ЦФТ ЦЕНТР ФИНАНСОВЫХ ТЕХНОЛОГИЙ

Администратора доступа 2.0

Руководство пользователя

Версия 1.0.16

Оглавление

1. Системные требования

- Java Development Kit (JDK) версии 11.0.16 и выше.

Тестирование проводилось и проводится на актуальных на текущий момент браузерах:

- Google Chrome 108 и выше
- Opera 94 и выше
- Microsoft Edge 108 и выше
- Яндекс Браузер 22.9.1 и выше

Работоспособность в браузерах более старых версий не проводится и не гарантируется.

Для корректной работы необходимо следующее разрешение рабочей области экрана:

- Минимальное разрешение: 1280×720 px
- Рекомендованное разрешение: 1920×1080 px

2. Предварительная настройка

В Администраторе доступа 2.0 изменились некоторые подходы к использованию данных подсистемы доступа. Изменения продиктовано совместимостью с DBI и устранению исторически возникших проблем.

По этой причине перед установкой и настройкой UA2 необходимо проведение корректировки данных подсистемы доступа, если она не была произведена в ТЯ или до миграции с режима ТЯ на DBI.

Для этого подготовлен ряд скриптов для устранения проблемных мест в прикладных данных подсистемы доступа.

- ТЯ - https://nexus.cft.ru/dbi/uadmin/migrate/ua2-migrate-scripts-core-oracle.zip
- DBI - https://nexus.cft.ru/dbi/uadmin/migrate/ua2-migrate-scripts-dbi-pg.zip

При этом для PostgreSQL есть скрипты как для запуска под Windows, так Linux-ориентированными операционными системами.

Для миграции данных подсистемы доступа присутствуют следующие скрипты:

- `convert_invalid_dbi_roles.bat|.sh` - удаляет неиспользуемые в DBI роли у пользователей. Фактически необходим только для работы в режиме DBI. Продиктовано тем, что такие роли как `Администратор`, `Администратор проектов`, `Администратор проектов (перенос прав доступа)`, неприменимы в контексте DBI.
- `convert_personal_rights.bat|.sh` - перемещает личные права пользователя в новую группу, в которую включает пользователя. Продиктовано тем, что в DBI все права пользователей наследуются от групп доступа и у пользователя отсутствуют личные права на какие бы то ни было объекты доступа.

Каждый из скриптов сначала выводит список некорректных объектов анализа и предлагает автоматически исправить зафиксированные проблемы. Если пользователь соглашается с автоматическим исправлением, то скрипты сами произведут все необходимые действия. В противном случае предлагается принять организационные и прочие усилия для устранения проблемных данных своими силами.

Вызов каждого скрипта производится владельцем БД командой

```
# oracle
convert_personal_rights.bat localhost 1521 ORCLPDB1 IBS ******

# pg
convert_personal_rights.bat localhost 5432 postgres postgres ******
```

Для запуска скриптов для ТЯ необходимо наличие установленного `Oracle Client`.

Для запуска скриптов для DBI необходимо наличие установленного `psql` - терминального клиента для работы с PostgreSQL.

3. Установка, настройка и запуск

Приложение позволяет работать в нескольких режимах:

- **DBI** - для работы с БД PostgreSQL. Поставляется в виде war и jar архивов.
- **CORE** - для работы с БД Oracle вместо старого exe АРМа Администратор доступа. Поставляется в виде jar архива.

Для загрузки актуальной версии war архива использовать команду

```
mvn org.apache.maven.plugins:maven-dependency-plugin:2.4:get
-DremoteRepositories=https://repo.cft.ru/ -Dartifact=ru.cft.platform:useradmin
-war:LATEST:war -Dtransitive=false -Ddest=uadmin.war
```

3.1. Запуск jar

Сохранить сконфигурированный файл `application.properties` рядом с jar архивом.

