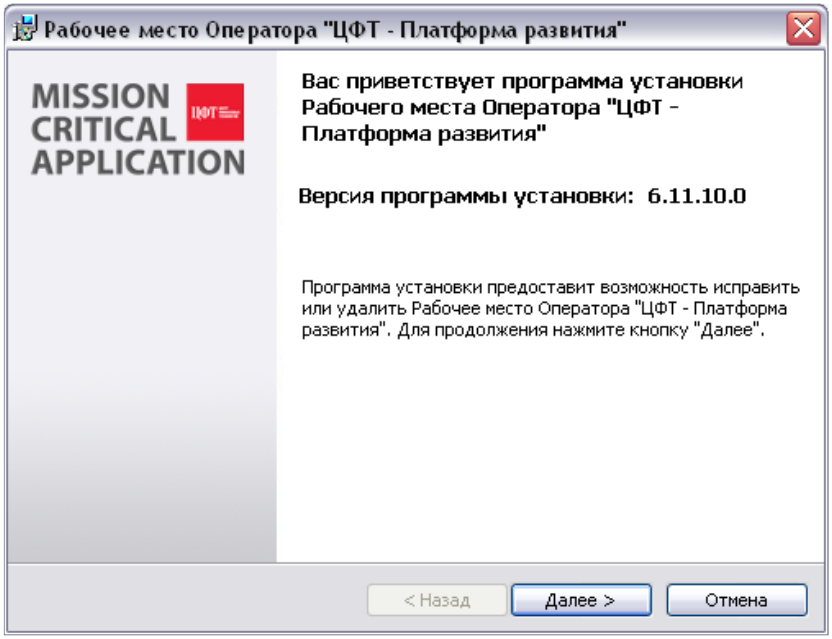


Рисунок 6

5. Перейти к следующему шагу установки щелчком по кнопке **Далее**. В окне Устанавливаемые компоненты отобразятся **Компоненты АРМ «ЦФТ –Навигатор».** Отказаться от их установки нельзя (рисунок 7).

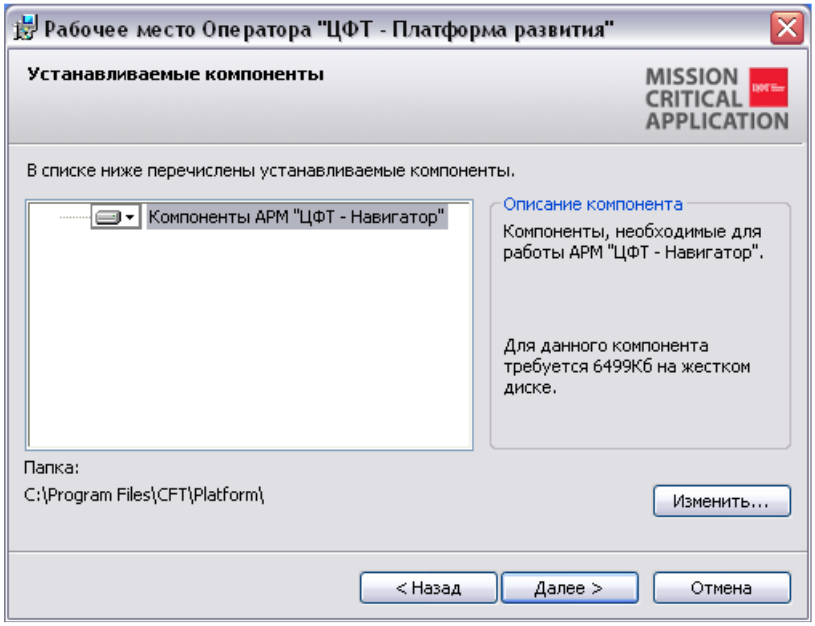


Рисунок 7

По умолчанию для установки выбранных компонентов указана папка C:\Program Files\CFT\Platform. Для 64-разрядных ОС указывается папка C:\Program Files (x86)\CFT\Platform. Переопределить папку назначения можно в диалоговом окне, которое открывается по кнопке **Изменить…**.

Переход к следующему шагу работы в окне программы установки осуществляется по кнопке **Далее**, возврат на предыдущий шаг работы с возможностью внести изменения – по кнопке **Назад**. Прервать работу и выйти из программы установки можно по кнопке **Отмена**.

6. Запустить процесс установки **Рабочего места Оператора** щелчком по кнопке **Установить**.
7. После завершения процесса установки выход из программы установки осуществляется по кнопке **Готово**.
8. В указанной для установки папки появится значок «АРМ «ЦФТ-Навигатор».

Если на PC пользователя уже установлена более ранняя версия **Рабочего места Оператора**, то возможны следующие варианты действий:

А) Удаление имеющейся на PC пользователя версии **Рабочего места Оператора** штатными средствами Windows для удаления программ, а затем установка новой версии с последующим запуском нового установочного файла.

Б) Установка новой версии программы без удаления предыдущей версии.

Если старый установочный файл находится в той папке, откуда его устанавливали, программа автоматически удалит старую версию **Рабочего места Оператора** и установит новую. Если старый установочный файл был перемещён или удалён, программа в процессе установки выдаст сообщение о том, что нужный файл недоступен (рисунок 8). В сообщении путь к файлу можно указать в поле

Использовать источник или выбрать нужный файл с помощью кнопки **Обзор**, и нажать кнопку **ОК** для продолжения установки.

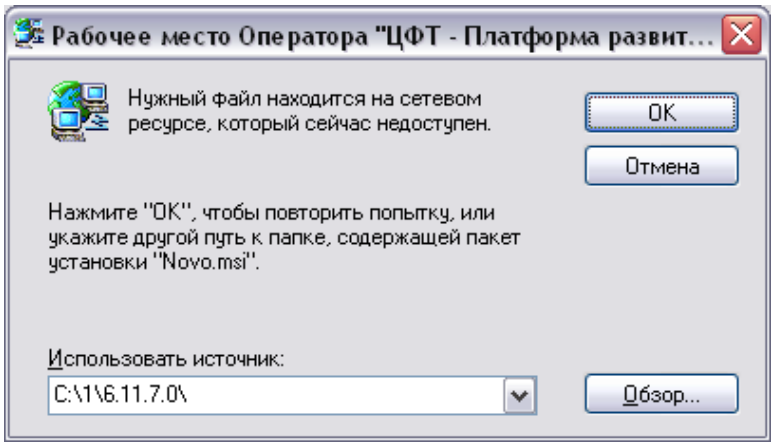


Рисунок 8

Если по данному пути файл недоступен, то данное сообщение появится снова. По нажатии кнопки **Отмена** установка будет продолжена и завершена **успешно**.

В этом случае в разделе «Установка и удаление программ» в списке программ будут отображаться обе версии **Рабочего места Оператора**. В дальнейшем удаление предыдущей версии возможно при наличии соответствующего установочного файла. Новую версию программы данное удаление не затронет.

5.2.1. Установка и удаление в «тихом» режиме

Программа **Рабочее место Оператора** (установочный файл вида **InstallNovo {версия} .msi**) может быть установлена и удалена в «тихом» режиме.

Для этого в командной строке следует прописать следующие команды:

1. Для «тихой» установки в произвольный каталог:

msiexec /i <название установочного файла> /quiet

2. Для «тихой» установки в заданный каталог:

msiexec /i <название установочного файла> /quiet INSTALLDIR="<путь до необходимой папки>"

3. Для удаления программы:

msiexec /x <название инсталлятора> /quiet

5.3. Установка АРМов

АРМы, необходимые для работы пользователя, могут быть установлены в каталог файлового сервера, доступ к которому разрешен пользователям, или локально, на PC пользователя.

Установка АРМов заключается в копировании исполняемого файла в заданный каталог и предоставлении пользователю прав на чтение данного файла.

5.3.1. Установка АРМов в каталог файлового сервера

1. Создать на файловом сервере произвольный каталог, в котором будут располагаться АРМы, необходимые для работы пользователя.
2. Скопировать в него АРМы.
3. Дать права пользователям на чтение файлов в данном каталоге.
4. Создать на РС ярлык на необходимые АРМы.

5.3.2. Установка АРМов на рабочей станции пользователя

1. Скопировать АРМы в каталог на РС пользователя.
2. Дать права пользователям на чтение файлов в данном каталоге.
3. Создать на рабочем столе РС пользователя ярлык на необходимый АРМ.

6. ЭКСПЛУАТАЦИЯ И ОБСЛУЖИВАНИЕ СИСТЕМЫ

6.1. Управление серверными компонентами системы

Проверка общей работоспособности всех серверных компонент системы выполняется администратором в процессе их обслуживания и при проведении работ по техническому обслуживанию оборудования имеющимися в организации техническими и программными средствами, с периодичностью и в соответствии с внутренней регламентной документацией организации, а также согласно указаниям технической документации производителя соответствующих средств и требованиям по эксплуатации, указанным в формуляре RU.23578167.00001-01 30.

Для проверки подписей исполняемых файлов и файлов конфигурации Системы используется стандартная утилита jarsigner из состава JDK\JRE. Рекомендуется скачать ее с официального сайта производителя и сохранить на PC администратора в произвольный каталог. После чего необходимо запустить утилиту, указав полный путь до места расположения проверяемого файла.

Пример для вызова:

jarsigner -verify -verbose D:\Apps\cft-platform-ide-2mca\plugins\ru.cft.platform.deployment.index_1.0.239.jar > d:\temp\verify.txt

Если проверка прошла успешно, то в файле выходных данных (verify.txt), путь до которого указан в команде вызова, отображается результат:

jar verified

Проверка подписей исполняемых файлов и файлов конфигурации Системы осуществляется в следующих случаях:

- при каждой установке обновления Системы;
- с периодичностью, указанной во внутренней регламентной документации организации.

Также рекомендуется производить контроль целостности неизменяемых файлов, входящих в дистрибутив Системы. Перечень файлов с указанием контрольных сумм приведен в Приложении А формуляра RU.23578167.00001-01 30. Контрольные суммы рассчитываются с использованием программы фиксации и контроля целостности информации «ФИКС» (версия 2.0.2) (сертификат № 1548, выдан ФСТЭК России 15 января 2008 года) по алгоритму «Уровень 3, программно».

Контроль целостности неизменяемых файлов осуществляется во всех вышеперечисленных случаях, а также перед установкой Системы.

Если при проверке контрольные суммы не совпадают, администратору рекомендуется обратиться в службу по сопровождению Системы.

6.2. Управление базой данных

В процессе эксплуатации БД администратором выполняются следующие работы:

- настройка и контроль периодического резервного копирования БД и образов виртуальной машины (далее – ВМ) (в ручном или автоматическом режиме);
- участие в восстановлении БД и образов ВМ после сбоев оборудования, вызвавших повреждение структуры файлов, или при переносе системы на другое оборудование;
- обновление текущей версии БД.

Периодическое резервное копирование образов ВМ и полной копии БД является одной из мер защиты данных при авариях и сбоях работы оборудования. Резервное копирование образов ВМ рекомендуется выполнять до и после установки обновлений ОС, системного и вспомогательного ПО. Резервное копирование файлов БД рекомендуется выполнять перед установкой обновлений ОС и СУБД на сервере БД.

Периодичность резервного копирования образов ВМ и файлов БД, а также последовательность действий администратора регламентируется:

- внутренней организационно-распорядительной документацией организации;
- технической документацией, размещенной на сайте производителя БД – https://postgrespro.ru/ (для создания копий файлов БД);
- руководствами и инструкциями от производителя соответствующих средств виртуализации.

7. УПРАВЛЕНИЕ УЧЕТНЫМИ ЗАПИСЯМИ ПОЛЬЗОВАТЕЛЯ

В процессе эксплуатации Системы администратор посредством АРМ «Администратор доступа» может реализовывать следующие действия по управлению УЗ пользователей:

- создание, редактирование, блокирование УЗ пользователей;
- создание, редактирование групп;
- включение пользователей в группу (группы);
- просмотр записей регистрации событий безопасности.

7.1. Интерфейс АРМ «Администратор доступа»

7.1.1. Основное меню

Процесс запуска АРМ «Администратор доступа» подробно описан в разделе «Запуск АРМ «Администратор доступа». Создание администратора доступа».

Следует помнить, что после создания первого администратора доступа и выключения в файле application.properties возможности доступа по паролю, доступ к АРМ «Администратор доступа» возможен только по данным УЗ в системе ADFS (рисунок 9).

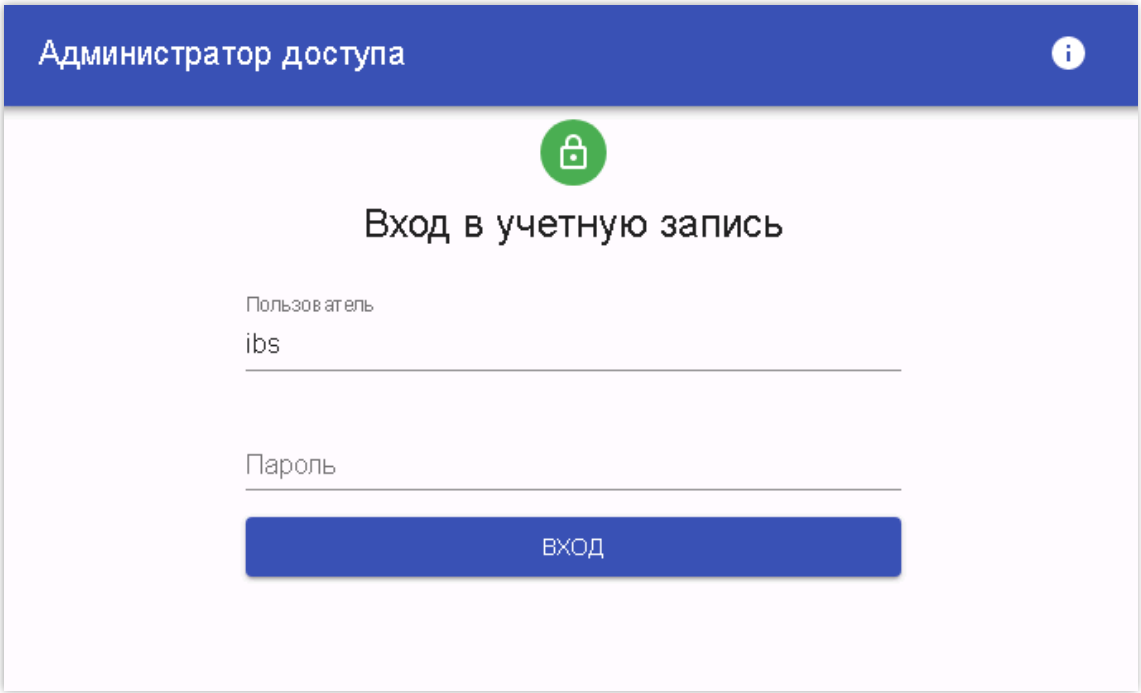


Рисунок 9

При успешной авторизации в АРМе администратору становится доступно основное меню, включающее в себя следующие элементы управления:

7.1.1.1. Окно Пользователи

По щелчку левой кнопкой мыши на пункт **Пользователи** происходит вызов окна для создания УЗ новых пользователей, а также для просмотра и модификации списка уже созданных пользователей (рисунок 10).