Запустить приложение из командной строки или терминала:

Windows

```
java -jar файл.jar
```

Linux

```
nohup java -jar -Duser.language=ru -Duser.country=RU файл.jar>./uadmin.log 2>&1 &s
```

3.1.1. Настройка application.properties для режима DBI

- Режим работы

```
orm.database=DBI
```

- URL для подключения к 2МСА DBI

```
orm.uri=http://СЕРВЕР:ПОРТ/КОНТЕКСТ_СЕРВЕРА_ПРИЛОЖЕНИЙ/rest
```

- Настройка соединения с БД Postgres:

```
orm.data.dialect=org.hibernate.dialect.PostgreSQLDialect
orm.data.driver=org.postgresql.Driver
orm.data.url=jdbc:postgresql://СЕРВЕР:ПОРТ/СХЕМА?ApplicationName=useradmin&currentSche
ma=uadm,aud,app,rtl,public
orm.data.username=uadmin_usr
orm.data.password=uadmin_usr
```

- Настройка соединения с БД Ignite:

```
orm.metamodel.dialect=org.hibernate.dialect.H2Dialect
orm.metamodel.driver=org.apache.ignite.IgniteJdbcThinDriver
orm.metamodel.url=jdbc:ignite:thin://СЕРВЕР:ПОРТ;schema=СХЕМА
orm.metamodel.username=
orm.metamodel.password=
```

- Выключить внешний пул соединений:

```
orm.cp.external=false
```

3.1.2. Настройка application.properties для режима ТЯ

- Режим работы

```
orm.database=CORE
```

- Выбрать и указать тип авторизации:

```
useradmin.security.authorization=[PASSWORD|OAUTH2|ANY]
```

- Путь до файла tnsnames.ora с настройками подключений к БД Oracle без указания наименования самого файла. Windows: Заменить в адресе `\` на `/`.

```
oracle.net.tns_admin=путь_до_TNS_файла
```

- Выключить внешний пул соединений:

```
orm.cp.external=false
```

3.2. Запуск war

Поддерживается работа только в режиме DBI

В `${catalina.base}/lib` нужно вручную добавить postgresql-x.x.x.jar (Подробнее про добавление библиотек см. документацию на официальном сайте https://tomcat.apache.org/).

В `JAVA_OPTS` указать каталог с расположением конфигурационного файла `-Dspring.config.additional-location=${catalina.base}/uadmin-settings/application.properties`.

В этот каталог поместить конфигурационный файл `application.properties`.

3.2.1. Настройка application.properties при работе без использования внешнего пула соединений

- Режим работы

```
orm.database=DBI
```

- URL для подключения к 2MCA DBI

```
orm.uri=http://СЕРВЕР:ПОРТ/КОНТЕКСТ_СЕРВЕРА_ПРИЛОЖЕНИЙ/rest
```

- Настройка соединения с БД PostgreSQL:

```
orm.data.dialect=org.hibernate.dialect.PostgreSQLDialect
orm.data.driver=org.postgresql.Driver
orm.data.url=jdbc:postgresql://СЕРВЕР:ПОРТ/СХЕМА?currentSchema=uadm,aud,app,rtl,public
orm.data.username=ИМЯ_ВЛАДЕЛЬЦА_СХЕМЫ
orm.data.password=ПАРОЛЬ_ВЛАДЕЛЬЦА_СХЕМЫ
```

- Настройка соединения с БД Ignite:

```
orm.metamodel.dialect=org.hibernate.dialect.H2Dialect
orm.metamodel.driver=org.apache.ignite.IgniteJdbcThinDriver
orm.metamodel.url=jdbc:ignite:thin://СЕРВЕР:ПОРТ;schema=СХЕМА
orm.metamodel.username=
orm.metamodel.password=
```

- Выключить внешний пул соединений:

```
orm.cp.external=false
```

3.2.2. Настройка application.properties при использовании внешнего пула соединений

- Режим работы

```
orm.database=DBI
```

- URL для подключения к 2MCA DBI

```
orm.uri=http://СЕРВЕР:ПОРТ/КОНТЕКСТ_СЕРВЕРА_ПРИЛОЖЕНИЙ/rest
```

- Источник данных для внешнего пула соединений:

```
orm.cp.datasource=java:/comp/env/postgres
```

- Настройка соединения с БД Ignite:

```
orm.metamodel.dialect=org.hibernate.dialect.H2Dialect
orm.metamodel.driver=org.apache.ignite.IgniteJdbcThinDriver
orm.metamodel.url=jdbc:ignite:thin://СЕРВЕР:ПОРТ;schema=СХЕМА
orm.metamodel.username=
orm.metamodel.password=
```

Настроить контейнер сервлетов. На примере Apache Tomcat:

В файле `${catalina.base}/conf/context.xml` в секции `Context` прописать:

```
<Resource name="postgres"
    auth="Container"
    type="javax.sql.DataSource"
    driverClassName="org.postgresql.Driver"
    url="jdbc:postgresql://СЕРВЕР:ПОРТ/СХЕМА?currentSchema=uadm,aud,app,public,rtl"
    username=ИМЯ_ВЛАДЕЛЬЦА_СХЕМЫ
    password=ПАРОЛЬ_ВЛАДЕЛЬЦА_СХЕМЫ
    removeAbandonedOnBorrow="true"
    removeAbandonedTimeout="90" />
```

3.3. Настройка работы за балансировщиком

- Необходима настройка передачи заголовков на балансировщике:

```
X-Forwarded-Proto: https
X-Forwarded-For
```

- В `application.properties` добавить:

```
server.forward-headers-strategy=native
server.tomcat.remote-ip-header=x-forwarded-for
server.tomcat.protocol-header=x-forwarded-proto
```

3.4. Логирование

Для записи логов во внешний файл в `application.properties` необходимо добавить:

```
logging.file.name=ПУТЬ_ДО_ПАПКИ_С_ЛОГАМИ/НАЗВАНИЕ_ФАЙЛА.log
```

3.5. Настройка авторизации ADFS

Для аутентификации через ADFS нужно указать настройки в `application.properties`:

```
spring.security.oauth2.client.registration.adfs.client-id=client-id
spring.security.oauth2.client.registration.adfs.client-secret=client-secret
spring.security.oauth2.client.registration.adfs.authorization-grant-
type=authorization_code
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://issuer-uri/adfs
```

`client-id` - Уникальный идентификатор клиента аутентификации. Этот идентификатор можно получить после регистрации приложения в ADFS.

`client-secret` - Секрет клиента. Его можно получить после регистрации приложения в ADFS.

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

- os_user – имя пользователя;
- os_domain – название домена.

Имя пользователя и название домена должны совпадать, с учётом регистра с сетевым именем и сетевым доменом пользователя подсистемы доступа.

Протокол ADFS использует цифровую подпись для обеспечения целостности данных, поэтому необходимо добавить доверительный сертификат в хранилище сертификатов Java (подробнее см. документацию на официальном сайте https://docs.oracle.com/en/java/javase/17/docs/specs/man/keytool.html#importing-a-certificate-for-the-ca).

Подробную информацию по возвожным ошибкам при авторизации с использованием ADFS необходимо уточнять в документации ADFS.

3.6. Настройка авторизации Keycloak

Для аутентификации через Keycloak нужно указать настройки в `application.properties`:

```
spring.security.oauth2.client.registration.keycloak.client-id=client-id
spring.security.oauth2.client.registration.keycloak.client-secret=client-secret
spring.security.oauth2.client.registration.keycloak.authorization-grant-
type=authorization_code
spring.security.oauth2.client.registration.keycloak.redirect-
uri={baseUrl}/login/oauth2/code/{registrationId}
spring.security.oauth2.client.registration.keycloak.scope=openid
spring.security.oauth2.client.provider.keycloak.issuer-uri=https://issuer-
uri/realms/your-realm
```

`client-id` - Уникальный идентификатор клиента аутентификации. Этот идентификатор можно получить после регистрации приложения в Keycloak.

`client-secret` - Секрет клиента. Его можно получить после регистрации приложения в Keycloak.

Обязательные поля, которые Keycloak должен передавать приложению в составе токена OpenID:

- os_user – имя пользователя;
- os_domain – название домена.