Здесь в виде таблицы представлены свойства пользователя:

- Имя;
- Полное имя;
- Статус.

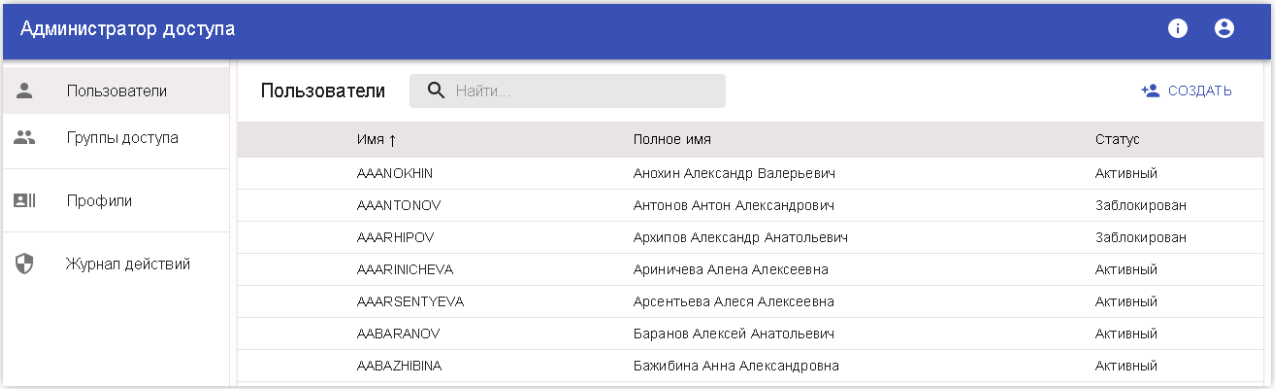


Рисунок 10

Подробнее о свойствах пользователя см. раздел Свойства пользователя.

7.1.1.2. Окно Группы доступа

По щелчку левой кнопкой мыши на пункт меню **Группы доступа** происходит вызов окна для создания группы (групп) доступа, загрузки группы (групп) доступа, а также просмотра уже созданных групп доступа (рисунок 11).

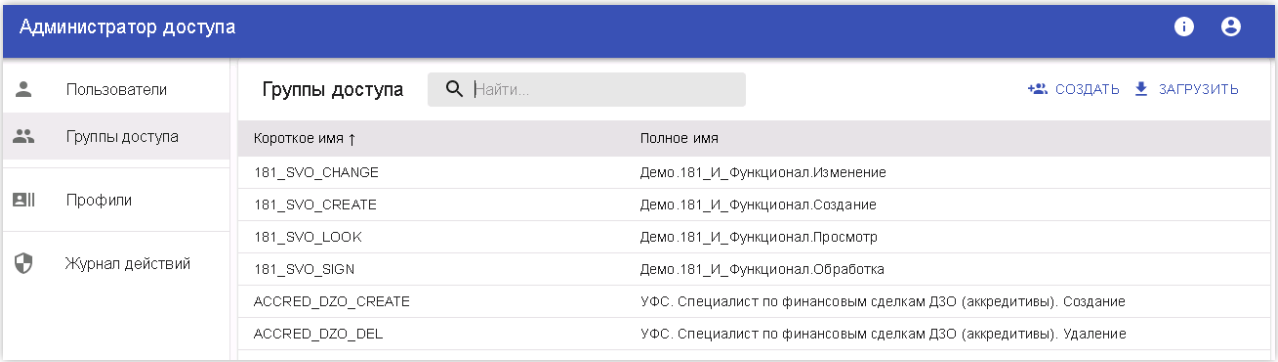


Рисунок 11

Подробнее о группах доступа см. разделы Создание группы доступа, Свойства группы доступа, Удаление группы доступа.

7.1.1.3. Окно Профили

По щелчку левой кнопкой мыши на пункт меню Профили происходит вызов окна Профили пользователей (рисунок 12). Окно содержит список возможных профилей для пользователей и набор свойств для каждого профиля.

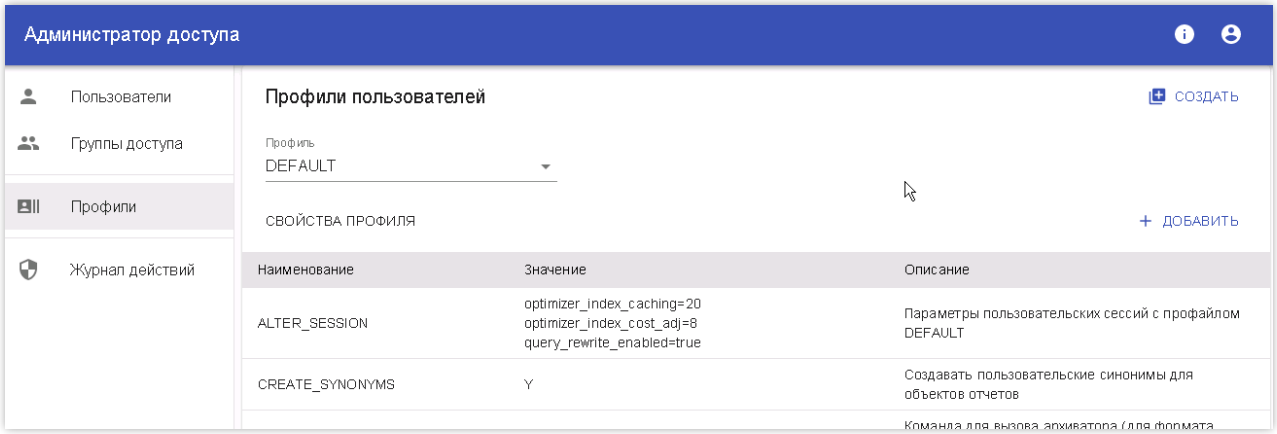


Рисунок 12

Подробнее см. раздел [Профили пользователей](#).

7.1.1.4. Окно Журнал действий

По щелчку левой кнопкой мыши на пункт меню Журнал действий происходит вызов окна для просмотра журнала с описанием выполненных в АРМ «Администратор доступа» действий пользователей (рисунок 13).

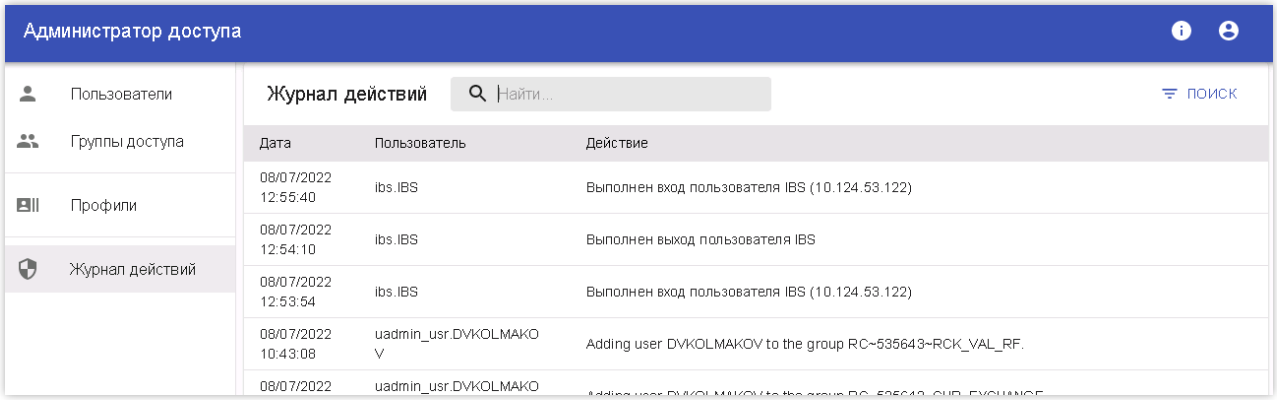


Рисунок 13

Журнал действий содержит перечень действий пользователей в АРМе и позволяет определить, кем и когда были выполнены конкретные действия по администрированию доступа в системе. Окно имеет вид таблицы со следующими столбцами:

- Дата – дата и время совершения действия;
- Пользователь – сетевое имя пользователя, выполнившего действие;

- Действие – расшифровка выполненных действий. В расшифровке описан субъект или объект, над которым производились манипуляции, и их краткая суть. Количество страниц журнала действий отображается в правом нижнем углу таблицы. Просмотреть следующую или предыдущую страницу списка действий можно по нажатию на стрелки ← и → (рисунок 14).

09/09/2021 19:55:13	uadmin_usr.GES	Выполнен вход пользователя GES (10.5.19.191)
09/09/2021 19:54:40	uadmin_usr.GES	Выполнен выход пользователя GES
09/09/2021 19:54:35	uadmin_usr.GES	Выполнен вход пользователя GES (10.5.19.191)
09/09/2021 19:32:02	uadmin_usr.GES	Выполнен выход пользователя GES
09/09/2021 18:58:56	uadmin_usr.GES	Выполнен вход пользователя GES (10.5.19.191)

3 из 21

Рисунок 14

7.1.2. Поиск и сортировка данных

В окнах Пользователи, Группы доступа и Журнал действий можно воспользоваться функцией поиска данных. Для этого в поле Найти рядом со значком 🔍 следует ввести любое количество значимых или служебных символов (рисунок 15).

Пользователи 🔍 Найти...

Имя	Полное имя
TEST_DBI1	TEST_DBI1
UADMIN	UADMIN
UADMIN2	UADMIN2
OPERATOR1	Оператор 1

Рисунок 15

Данные в столбцах таблиц окон Пользователи, Группы доступа, Журнал действий, могут быть также отсортированы по возрастанию или убыванию признака, указанного в заголовке столбца (например, по алфавиту, по дате). Для сортировки необходимо однократно щелкнуть левой кнопкой мыши по произвольному столбцу. Рядом с заголовком столбца появится значок ↑ или ↓, означающие сортировку по возрастанию или убыванию.

В окне Журнал действий доступна также функция поиска по заданным параметрам:

- Пользователь
- Действие
- Дата с…
- Дата по…

Чтобы произвести поиск, необходимо однократно щелкнуть левой кнопки мыши на кнопку поиск, в открывшемся окне заполнить одно или несколько полей и нажать на кнопку **Найти**. Очистить поля поиска можно по кнопке **Сбросить всё**. Выйти из окна поиска можно по нажатию на кнопку **Закрыть** или однократному щелчку левой кнопкой мыши в произвольном месте окна (рисунок 16).

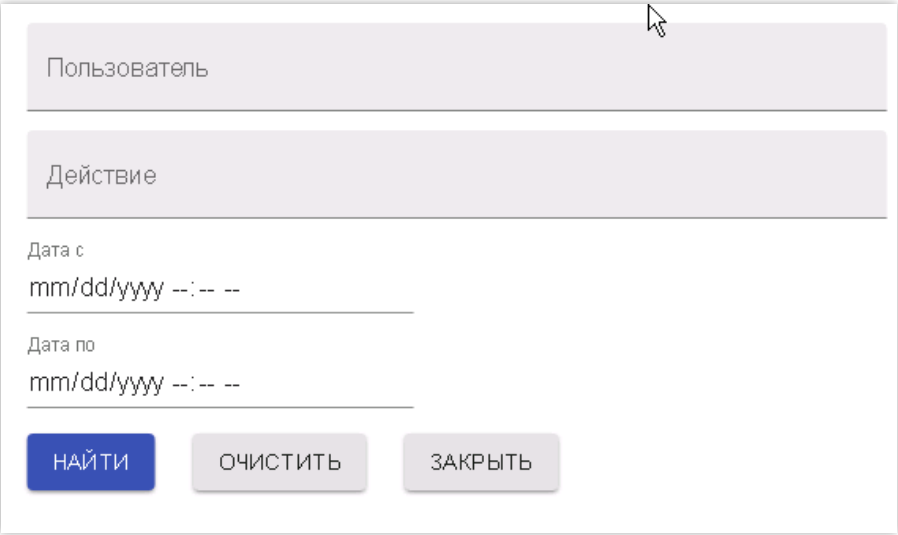


Рисунок 16

7.1.3. Выход из АРМа

Выход из АРМ «Администратор доступа» осуществляется по нажатию левой кнопкой мыши по значку в правом верхнем углу окна АРМа.

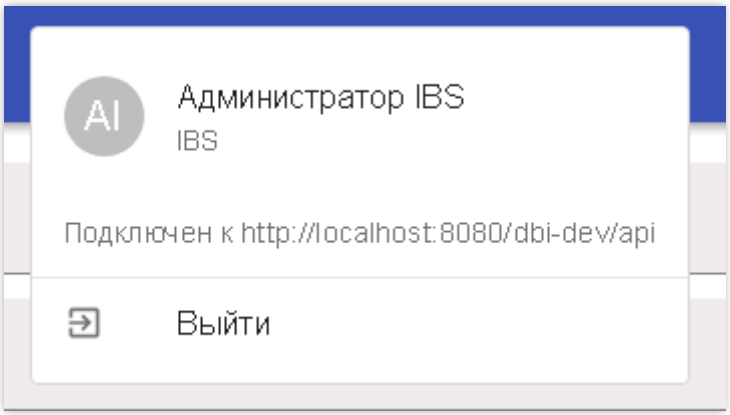


Рисунок 17

7.2. Работа с субъектами доступа

7.2.1. Создание первого администратора доступа

Для работы в Системе необходимо создать первого администратора доступа – пользователя с правом создавать дальнейших пользователей-операторов.