Наименование свойств os_user и os_domain в Keycloak задаются строго в нижнем регистре. Имя пользователя и название домена должны совпадать, с учётом регистра с сетевым именем и сетевым доменом пользователя подсистемы доступа.

3.7. Настройка времени жизни токена авторизации

По умолчанию время жизни токена авторизации ограничено и равно 5 минутам. Значение может быть изменено путём непосредственного задания настройки в `application.properties`:

```
security.authentication.jwt.expiration=TIME
```

`TIME` - Время в минутах (m), часах (h) или днях (d). Например, если время жизни токена должно быть равным 30 минутам, то значение настройки следует указать: 30m

Обращаем ваше внимание, что в целях безопасности не рекомендуется устанавливать время жизни токена длительностью более 30 минут.

4. Процедура настройки системы доступа для режима DBI

1. Установить PostgreSQL.
2. Проинициализировать БД с помощью CFT Platform IDE.
3. Создался предустановленный суперпользователь `ibs`.
    a. Администратор средствами БД изменяет пароль `ibs` на безопасный.
    b. Пароль рекомендуется разделить на несколько частей и распределить хранение данных частей по разным сотрудникам.
4. Создались предустановленные технические пользователи: `app_adm`, `app_srv`, `uadmin_usr`.
    a. Администратор средствами БД изменяет пароли технических пользователей на безопасные.
5. Администратор настраивает АРМ "Администратор доступа":
    a. Включает возможность входа по паролю.
    b. Добавляет настройки авторизации по `ADFS`.
    c. Добавляет настройки пула соединения с пользовательскими данными.
    d. Добавляет настройки пула соединения с метаданными.
6. В `ADFS` заводится пользовательская запись, соответствующая `ibs`. Пароль рекомендуется разделить на несколько частей и распределить хранение данных частей по разным сотрудникам.
7. Администратор заходит в АРМ "Администратор доступа" под `ibs`.
    a. Редактирует запись `IBS`. Задает данные для аутентификации по `ADFS`: сетевое имя и домен. Сетевое имя и домен должны соответствовать пользовательской записи из пункта 6.
    b. Создает администраторов доступа.
8. Администратор заходит в АРМ "Навигатор" под `ibs`.
    a. Создает первого прикладного пользователя, того, кто в последствии будет создавать других прикладных пользователей.
    b. Администратор выключает возможность входа по паролю в АРМ "Администратор доступа". Теперь доступ в АРМ возможен только через аутентификации по `ADFS`.
    c. Администратор доступа заходит в АРМ "Администратор доступа" под своей учетной записью.
    d. Создает оператора, соответствующего прикладному.
    e. Наделяет оператора правами создавать прикладных пользователей.
9. Дальнейшее создание пользователей-операторов и наделение их правами производится администраторами доступа под своей учетной записью.

Администратор доступа не может создать другого администратора доступа. Во избежание противоправных действий. При необходимости создания новых администраторов доступа производится под учетной записью суперпользователя ibs.

5. Организация доступа в системе

Система доступа "ЦФТ – Платформа Развития" является надстройкой над системой контроля доступа СУБД. Ее работа базируется на следующих принципах:

- Обеспечить необходимый уровень гибкости и детализации контроля доступа пользователей к информационным ресурсам системы.
- Реализация системы доступа на стороне СП 2 МСА (режим DBI) или сервера БД (режим ТЯ), чтобы пользователь не смог получить доступ к информационным ресурсам "в обход" системы контроля доступа, используя программное обеспечение для работы с СУБД, отличное от клиентских АРМов "ЦФТ – Платформа Развития".

Администрирование и работа с объектами доступа (информационными ресурсами) осуществляется только через зарегистрированные в системе доступа учетные записи (субъекты доступа).

Все объекты функциональной части системы хранятся в отдельной схеме, называемой схемой – владельцем системы OWNER.