Для этого рекомендуется выполнить следующую последовательность действий:

1. Создать в системе аутентификации (ADFS) УЗ пользователя с параметрами, соответствующими параметрам пользователя IBS. Пароль данного пользователя рекомендуется разделить на несколько частей и обеспечить распределенное хранение каждой части разными сотрудниками.
2. В АРМ «Администратор доступа» авторизоваться под предзаданной УЗ суперпользователя IBS (рисунок 18).

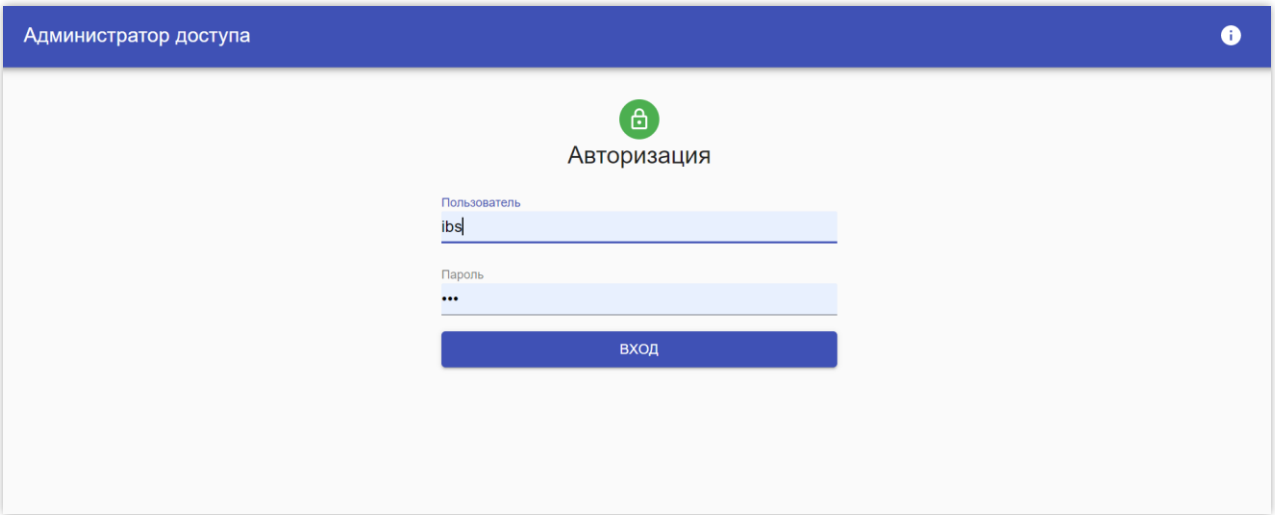


Рисунок 18

3. Отредактировать УЗ IBS, задав во вкладке Аутентификация сетевое имя и домен, соответствующие УЗ пользователя IBS в ADFS (рисунок 19).

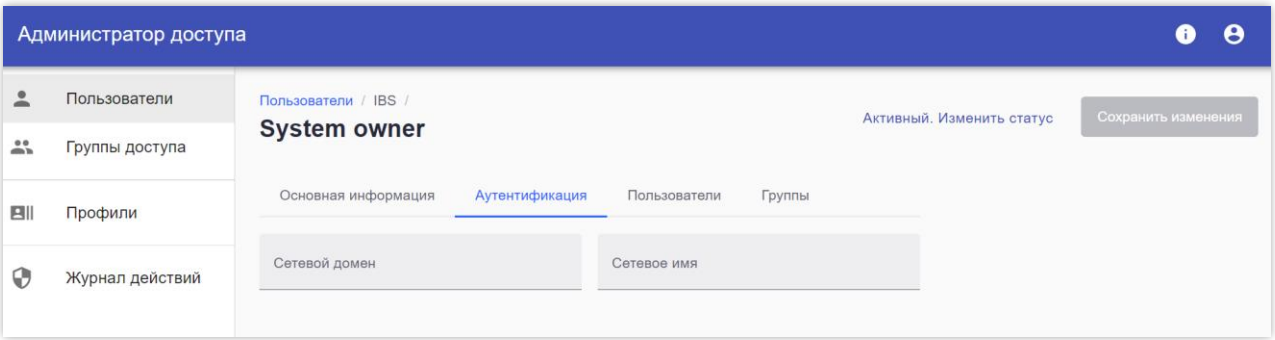


Рисунок 19

4. Создать пользователя с ролью Администратор доступа:

А) В окне Пользователи левой кнопкой мыши нажать кнопку **Создать**.

Б) Во вкладке Основная информация задать короткое и полное имя пользователя, соответствующие аналогичным данным в ADFS. Указать роль пользователя – Администратор доступа (рисунок 20).

В) В выпадающем списке Профиль выбрать необходимый профиль. Подробнее см. раздел Свойства пользовательских профилей.

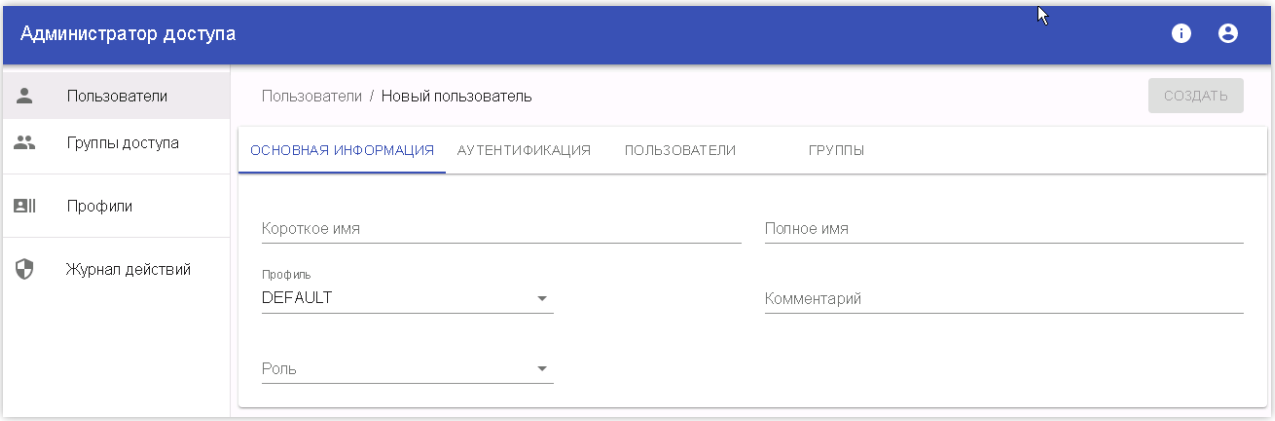


Рисунок 20

Г) Во вкладке Аутентификация указать сетевой домен и сетевое (короткое) имя – уникальный идентификатор пользователя на уровне всех субъектов доступа системы (рисунок 21).

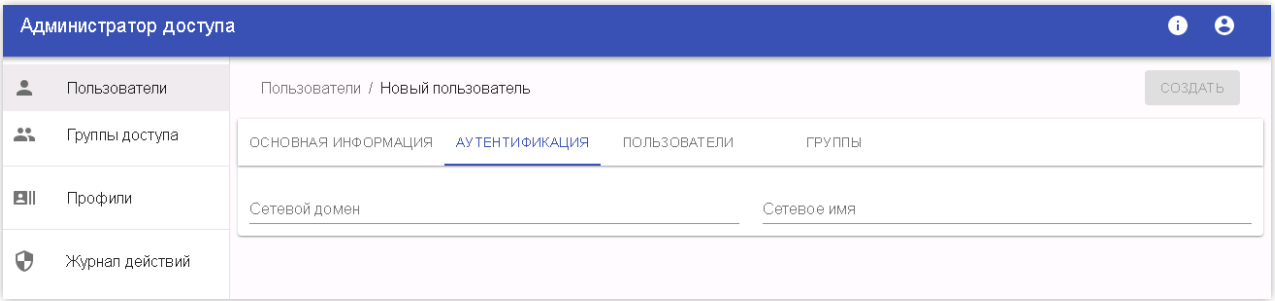


Рисунок 21

Д) Для сохранения изменений нажать кнопку **Создать**, которая после заполнения всех данных станет активной (синего цвета). Данные об УЗ Администратора доступа отобразятся в таблице в окне Пользователи.

Е) После создания первого администратора доступа в файле application.properties необходимо выключить возможность входа по паролю в АРМ «Администратор доступа» и оставить возможность доступа в АРМ только через аутентификацию по ADFS.

Пример:

useradmin.security.authorization= OAUTH2

7.2.2. Создание первого пользователя-оператора

Для создания первого пользователя в прикладной системе администратору рекомендуется выполнить следующую последовательность действий:

1. Зайти в АРМ «ЦФТ-Навигатор» под УЗ суперпользователя IBS.
2. В меню «Пользователи» выполнить операцию «Добавить».
3. Задать пользователю короткое (сетевое) имя – уникальный идентификатор пользователя на уровне всех субъектов доступа системы (пользователей и групп пользователей).

Следует иметь в виду, что короткое имя пользователя:

- должно быть заведено в верхнем регистре;
- не может быть пустым;
- не может начинаться с цифры или со служебных символов # и _;
- не должно содержать служебных символов: ",<>.~`@№^:;&*()+-][{}!?'|\/

7.2.3. Создание операторов

Чтобы иметь возможность работать с бизнес-данными посредством АРМ «ЦФТ-Навигатор», необходимо создать пользователя-оператора. Для этого следует создать в прикладной системе и системе доступа УЗ пользователя с одинаковыми характеристиками (короткими именем), проассоциировав («связав») тем самым две УЗ одного пользователя в разных системах.

Создание пользователя в прикладной системе осуществляется администратором доступа в АРМ «ЦФТ-Навигатор» под своей УЗ по алгоритму, описанному выше.

Для создания аналогичного пользователя–оператора (с тем же коротким именем) в системе доступа, администратору доступа необходимо:

1. Зайти в АРМ «Администратор доступа» под своей УЗ в системе ADFS (рисунок 22);

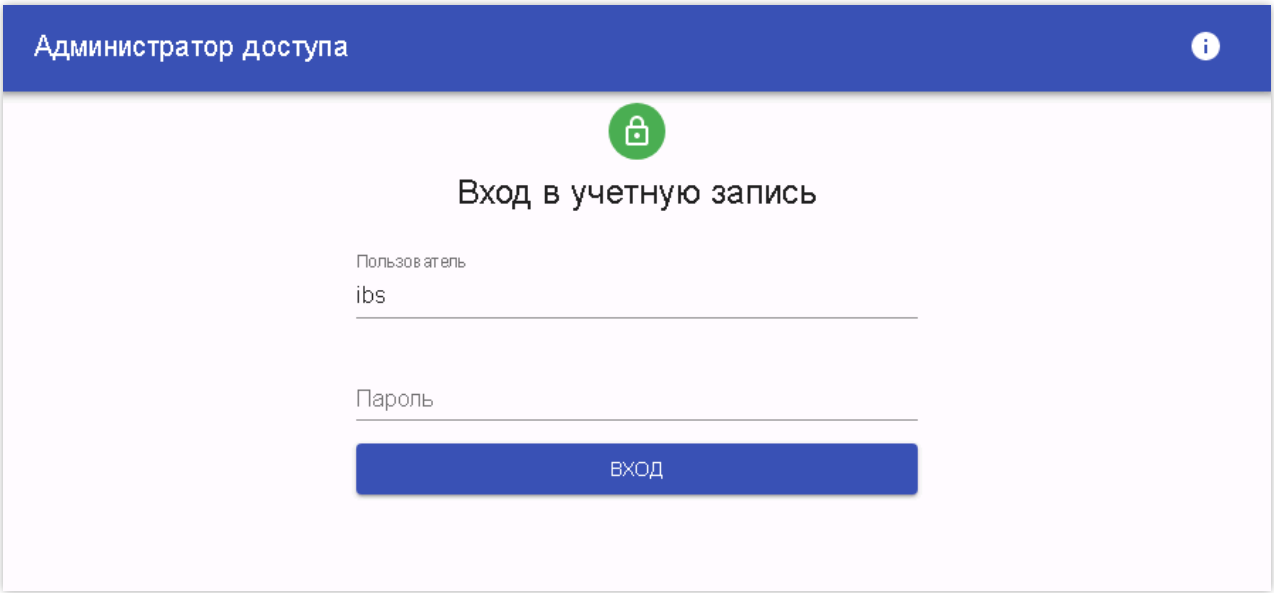


Рисунок 22

2. В окне Пользователи нажать кнопку **Создать** (рисунок 23).

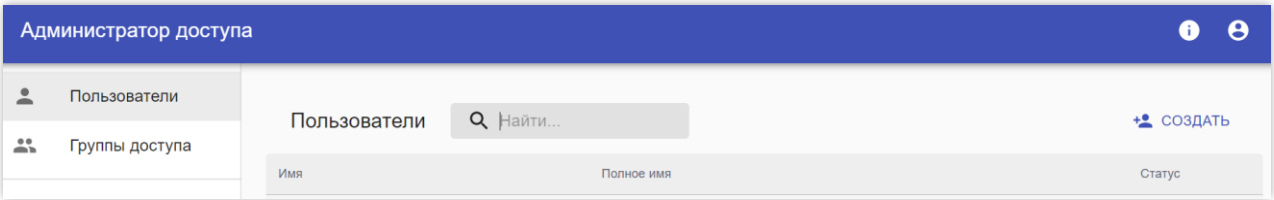


Рисунок 23

3. Указать для нового пользователя то же самое короткое (сетевое) имя, что было указано в прикладной системе.
4. В поле Профиль выбрать необходимый профиль пользователя. Подробнее см. раздел Профили пользователей.
5. Назначить новому пользователю роль Оператор.
6. Для сохранения введенных данных нажать кнопку **Создать**.
7. При успешном создании пользователя-оператора его данные отобразятся в таблице в окне Пользователи.