Их можно условно разделить на две части:

- Объекты, с которыми взаимодействует администратор системы;
- Объекты, с которыми взаимодействуют пользователи (пользовательские объекты), которые, в свою очередь, делятся на:
  - Системные, относящиеся к ТЯ;
  - Прикладные, относящиеся к ПЯ.

Пользователь не имеет непосредственного доступа к таблицам БД, где хранятся данные предметной области. Вместо этого для просмотра данных он имеет доступ к представлениям (VIEW), внутри которых выполняются следующие проверки:

- доступность данного представления;
- доступность Типов Базовых Понятий, экземпляры которых просматриваются;
- доступность экземпляров (по дополнительному условию при создании представления).

Для манипуляции с данными пользователь имеет доступ к операциям и функциям подсистемы смены состояний. При попытке вызова операции или смены состояния выполняется проверка на доступность пользователю соответствующей операции или перехода.

При нормальном функционировании системы схема-владелец (содержащая все объекты ПЯ) должна быть закрыта от прямого доступа под именем владельца схемы (как правило: IBS или app), создаваемых ролей достаточно для полнофункциональной работы системы. Схема может быть открыта только для выполнения каких-либо регламентных работ.

5.1. Субъекты доступа

Под субъектами доступа в системе подразумеваются пользователи и группы пользователей.

Пользователь

Это учетная запись в системе доступа "ЦФТ – Платформа Развития", под которой осуществляется взаимодействие сотрудника с системой. В зависимости от возложенных обязанностей пользователю назначают необходимую роль.

Группа пользователей

Для оптимизации процесса администрирования доступа пользователей вводится понятие "Группа пользователей" (или "Группа доступа"). Группа пользователей является субъектом доступа и для нее может быть установлен собственный набор прав доступа к информационным ресурсам. В группу могут быть включены: как пользователи, так и другие группы. При этом субъект доступа, включенный в группу, получает те же права, что и эта группа. Таким образом, права пользователя определяются как совокупность (объединение) прав всех групп (иерархии групп), в которые он включен, и его личных прав.

С целью большей прозрачности и лучшей управляемости подсистемы доступа рекомендуется не назначать пользователям никаких личных прав на прикладные объекты. Хорошим тоном считается создание различных групп, соответствующих определенным технологиям работы организации, и включение пользователей в соответствующие группы.

В режиме DBI отсутствует возможность назначения пользователю личных прав. Все права пользователь получает через включение в группы доступа.

Основные классы создаваемых групп:

Индивидуальная

Личная группа пользователя. Как правило, создаётся сразу же при заведении пользователя в прикладной подсистеме операцией "Доступ". Короткое имя создаваемой группы формируется из короткого имени пользователя с добавлением префикса "_" (нижнее подчёркивание). При создании группы ей могут быть сразу назначены права доступа по реквизитам "подразделение" и "филиал", на основании подразделения и филиала, которым принадлежит пользователь, для которого создаётся индивидуальная группа. Рекомендуется использовать эту группу для агрегации прав, характерных исключительно для данного пользователя.

Функциональная

Используется для назначения набора прав, соответствующих определённым должностным обязанностям (например, "Бухгалтер", "Операционист", "Кредитный инспектор").

Организационная

Группа, относящаяся к определенному подразделению (филиалу) организации и характеризующая права доступа к совокупности объектов, относящихся к этому подразделению.

В режиме DBI отсутствует возможность работы с подразделениями

В системе существует специальная группа с идентификатором `ADMIN_GRP`. Если пользователь включен в эту группу, то для него не проверяются права на прикладные элементы модели, все элементы будут доступны такому пользователю. Следует иметь в виду, что поддержка специальной группы `ADMIN_GRP` может быть отключена в системе.

Группа пользователей – это внутренний объект системы доступа "ЦФТ – Платформа Развития" и не является пользователем или ролью БД.

5.2. Доступ к элементам ПЯ

В системе доступа различают следующие типы элементов ПЯ:

- Типы Базовых Понятий (ТБП);
- Представления ТБП;
- Экземпляры ТБП;
- Операции ТБП;

- Переходы ТБП;
- Процедуры. Только в режиме ТЯ.

АРМ "Администратор доступа" позволяет назначать доступ двух типов:

1. Доступ на просмотр данных;
2. Доступ на выполнение действий с данными.

Доступ на просмотр данных

Пользователь не имеет непосредственного доступа к таблицам БД, где хранятся данные предметной области. Вместо этого для просмотра данных он имеет доступ к ТБП и нужным представлениям (view) этого ТБП. В коде представлений имеются следующие проверки:

- доступность данного представления (проверка выполняется безусловно);
- доступность Типов Базовых Понятий, экземпляры которых просматриваются (для представлений для просмотра проверка выполняется безусловно; для представлений для отчётов проверка доступности ТБП может быть включена в свойствах текущего представления);
- доступность экземпляров (если проверка экземпляров включена в свойствах текущего представления).

Доступ на выполнение действий с данными

Для обеспечения требуемого уровня гибкости и детализации доступа права пользователя-оператора ограничиваются средствами подсистемы доступа "ЦФТ – Платформа Развития".

Для выполнения операции пользователь должен иметь доступ к ТБП и нужным операциям этого ТБП. В АРМе "ЦФТ – Навигатор" доступны только те операции, которые доступны пользователю и имеют признак **"Может быть активизирована пользователем"**. При попытке вызова операции или при попытке смены состояния выполняется проверка на доступность пользователю соответствующих операции или перехода.

5.2.1. Доступ к ТБП

Доступ к ТБП сам по себе является необходимым, но недостаточным условием того, чтобы пользователь мог просматривать данные указанного типа или манипулировать ими.

При назначении субъекту доступа прав доступа к ТБП может быть дополнительно указан признак **"Показывать в меню"**. В этом случае такой ТБП будет участвовать в формировании главного меню АРМа "ЦФТ – Навигатор" при работе пользователя, имеющим такое право. Но если у этого пользователя не будет права доступа ни на одно представление для просмотра из данного ТБП, то ничего более пользователь с ТБП сделать не сможет.

В АРМе "Администратор доступа" доступ к ТБП для конкретного субъекта доступа может быть назначен различным образом:

- Раздача доступа на разные объекты одному субъекту.
- Раздача доступа на один объект разным субъектам.

5.2.2. Доступ к представлениям

В рамках каждого ТБП для субъекта определяется список доступных ему представлений. При выполнении выборки данных из каждого представлении, накладываются условия проверки доступа к представлению и к его экземплярам.

Особенности "видимости" представлений, кроме непосредственных прав доступа, определяются так

же некоторыми свойствами самих представлений, а именно:

- "Флаги" – "Проверка доступа";
- "Флаги" – "Наследуется дочерними типами";
- "Флаги" – "Доступно только в операциях";
- "Флаги" – "Доступно только для просмотра экземпляра/коллекции";
- "Флаги" – "Доступно только при вызове в PLPVIEW".

При обращении пользователя в АРМе "ЦФТ – Навигатор" к какому-либо доступному ему ТБП, список доступных ему представлений будет формироваться из всех представлений для просмотра этого типа и родительских ему типов, с учётом вышеприведённых свойств и прав пользователя на доступ к этим представлениям.

Так же ряд свойств представлений влияют на доступ к операциям, которые могут быть вызваны над экземплярами, демонстрирующимися в данном представлении, и на доступ к экземплярам, которые могут демонстрироваться в данном представлении пользователю.

Работа с представлениями для отчётов происходит по тем же правилам, с учётом того, что права на представления для отчётов, в основном, раздаются автоматически, опосредованно, на основании определённых прав доступа на операции типа "Отчёт", базирующихся на рассматриваемых представлениях для отчётов.

В АРМе "Администратор доступа" доступ к представлению для конкретного субъекта доступа может быть назначен различным образом:

- Раздача доступа на разные объекты одному субъекту.
- Раздача доступа на один объект разным субъектам.