Примечание

Для исключения возможного бесконтрольного самостоятельного расширения пользователями представленных им прав логического доступа (в том числе к бизнес-функциям) администратор доступа не может создать другого администратора доступа.

7.2.4. Свойства пользователя

В окне Пользователи доступен просмотр и редактирование свойств УЗ пользователей.

> ***Примечание***
>
> *Суперпользователю (владельцу схемы) разрешено изменять некоторые собственные свойства, а также список сетевых адресов. Другие пользователи с ролью «Администратор доступа» не имеют права изменять собственные свойства.*

Доступ к свойствам осуществляется по щелчку левой кнопкой мыши на строчке выбранной УЗ. В открывшемся окне отображаются следующие характеристики:

- **Вкладка Основная информация** (рисунок 24):

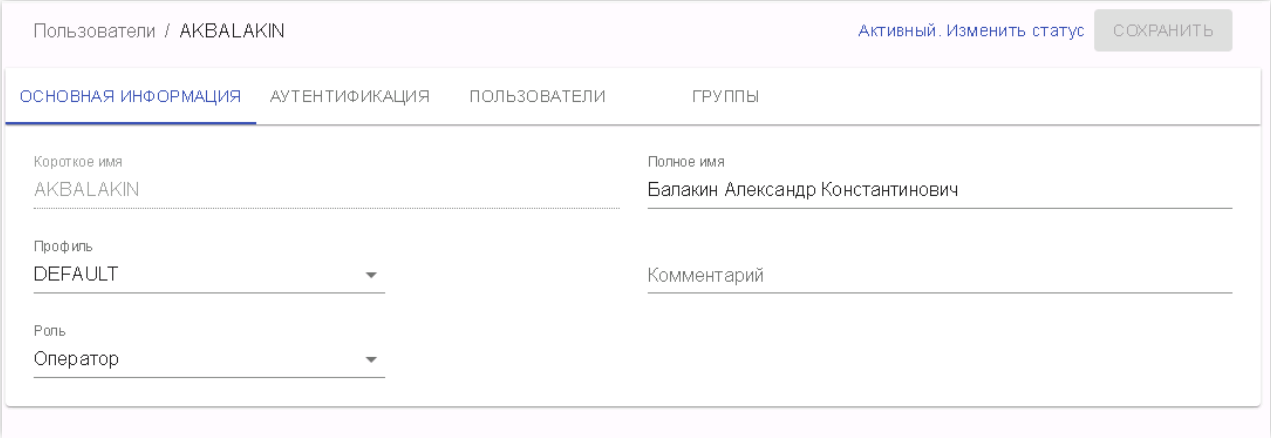


Рисунок 24

Короткое имя

Сетевое имя пользователя, которое является его идентификатором и должно быть уникальным на уровне всех субъектов доступа системы (пользователей и групп пользователей). Недоступно для редактирования.

Полное имя

Обычно это ФИО пользователя. Доступно для редактирования.

Профиль

Набор настроек системы, которые назначаются конкретному пользователю и учитываются при дальнейшей работе системы под данным пользователем. Профиль с нужными свойствами выбирается из выпадающего списка. Подробнее см. раздел Свойства пользовательских профилей.

Роль

Принадлежность к роли Оператор или Администратор доступа задается администратором доступа в момент создания УЗ. Невозможно одновременно назначить пользователю роль Оператора и Администратора доступа.

Статус

Поле является информационным и содержит текущий статус пользователя: Активный, Заблокирован. Доступно для редактирования. Подробнее см. раздел Блокирование и разблокирование пользователя.

- **Вкладка Аутентификация** (рисунок 25)

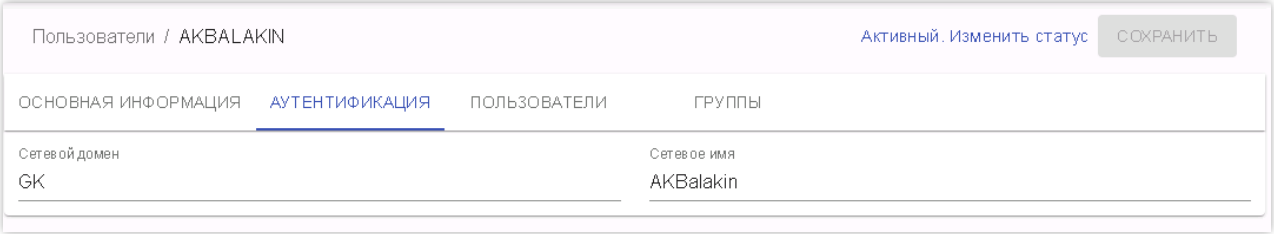


Рисунок 25

Поля Сетевой домен и Сетевое имя являются обязательными для заполнения. Заполняются согласно параметрам сети, в которой происходит работа. Значения пары этих полей должны быть уникальными. В противном случае при сохранении пользователя выдается сообщение об ошибке. Доступны для редактирования.

- **Вкладка Пользователи**

Во вкладке в виде двух панелей отображаются списки пользователей, которые передали или не передали права выбранному для просмотра и/или редактирования пользователю (подробнее см. раздел Передача прав пользователей).

Также доступна функция поиска пользователей по заданным параметрам. Для этого в поле Поиск необходимо ввести любое количество значимых или служебных символов (рисунок 26).

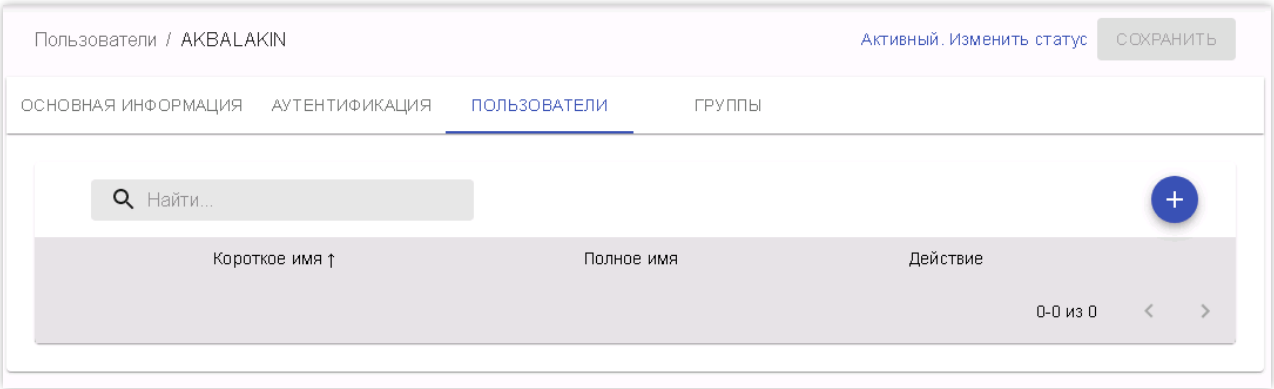


Рисунок 26

- **Вкладка Группы**

Здесь в виде двух панелей отображаются списки групп, в которые входит или не входит пользователь (рисунок 27).

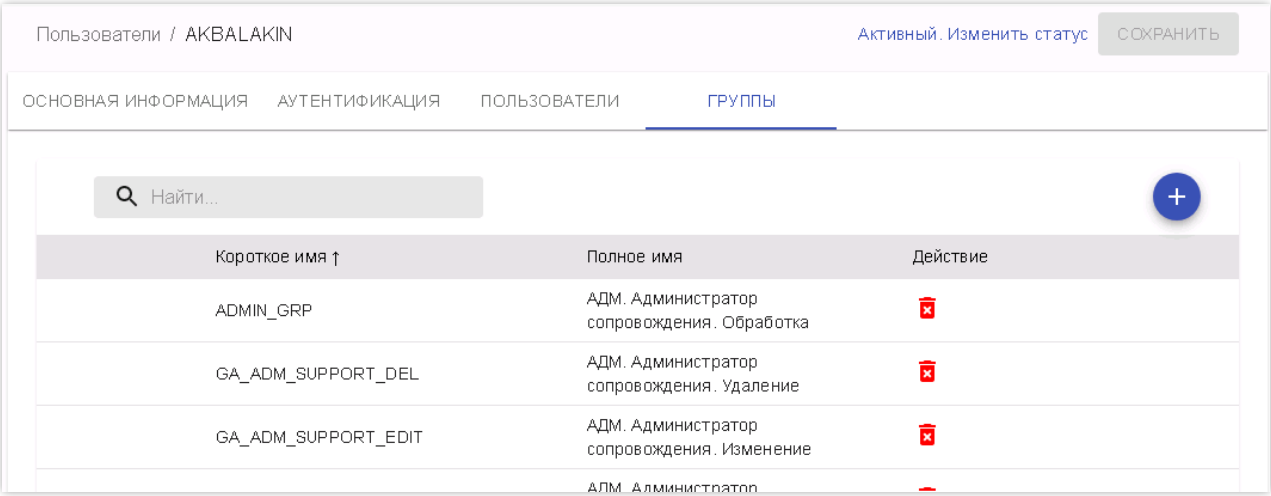


Рисунок 27

Подробнее см. раздел Создание группы доступа.

7.2.5. Изменение пароля

Изменение пароля пользователя осуществляется средствами системы аутентификации (ADFS).

7.2.6. Блокирование и разблокирование пользователя

Блокирование и разблокирование пользователя происходит посредством смены его текущего статуса: Активный или Заблокированный.

Чтобы изменить текущий статус пользователя необходимо щелкнуть левой кнопкой мыши на строчку с текущим статусом (например, Активный. Изменить статус) в правом верхнем углу окна АРМ «Администратор доступа. Затем в открывшемся модальном окне выбрать действие со статусом (например, **Блокировать**) (рисунок 28).

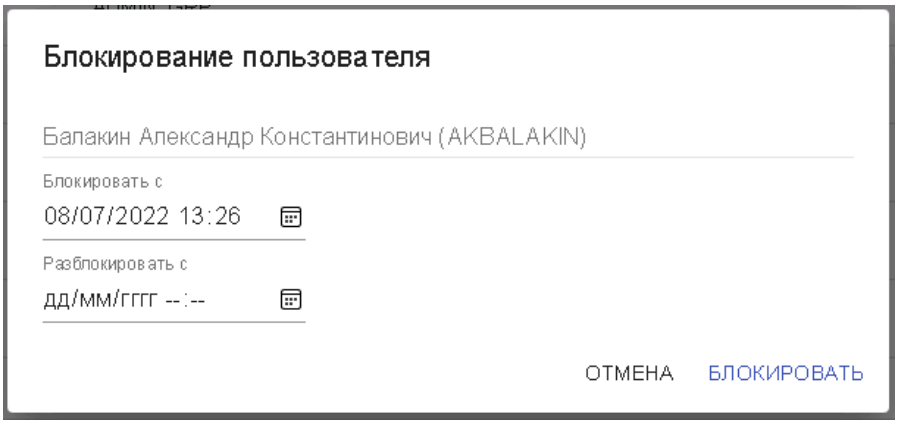


Рисунок 28

7.2.7. Создание группы доступа

Права пользователя на доступ к объектам определяются как совокупность (объединение) прав всех групп (иерархии групп), в которые он включен, и его личных прав.

Окно Группы доступа предназначено для создания новых групп, загрузки предварительно созданных, а также редактирования уже созданных групп. Механизм групп позволяет оптимизировать распределение и администрирование однотипных наборов прав нескольким пользователям (рисунок 29).

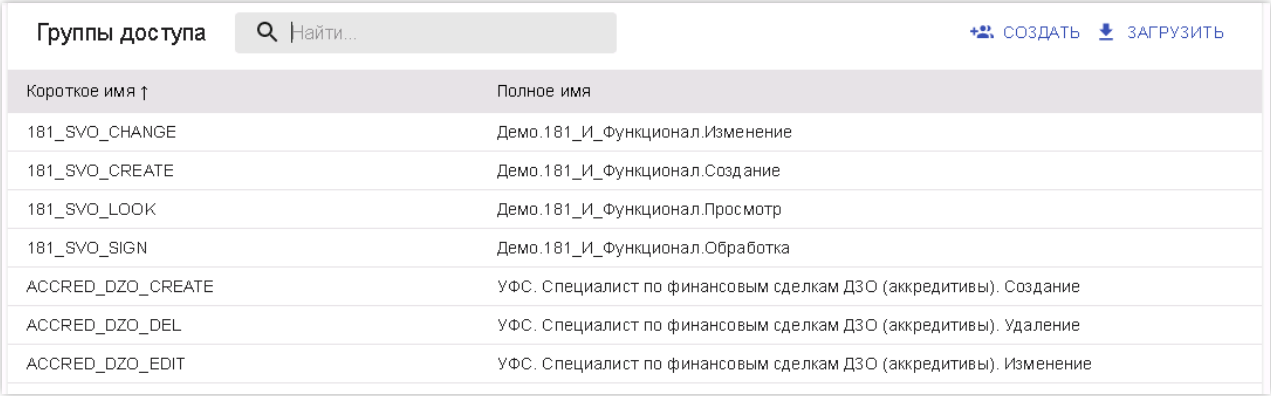


Рисунок 29

В данном окне доступны следующие действия:

- **Создать группу доступа** и задать ее характеристики можно по нажатию на кнопку **Создать**.

Окно создания группы (рисунок 30) состоит из следующих вкладок:

- основная информация – уникальные идентификаторы группы (имена), а также комментарий;
- права доступа – настройка прав доступа для пользователей из данной группы;

– группы – списки групп, в которые включается текущая группа;
– доступ по реквизиту – настройка реквизитов доступа.

Для создания группы необходимо заполнить информацию о ней и нажать на кнопку «Создать».

Примечание. Более подробное описание свойств группы доступа приведено в п. 7.2.8.

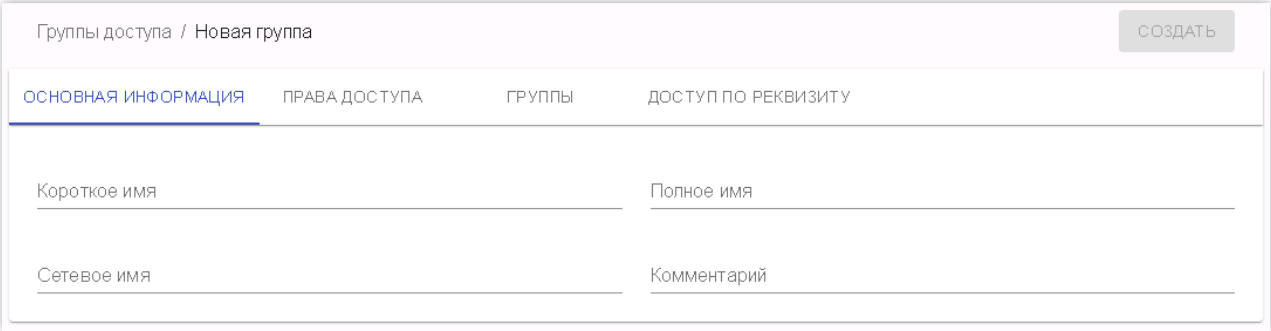


Рисунок 30

- **Загрузить группу доступа**, предварительно созданную или отредактированную в текстовом редакторе типа «Блокнот». Для этого следует нажать на кнопку **Загрузить** и в открывшемся модальном окне выбрать предварительно созданный файл в формате *.grp (рисунок 31).

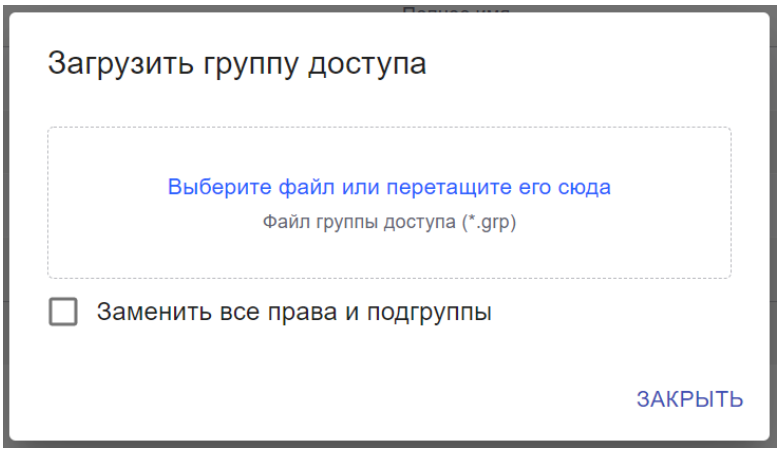


Рисунок 31

Флаг «Заменить все права и подгруппы»

По умолчанию флаг снят. Если установить его, то все ранее назначенные пользователю права, а также все группы, в которые он был помещен, заменятся на вновь загруженные.

Данные, содержащиеся в столбцах таблицы окна Группы доступа, можно отфильтровать по заданному параметру. Для этого в поле Фильтр необходимо ввести любое количество значимых или служебных символов.

7.2.8. Свойства группы доступа

Для просмотра и редактирования характеристик группы доступа необходимо левой кнопкой мыши щёлкнуть на выбранную группу. Перемещаясь по вкладкам в открывшемся окне можно изменять, добавлять и удалять свойства группы доступа.

Чтобы отредактировать свойства, рекомендуется следующая последовательность действий:

1. Нажать кнопку **Скачать**;
2. Указать произвольную директорию, в которую будут сохранен файл с описанием свойств группы;
3. Открыть файл в текстовом редакторе типа «Блокнот» и внести необходимые изменения;
4. Загрузить обновленный файл в окне Группы доступа, нажав на кнопку **Загрузить группу доступа** (подробнее см. раздел Создание группы доступа).

- **Вкладка Основная информация**

Основная информация о группе представлена в виде следующих редактируемых полей (рисунок 32):

– краткое имя;
– полное имя;
– сетевое имя;
– комментарий.

Поля Короткое имя и Полное имя являются уникальными идентификаторами на уровне всех субъектов доступа системы (пользователей и групп пользователей). Задаются при создании группы. Доступны для редактирования (рисунок 32).

Поле Сетевое имя – соответствует названию группы доступа в службе каталогов.

Следует иметь в виду, что идентификатор группы:

– не может быть пустым;
– не может начинаться с цифры;
– не должен содержать служебных символов: ",<>.~`@№^:;&*()+-][{}!?'|\/.

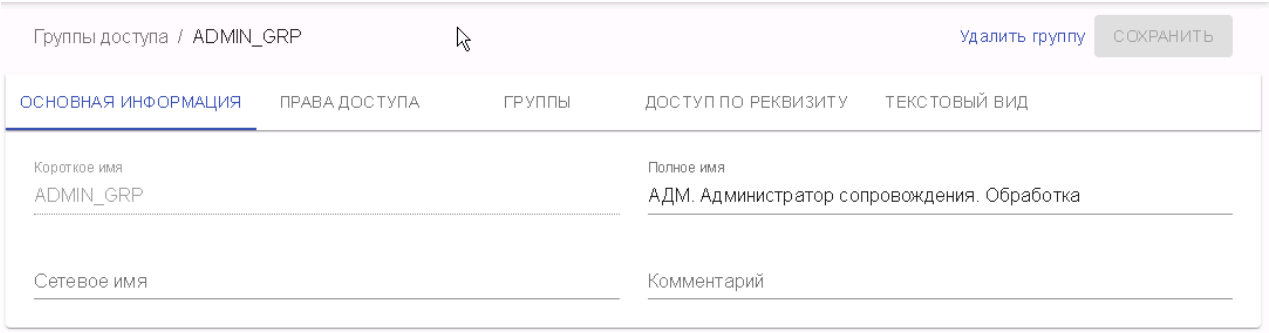


Рисунок 32

- **Вкладка Права доступа**

Данные о доступных для пользователя действиях отображаются в виде таблице со столбцами (рисунок 33):

1) Категория объекта доступа – представлены в виде значков с соответствующими идентификаторами (буквами):
   - тип базового понятия (T);
   - представление (V);
   - операция (M);
   - переход (W).

2) Короткое имя – уникальный идентификатор на уровне всех субъектов доступа системы (пользователей и групп пользователей).

3) Полное имя – уникальный идентификатор на уровне всех субъектов доступа системы (пользователей и групп пользователей).

Для добавления прав доступа необходимо нажать на «+» и выбрать соответствующие объекты доступа из открывшего списка.

Поиск добавленных объектов доступа осуществляется вручную или с использованием поля поиска.

Для удаления объекта доступа необходимо выбрать его из списка и нажать на корзину.

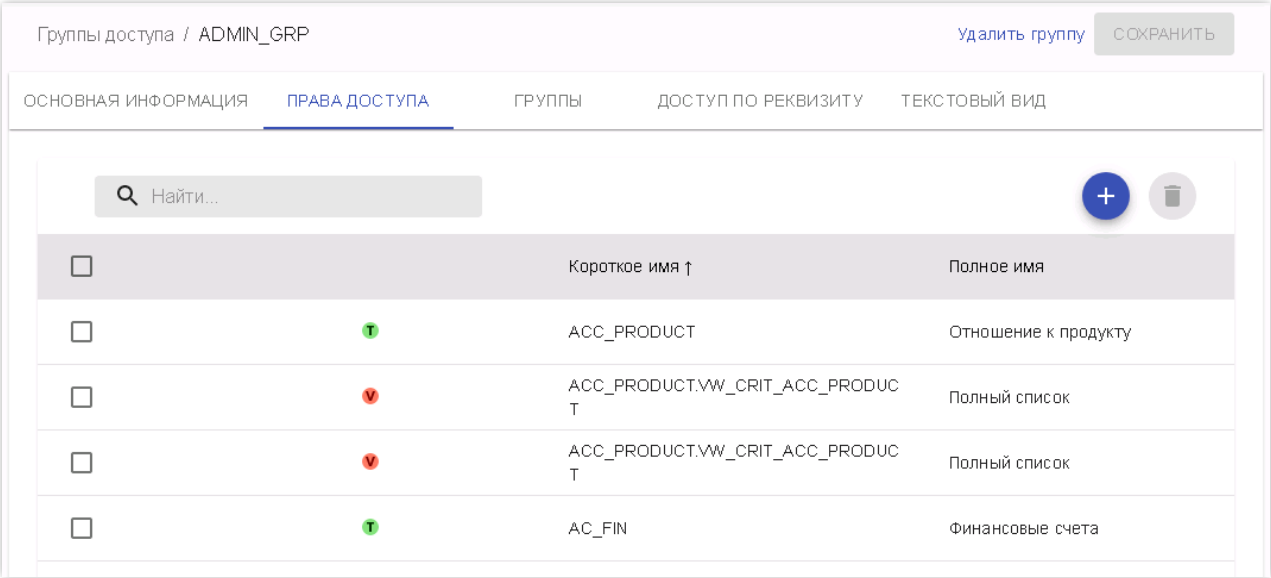


Рисунок 33

По нажатию на кнопку **«+»** администратор может назначить пользователю или группе пользователей право доступа до определенного объекта доступа. Подробнее см. раздел Назначение прав доступа группе пользователей.

- **Вкладка Группы**

В виде двух панелей отображаются списки групп, в которые включается текущая группа. Переопределение списков выполняется посредством перемещения элементов между панелями. В списках субъектов данной вкладки не отображается пользователь-владелец схемы, так как изменить принадлежность группе для данного пользователя невозможно (рисунок 34).

+ - возможность поиска группы доступа и добавление/удаление

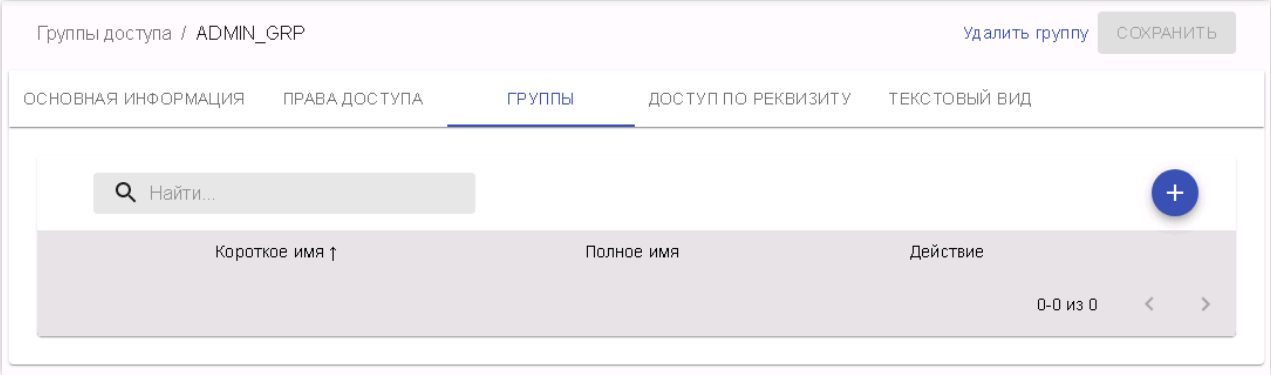


Рисунок 34

Во вкладке доступна функция поиска уже созданных групп. Для этого в поле Поиск необходимо ввести любое количество значимых или служебных символов.

- **Вкладка Доступ по реквизиту**

На вкладке «Доступ по реквизиту» настраивается доступ по реквизиту для группы доступа (рисунок 35).

Вкладка состоит из трех частей:

1) ТБП, в котором проверяется доступ;
2) ТБП, на который ссылается реквизит;
3) Экземпляры.

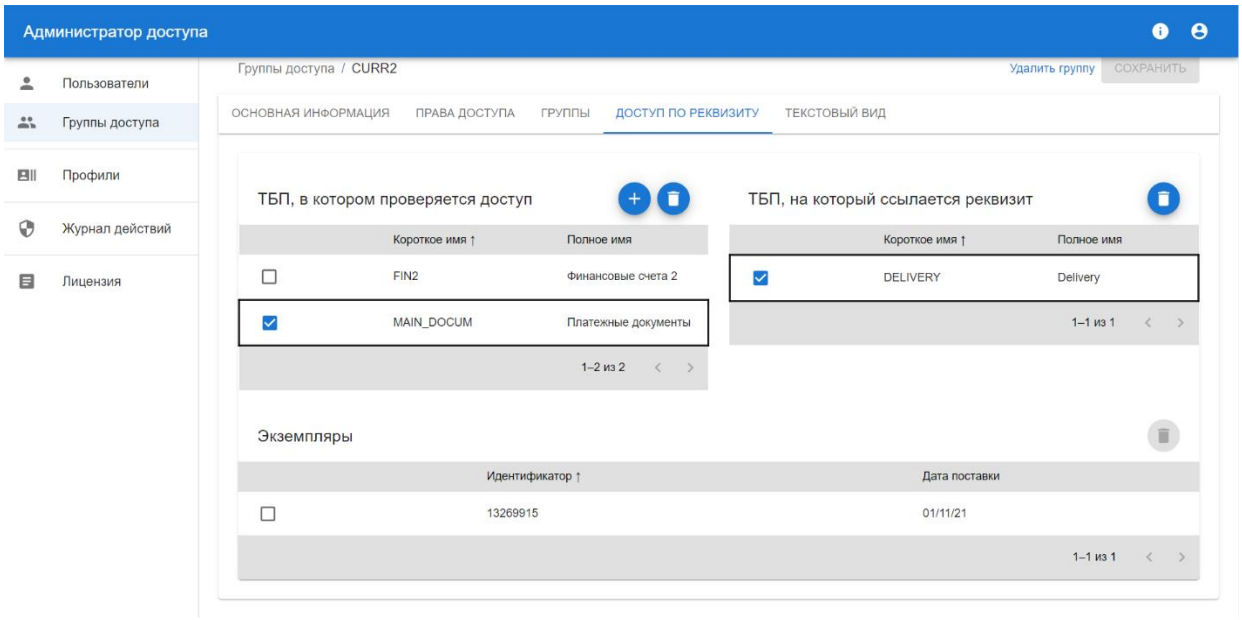


Рисунок 35

В части «ТБП, в котором проверяется доступ» указывается ТБП в котором необходимо контролировать доступ к реквизиту.

Для просмотра данных ТБП необходимо выбрать его из списка. Данные в полях 2 и 3 заполнятся автоматически.

Для удаления ТБП необходимо выбрать его из списка и нажать на значок «Корзина».

Добавление нового правила доступа по реквизиту для группы доступа осуществляется через значок «+» в части «ТБП, в котором проверяется доступ». Открывается интерфейс добавления нового правила доступа состоящий из 3-х шагов:

1 шаг – выбираем ТБП, в котором проверяется доступ (рисунок 36).

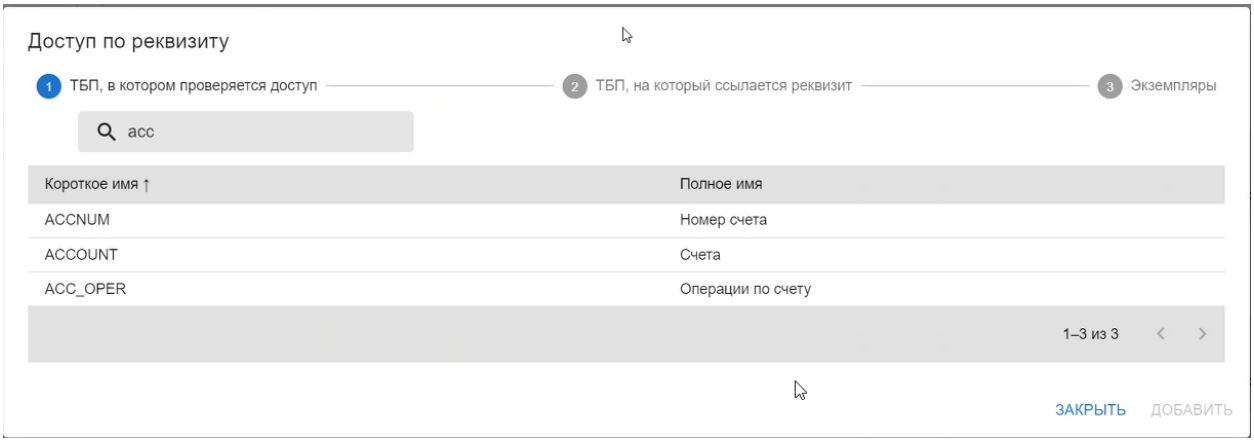


Рисунок 36

2 шаг – выбираем ТБП, на который ссылает ТБП (рисунок 37)

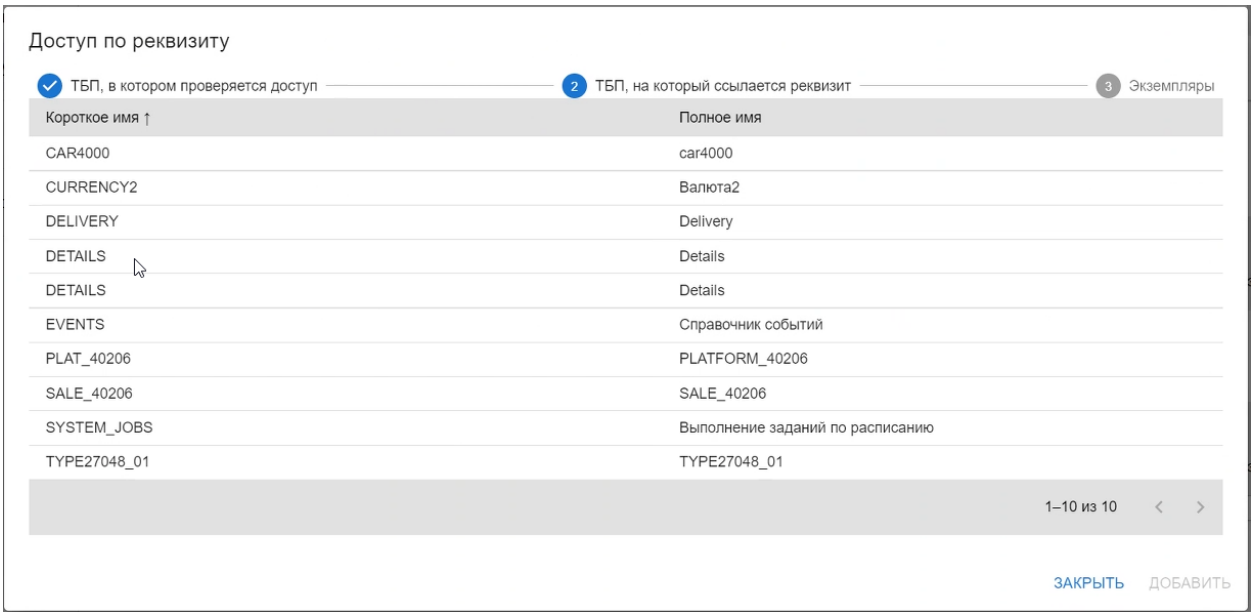


Рисунок 37

3 шаг – выбираем конкретные экземпляры реквизитов, к которым предоставляется доступ (рисунок 38).

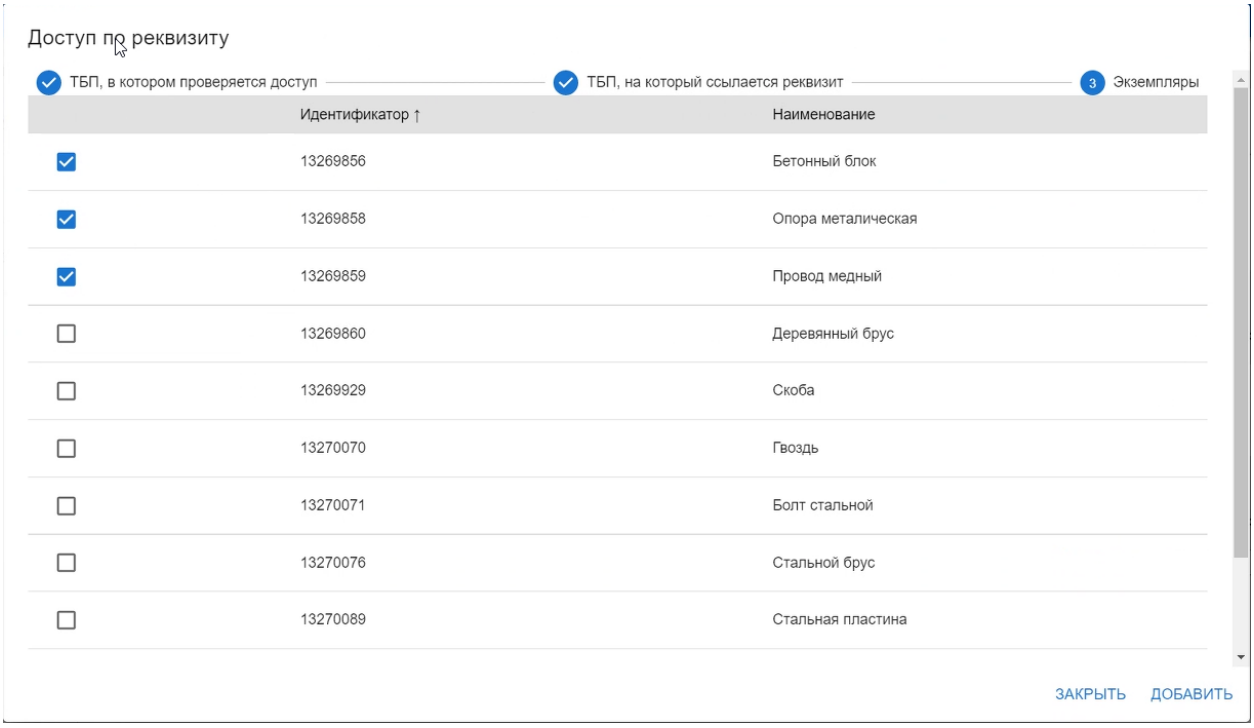


Рисунок 38

- **Вкладка Текстовый вид**

Свойства группы представлены в виде текста (рисунок 39).

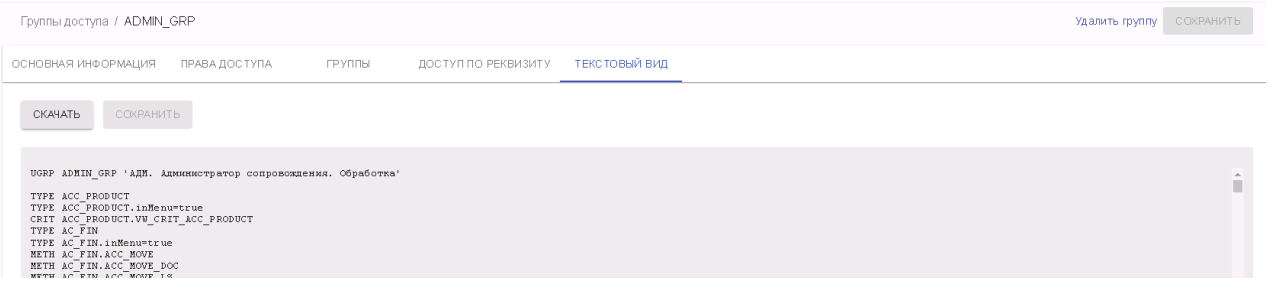


Рисунок 39

7.2.9. Удаление группы доступа

Удалить группу доступа можно по нажатию на ссылку Удалить группу, доступную в любой из вкладок окна Группы доступа (рисунок 40). Действие необратимо, поэтому следует быть внимательным при его подтверждении.

Рисунок 40

7.2.10. Профили пользователей

По нажатию на пункт меню Профили происходит вызов окна Профили пользователей (рисунок 41). Окно содержит список возможных профилей для пользователей и набор свойств для каждого профиля.

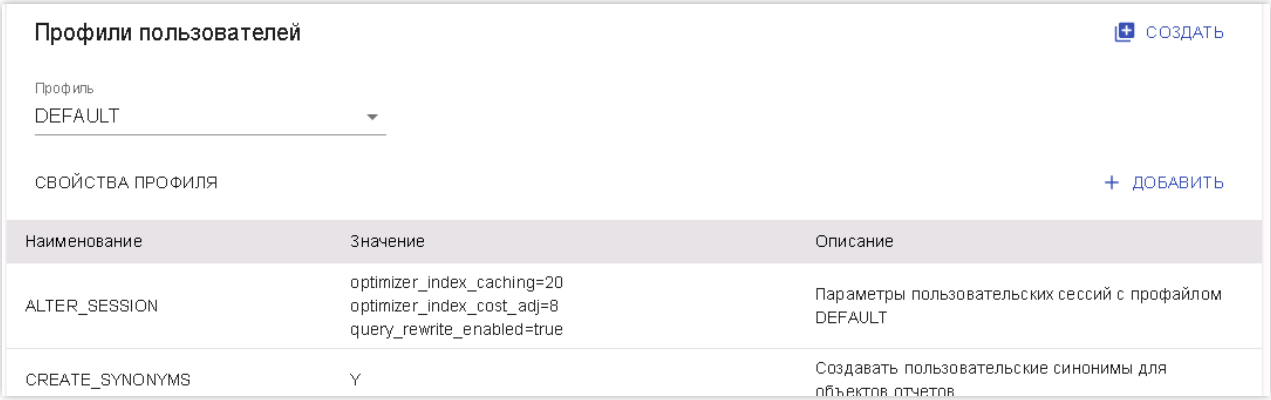


Рисунок 41

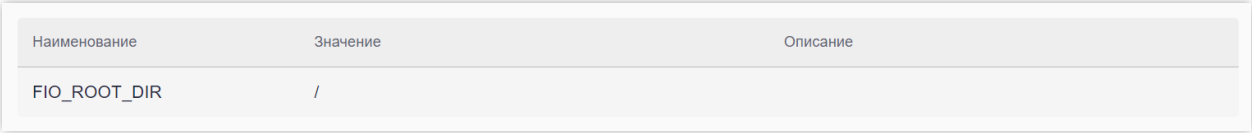
Профиль

Выпадающий список содержит все существующие на схеме профили (рисунок 42). Свойства выбранного в списке профиля отображаются в приведенной ниже таблице.

Рисунок 42

Таблица свойств профиля

Свойства текущего профиля представлены таблицей со столбцами Наименование, Значение и Описание (рисунок 43). Подробнее о возможных свойствах профиля см. раздел Свойства пользовательских профилей.



Наименование	Значение	Описание
FIO_ROOT_DIR	/	

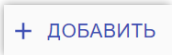
Рисунок 43

Кнопка Создать

По кнопке

запускается процесс создания нового профиля. Для этого требуется ввести его наименование. При создании нового профиля создается только одно свойство – Корневой каталог FIO (FIO_ROOT_DIR).

Кнопка Добавить

По кнопке 

открывается окно для задания свойств профиля (рисунок 44). Следует заполнить поля Наименование, Значение, Описание. Подробнее о возможных свойствах профиля см. раздел Свойства пользовательских профилей.

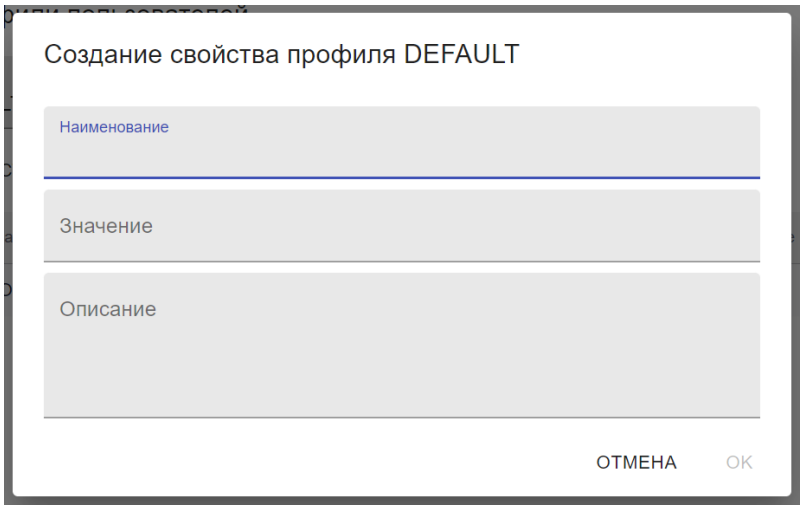


Рисунок 44

7.2.11. Свойства пользовательских профилей

При заполнении полей свойств пользовательских профилей значения могут принимать в том числе значения, указанные в таблице 3.

Таблица 3

Наименование свойства	Возможные значения	Описание
ACCOUNT_LOCK_TIME	Число (количество дней)	Блокировка учетной записи пользователя при отсутствии соединений с БД в течение периода, превышающего заданный. Свойство имеет смысл, только при корректной отработке операции "Блокировка пользователей по настройке в профилях [LOCK_USERS]". Подробнее см. Блокирование пользователя .
ADMIN_READ_ONLY	YES/NO	Режим модификации модели в сессии : YES – запрет на модификацию модели пользователем, NO – модификация модели пользователем разрешается. Значение параметра не учитывается, если на схеме выставлено значение системного параметра ADMIN_READ_ONLY = YES.
ALTER_SESSION	ALTER_SESSION	Флаг определяет доступность пользователю функции «Просмотр журнала состояний» в АРМ «ЦФТ – Навигатор»: YES - функция доступна; NO - функция недоступна.
AUD.NAV.VW.VALUES	YES/NO	Флаг необходимости журналирования открытия представлений для конкретного пользователя: YES – все открытые пользователем представления всегда журналируются; NO – значение по умолчанию

AUD.PARAM_OPER	YES/NO	Флаг необходимости журналирования значений параметров при выполнении операций для конкретного пользователя: YES – значения параметров всех выполненных пользователем операций всегда журналируются; NO – значение по умолчанию
AUD.VIEW_COPY_ROWS	YES/NO	Флаг необходимости журналирования факта копирования строк из представления для конкретного пользователя: YES – факт копирования строк из представления журналируется; NO – значение по умолчанию, копирование строк из представлений не журналируется
CREATE_SYNONYMS	YES/NO	Режим инициализации сессий пользователей для отчётов: YES – синонимы создаются по существующим зависимостям отчётов; NO – синонимы не создаются.
FIO_BASE_DIR	Перечисление сетевых путей доступных каталогов через ";"	Доступные каталоги FIO.
FIO_DEBUG_LEVEL	0 – нет журналирования; 1 – регистрация сессий, ошибки выполнения функций; 2 – переименование, удаление файлов, создание каталогов, выполнение shell-команд; 3 – чтение каталогов, открытие, закрытие файлов; 4 – чтение, запись файлов, установка позиции в файле.	Уровень журналирования FIO.
FIO_EXE_DIR	Сетевой путь к каталогу	Путь к утилитам на сервере.
FIO_HOME_DIR	Сетевой путь к каталогу	Префикс имен каталогов настроек FIO (FIO_ROOT_DIR, FIO_BASE_DIR), т.е. указанный префикс автоматически добавляется ко всем именам каталогов, перечисляемым в настройках FIO_BASE_DIR и FIO_ROOT_DIR.
FIO_LHA_CMD	Соответствующая команда FIO	Команда FIO для получения архива (формат LHA).
FIO_LOG_FILE	Сетевой путь к log-файлу	Журнал файловых операций (FIO), в который записывается информация, соответствующая установленному уровню отладки.

FIO_MAKE_DIR	YES/NO	Флаг доступа к функциям создания/ удаления каталогов (YES – доступ есть, NO – нет)
FIO_MKDIR_CMD	Соответствующая команда FIO	Команда FIO для создания директории по заданному пути
FIO_REPLACE_DIR	Сетевой путь	Префикс имен каталогов, заменяемый на FIO_HOME_DIR при вызове функций FIO, т.е. указанный префикс автоматически замещается на FIO_HOME_DIR во всех функциях FIO, где используются параметры - имена каталогов или файлов
FIO_RMDIR_CMD	Соответствующая команда FIO	Удаление директории
FIO_ROOT_DIR	Название каталога	Корневой каталог FIO (текущая директория). Доступ к файлам разрешается от указанного каталога, включая все подкаталоги
FIO_TEMP_DIR	Название каталога	Относительный или абсолютный путь к каталогу временных файлов на сервере. В случае, когда указан относительный путь, помимо существования каталога с таким названием в корне директории, необходимо, чтобы этот каталог был перечислен в настройке FIO_BASE_DIR
FIO_ZIP_CMD	Соответствующая команда FIO	Команда FIO для получения архива (формат ZIP)
IDE_ADMIN_READ_ONLY	YES/NO	Режим модификации модели в сессии : YES – запрет на модификацию модели пользователем, NO – модификация модели пользователем разрешается
IDLE_TIME	Число (время в минутах)	Лимит бездействия АРМа "ЦФТ – Навигатор" и АРМа "Администратор доступа". По истечении этого периода произойдёт автоматическое отключение.
NAV.FORM.TAB.MULTILINE	YES/NO	Включает в АРМе "ЦФТ – Навигатор" режим каскадного расположения закладок на экранной форме операции (YES – закладки на ЭФО располагаются каскадом, NO – стандартное расположение закладок в одну строку, значение по умолчанию)
NAV.VW.REFCING	YES/NO	Флаг определяет доступность функции «Поиск ссылок на экземпляр» в АРМ «ЦФТ – Навигатор»: YES - функция доступна; NO - функция недоступна

NLS_DATE_FORMAT	Формат даты, например, 'DD/ MM/YY'	Настройка формата даты в клиентской сессии.
NLS_LANGUAGE	Название языка, например, ‘RUSSIAN’	Настройка языка в клиентской сессии.
NLS_NUMERIC_CHA RACTE RS	Разделители, например: '.,'	Настройка разделителей в клиентской сессии
NLS_SETTINGS	NLS-параметры и их значения. Например: NLS_LANGUAGE=RUSSIA N NLS_SORT=BINARY NLS_NUMERIC_CHARAC TER S='.,' NLS_TERRITORY=CIS NLS_DATE_FORMAT='DD / MM/YY'	Возможность задать NLS-параметры одной строкой.
NOVO.3L. FORBID_PASSWORD _CHA NGE	YES/NO	Свойство определяет возможность изменения пароля через АРМ "ЦФТ – Навигатор" в режиме соединения по 3L (YES – установлен запрет на изменение пароля, NO – значение по умолчанию, отключен запрет на изменение пароля).
NOVO.START_METH OD	Операция для запуска в формате	При соединении со схемой через АРМ "ЦФТ – Навигатор" автоматически запускается операция, указанная в параметре.
NOVO.REPORT_SCH EDULE	YES/NO	Флаг доступа к запуску отчётов по расписанию (YES – доступ есть, NO – доступа нет). Свойство влияет на допуск к опции только в АРМе "ЦФТ – Навигатор".
NOVO. FORBID_VIEW_COP Y_ROW S	YES/NO/OBJECTS_ONLY	Свойство доступности копирования строк из представлений: YES – установлен запрет на копирование строк; NO – значение по умолчанию, отключен запрет на копирование строк; OBJECTS_ONLY - запрещает копирование строк только в режиме просмотра списка экземпляров; Свойство влияет на допуск к опции только в АРМе "ЦФТ – Навигатор".
PLP_READ_ONLY_O N_STA RT	YES/NO	Режим модификации данных в сессии : YES – запрет на модификацию данных пользователем, NO – модификация данных пользователем разрешается. Значение параметра можно изменить для текущей сессии в АРМе "ЦФТ – Навигатор" с помощью операции " Установить режим модификации данных в сессии" в ТБП "Системные журналы". Значение параметра не учитывается, если на схеме выставлено

		значение системного параметра PLP_READ_ONLY = YES.
SESSIONS_PER_USER	Число (количество); 'пусто'; 'UNLIMITED'	Настройка допустимого количества сессий. Подробности см. далее, после таблицы.
SESSIONS_PER_USER_MODE	USE_ORACLE (по умолчанию) / USE_PROFILE	Определяет режим настройки допустимого количества сессий.
SHOW_LEGAL_NOTICE	YES/NO	Показ уведомления об ответственности при входе в АРМ "ЦФТ – Навигатор"
USER_CONTEXT	Название функции	Функция инициализации пользовательского контекста (должна возвращать строку).
USER_LOCK_OPEN	Название функции	Функция инициализации пользовательского сеанса (должна возвращать строку)

7.3. Назначение субъектам прав доступа

При открытии пользователем в АРМ «ЦФТ–Навигатор» некоторого представления, список экземпляров в этом представлении будет формироваться в соответствии с правами пользователя на доступ к этим экземплярам.

В АРМ «Администратор доступа» доступ к экземпляру для конкретного субъекта доступа может быть назначен различным образом. Причем субъектом доступа является как отдельный пользователь, так и группа пользователей.

7.3.2. Назначение прав доступа пользователю

Чтобы назначить пользователю права доступа, его следует включить в группу, участникам которой открыт доступ к тем или иным субъектам доступа и действиям (рисунок 45).

Для добавления пользователя в группу необходимо нажать на кнопку «+» и выбрать пользователя из открывшегося списка.

Поиск пользователей группы производится вручную или с использованием поля поиска.

Для удаления пользователя из группы необходимо выбрать его из таблицы и нажать на корзину.

Примечание. Кнопка корзины становится доступна после выбора пользователя в таблице.

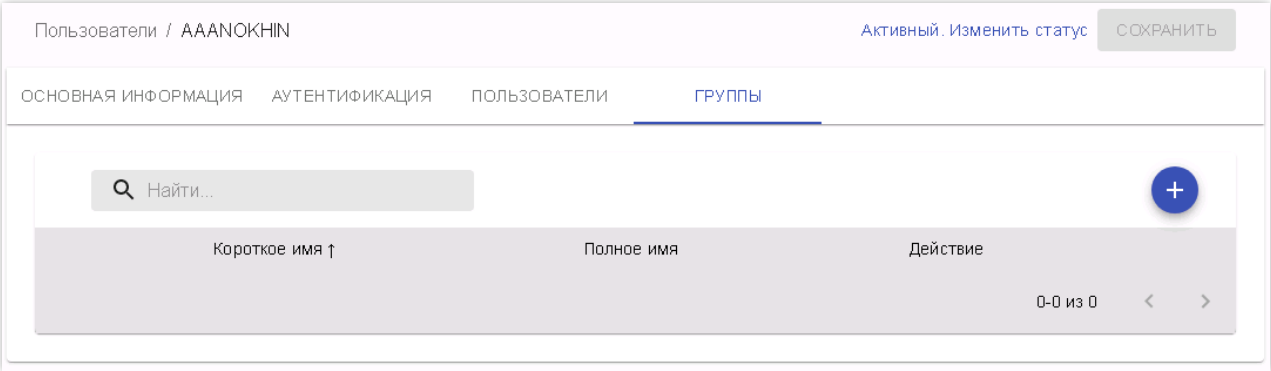


Рисунок 45

7.3.3. Назначение прав доступа группе доступа

На данной вкладке отображаются объекты, доступ к которым есть у данной группы (рисунок 46).

Поиск объектов возможен вручную или с использование поля поиска.

Для удаления объекта доступа необходимо выбрать его и нажать на кнопку корзины.

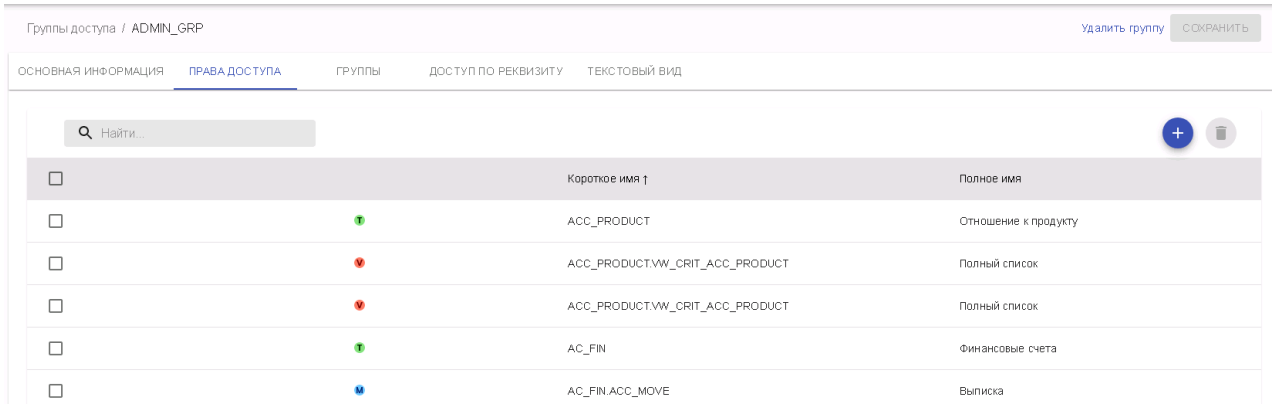


Рисунок 46

Чтобы назначить группе пользователей право доступа к какому-либо объекту доступа следует:

1. Нажать на кнопку «+».
2. В открывшемся окне (рисунок 47) выбрать из таблицы или найти при помощи поля Поиск необходимый объект доступа и подтвердить свой выбор нажатием на кнопку «добавить».

Рисунок 47

3. Чтобы выйти из окна без сохранения данных, следует нажать на кнопку **Закрыть**.

7.3.4. Передача прав пользователей

Назначение прав пользователю в АРМ «Администратор доступа» возможно также посредством передачи прав от одного пользователя другому (но не группе пользователей). При передаче прав передаются все права, включая наследование прав групп пользователей и переданные права других пользователей.

На данной вкладке отображается писок пользователей, которым были переданы права (рисунок 48).

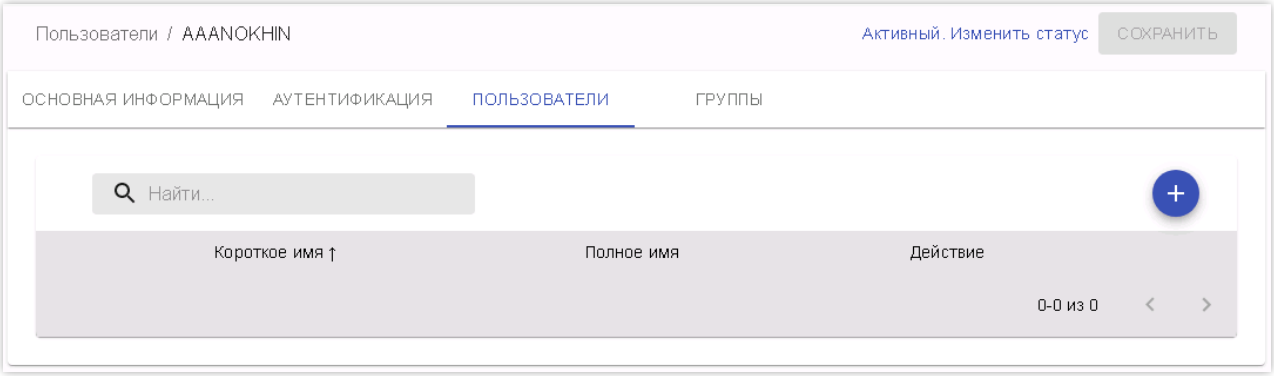


Рисунок 48

Поиск пользователей возможен вручную или с использованием поля поиска.

Для удаления пользователя необходимо выбрать его из списка и нажать на кнопку корзины.

Примечание. Кнопка корзины становится доступна после выбора пользователя из таблицы.

Для передачи прав следует:

1. Нажать на кнопку «+» (см. рисунок 48).
2. В открывшемся окне выбрать пользователя и нажать на кнопку «Добавить» (рисунок 49).

Рисунок 49

3. Пользователь будет добавлен на вкладку «Пользователи». Для сохранения изменений необходимо нажать на кнопку «Сохранить» (рисунок 50).

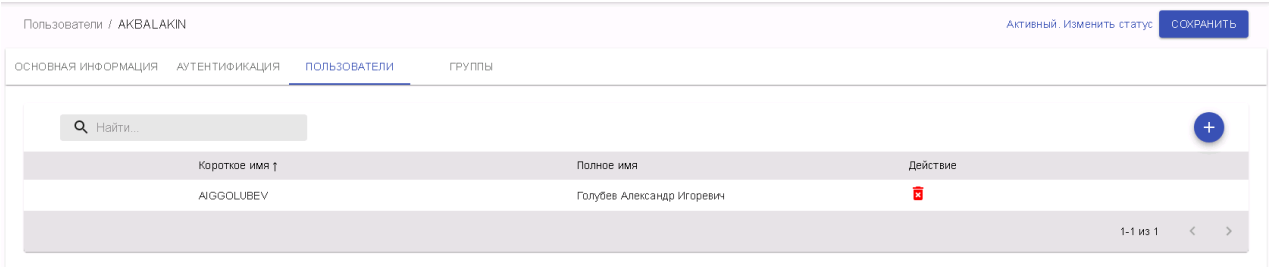


Рисунок 50

7.3.5. Отзыв ролей

В АРМ «Администратор доступа» можно отозвать у пользователя переданные ему ранее права другого пользователя. Для этого следует:

Для отзыва прав у пользователя необходимо выбрать его из таблицы и нажать на корзину (рисунок 51).

Поиск пользователя производится вручную или с использованием поля поиска.

Примечание. Кнопка корзины становится доступна после выбора пользователя из таблицы.

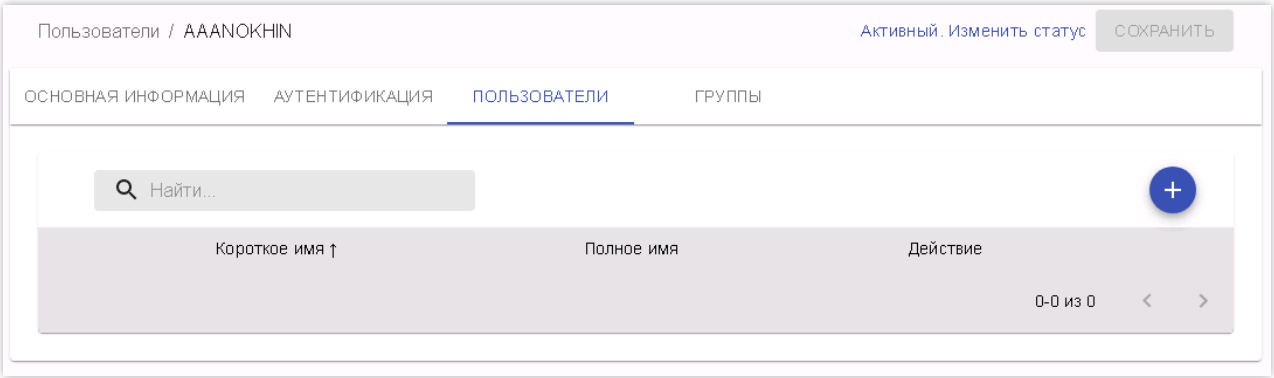


Рисунок 51

Вторым способом отзыва ролей у пользователя является смена его статуса с Активный на Заблокированный (подробнее см. раздел Блокирование и разблокирование пользователя).

8. ПОРЯДОК РАБОТЫ С ПРИКЛАДНЫМ ФУНКЦИОНАЛОМ СИСТЕМЫ

8.2. Процедуры обновления прикладного функционала

Обновления прикладного функционала Системы могут быть разработаны сотрудниками подразделений организации или получены от организации-разработчика. В комплект поставки обновления прикладного функционала Системы входит самораспаковывающийся веб-архив, имеющий расширение .war.

В общем виде алгоритм установки обновления прикладного функционала заключается в выпуске обновленного war-файла, который необходимо разместить в тот же каталог, где установлен уже существующий war-файл, требующий замены.

Для этого администратору необходимо соблюдать последовательность действий:

1. Выполнить остановку приложения на СП;
2. Заменить существующий war-файл в каталоге обновленным war-файлом;
3. Запустить приложение;
4. Проверить его работоспособность.

Подробнее об этом см. раздел Настройка сервера Tomcat.

9. ДЕЙСТВИЯ В СЛУЧАЕ СБОЯ

Наличие ошибок (errors) и предупреждений (warnings) в лог-файлах ещё не означает наличие критичных проблем. Например, в лог-файлы могут выводиться ошибки о неудачных запусках каких-то подсистем, которые не требуются в данном контексте.

9.2. Проверка корректности функционирования Сервера приложений

Для проверки работоспособности СП следует воспользоваться диагностической страницей /diag (подробнее см. раздел Проверка корректности установки Сервера приложений).

9.3. Включить дополнительное логирование в Сервера приложений

Для получения дополнительной отладочной информации при возможном возникновении тех или иных проблем в работе СП может помочь включение механизма расширенного логирования. Подробнее о функции логирования данных СП см. раздел log4j.properties.

9.4. Включение логирования работы АРМов

В некоторых случаях при подозрении, что АРМ работает некорректно, пользователю бывает необходимо провести логирование работы АРМа, чтобы служба поддержки могла быстрее и точнее установить причину некорректного поведения АРМа и предложить способ решения проблемы.

Примечание

Поскольку процесс логирования может замедлить работу АРМов, рекомендуется включать логирование только на время диагностики конкретной ситуации.

Включение логирования работы АРМ «ЦФТ-Навигатор» осуществляется в реестре.

Рекомендуемая последовательность действий:

1. Закрыть АРМ.
2. Включить логирование (описание см. ниже). Уровень отладки по возможности согласовать со службой поддержки или установить максимальную детализацию.
3. Запустить АРМ.

4. Выполнить действия, необходимые для воспроизведения ситуации. По возможности не выполнять посторонних действий, так как это может увеличить размер лога и может усложнить поиск причины возникающей неполадки.
5. Закрыть АРМ.
6. Выключить логирование.
7. Выслать описание возникшей ситуации и полученный лог-файл в службу сопровождения.

Для того чтобы включить логирование работы АРМа в реестре, необходимо:

1. В ключе реестра HKEY_CURRENT_USER\Software\FTC\IBS\<НазваниеАРМа> создать параметр типа DWORD LogLevel. Задать ему десятичное значение от 1 до 2047, в зависимости от требуемого уровня логирования. Уровень 100 или 511 включает все, кроме логирования компонента безопасности и стека вызовов. 2047 – максимально детальный уровень лога.
2. При необходимости явным образом задать имя лог-файла, в ключе реестра HKEY_CURRENT_USER\Software\FTC\IBS\<НазваниеАРМа> следует добавить строковый параметр LogFile. Задать ему значение – полный путь и имя лог-файла.

Log-файл может быть создан только в текстовом формате, но с любым расширением.

После этого при запуске АРМа пользователю будет выдаваться сообщение о включенном логировании и имени лог-файла.

В случае если указанный в реестре лог-файл (параметр LogFile) невозможно открыть на запись по какой-либо причине или параметр LogFile отсутствует, будут произведены попытки записи лога в другие файлы (в каталог запуска АРМа, в корневой каталог C:\). О таких ситуациях пользователю также будет выдано соответствующее сообщение.

Для удобства включения логирования может быть создан reg-файл (*.reg).

Пример файла для включения логирования

```
REGEDIT4

[HKEY_CURRENT_USER\Software\FTC\IBS\<ARM>]

"LogLevel"=dword:0000005b

"LogFile"="C:\<ARM>.log"
```

Для того чтобы отключить логирование, достаточно установить параметру LogLevel значение «0» (ноль), либо удалить этот параметр из реестра.

Пример файла для отключения логирования в АРМ «Навигатор»

```
REGEDIT4
[HKEY_CURRENT_USER\Software\FTC\IBS\Navigator]
"LogLevel"=dword:0
"LogFile"=""
```

Соответствие модулей и ключей реестра

«Навигатор»	Navigator	Уровень лога 1 – 100

9.5. Получение дампа памяти в АРМ «ЦФТ-Навигатор»

В некоторых случаях для выяснения причин нештатного завершения работы АРМа «Навигатор» может потребоваться анализ дампа оперативной памяти PC пользователя на момент возникновения ошибки.

Если во время работы модуля происходит критическая ошибка, то с помощью утилиты DwPltfm дамп памяти сохраняется в архив вместе с описанием окружения и логом, который создается АРМом при включенном в реестре логировании (см. раздел Включение логирования работы АРМов).

Примечание

*Архив **dwpltfm.zip** доступен для скачивания на сайте поддержки support.cft.ru*

Для сбора отладочной информации нужно выполнить следующие действия:

1. В каталог с исполняемым файлом АРМа «Навигатор» скопировать из архива dwpltfm.zip программу dwpltfm.exe и ее конфигурационный файл dwpltfm.ini.

Примечание

Программа DwPltfm поддерживает работу в ОС Windows 7/Vista/Server2008R2/XP.

2. В конфигурационном файле dwpltfm.ini указать значения следующих параметров:

- DumpPath – каталог для сохранения отладочной информации. Этот каталог должен быть доступен пользователям для записи. Всем пользователям можно назначить один каталог, так как имя файла с отладочной информацией уникально – оно включает время, имя пользователя и имя программы. Если значение параметра не указано, лог будет сохранен в корневой каталог диска C:\.

- DumpType – объём дампа памяти. Сбору наиболее полной информации соответствует значение WithFullMemory. Однако дамп в этом случае занимает ~60 Мб (в архиве ~16 Мб). Если такие объемы передавать затруднительно, следует установить значение Normal.
- DeleteOwnLog – настройка удаления собственного лога программы DwPltfm. Программа всегда создаёт лог C:\dwpltfm.log, либо C:\dwpltfmN.log (где N – число), если файл C:\dwpltfm.log не доступен для записи. Файл удаляется по завершении работы программы при установке параметру значения Y и в случае отсутствия ошибок. При установке значения N лог не удаляется.

3. Запустить АРМ «Навигатор». Теперь при возникновении критической ошибки, приводящей к аварийному завершению работы модуля, программа dwpltfm.exe отработает в соответствии со своими настройками.
4. Полученный в результате работы программы DwPltfm архив необходимо отправить на адрес электронной почты службы сопровождения.

Для проверки настроек можно использовать также программу dwtest.exe. Программу необходимо скопировать из архива dwpltfm.zip в каталог с программой dwpltfm.exe и запустить. Возникнет критическая ошибка, и программа DwPltfm предложит ввести описание ситуации. В комментарии необходимо кратко описать условия возникновения ошибки.

Пример конфигурационного файла dwpltfm.ini

[DwPltfm]

DeleteOwnLog = N

DumpType = WithFullMemory

DumpPath = \\astral\dumps

10. СООБЩЕНИЯ АДМИНИСТРАТОРУ

В процессе работы Системы администратору могут выводиться системные сообщения в виде модального диалогового окна (уведомления или всплывающего оповещения) на экране РС пользователя.

Сообщения могут быть трех видов:

1. Информационные;
2. Предупреждающие;
3. Блокирующие.

Информационные сообщения

В каких случаях возникают:

Если нужно оповестить о каком-либо событии, этапе процесса, показать расчетные значения, полученные в ходе исполнения алгоритма.

Что необходимо предпринять:

Внимательно ознакомиться с текстом сообщения и продолжить работу с учетом полученных данных.

Предупреждающие сообщения

В каких случаях возникают:

При возможности возникновения (или уже случившейся) несущественной ошибки в процессе эксплуатации Системы.

Что необходимо предпринять:

Рекомендуется предпринять действия, описанные в сообщении (например, скорректировать выбор функции, изменить введенные данные) для устранения проблемы.

Блокирующие сообщения

В каких случаях возникают:

При возникновении ошибки в процессе выполнения прикладных операций в АРМах.

Что необходимо предпринять:

Блокирующие сообщения останавливают выполнение заданной операции. Необходимо ознакомиться с текстом ошибки, при возможности устранить причины ошибки, либо перенаправить содержание текста ошибки в подразделение, осуществляющее поддержку Системы.

11. УСТРАНЕНИЕ ТИПИЧНЫХ ОШИБОК

В случае возникновения нештатных ситуаций в процессе эксплуатации Системы (зависаний ПО, сообщений об ошибке и других проблем, требующих помощи технического специалиста) рекомендуется проанализировать ситуацию и по возможности произвести действия, указанные в разделе «Действия в случае сбоя».

Если проблема не решена, рекомендуется обратиться в подразделение сопровождения Системы.