5.2.3. Доступ к операциям

В рамках каждого ТБП для субъекта определяется список доступных ему операций. При этом следует иметь в виду, что на операции, которые вызывает пользователь непосредственно из меню АРМа "ЦФТ – Навигатор" или через CALL-синтаксис из других операций, наличие прав доступа у пользователя проверяется обязательно, а если операции вызываются из пакетов других операций напрямую, то права доступа на них у текущего пользователя не проверяются.

Особенности "видимости" операций, кроме непосредственных прав доступа, определяются так же некоторыми свойствами самих операций, а также – представления, находясь в котором происходит попытка вызова операции, а именно:

- свойство текущего представления "Операции" – "Ограниченный набор операций";
- свойство операции "Дополнительные свойства" – "Может быть активизирована пользователем";
- свойство операции "Дополнительные свойства" – "Абсолютно доступна".

При обращении пользователя в АРМе "ЦФТ – Навигатор" к меню операций ТБП в представлении, список доступных ему операций будет формироваться из всех операций этого типа и родительских ему типов, с учётом вышеприведённых свойств и прав пользователя на доступ к этим операциям.

Следует помнить, что присутствие операции в меню не означает возможность её работы. Операция может быть запрещена к выполнению на основании других свойств (таких, как "Категория доступа", "Категория принадлежности", "Приоритет") или могут отработать валидации (проверки), назначенные для данной операции.

В АРМе "Администратор доступа" доступ к операции для конкретного субъекта доступа может быть назначен различным образом:

- Раздача доступа на разные объекты одному субъекту.
- Раздача доступа на один объект разным субъектам.

5.2.4. Доступ к переходам

В рамках каждого ТБП, имеющего состояния, для субъекта определяется список доступных ему переходов. Однако, при автоматическом выборе перехода проверка прав доступа происходит только если необходимость такой проверки указывается явно. Имеет смысл регламентировать права только на переходы, не имеющие признака автоматического выполнения.

Меню переходов в АРМе "ЦФТ – Навигатор" формируется из переходов данного ТБП с учётом прав пользователя на переходы и свойств переходов: * "Из состояния"; * "Автоматический выбор".

В АРМе "Администратор доступа" доступ к переходу для конкретного субъекта доступа может быть назначен различным образом:

- Раздача доступа на разные объекты одному субъекту.
- Раздача доступа на один объект разным субъектам.

5.2.5. Доступ к экземплярам

По умолчанию доступ к экземплярам ТБП определяется доступом к ТБП в целом. В системе реализована возможность ограничения множества доступных пользователю экземпляров. Для каждого Типа Базового Понятия реализовано несколько способов явного и неявного задания доступа к экземплярам.

К неявным способам относится назначение пользователю представлений на просмотр списка экземпляров ТБП, в условиях которых содержится ограничение области доступных экземпляров.

К явным способам относятся назначение режима доступа к конкретному экземпляру или указание ограничений на значения одного или нескольких реквизитов ТБП. Ограничение на значения реквизитов может быть установлено в следующем виде:

- для реквизита типа "ссылка" – указание точного значения;
- для реквизитов типа "строка" – указание символьного шаблона допустимых значений;
- для реквизитов типа "дата" или "число" – указание значения и условия сравнения;
- для реквизитов типа "справочник" – перечислением допустимых значений.

5.2.6. Доступ к процедурам

В режиме DBI отсутствует возможность разграничения доступа к хранимым процедурам БД.

Доступ раздаётся для любых хранимых процедур. Кроме того, можно иметь в виду, что доступ на процедуры, используемые в операциях типа "Отчёт" раздаётся опосредованно, при раздаче прав доступа на соответствующие операции.

В АРМе "Администратор доступа" непосредственный доступ к процедуре для конкретного субъекта доступа может быть назначен различным образом:

- Раздача доступа на разные объекты одному субъекту.
- Раздача доступа на один объект разным субъектам.

6. Пользователи

6.1. Создание/удаление пользователей

6.1.1. Создание пользователя

Для добавления нового пользователя необходимо перейти в раздел "Пользователи" и нажать кнопку "Создать". В открывшейся форме обязательными для заполнения являются поля "Короткое имя" и "Полное имя". В случае создания пользователя с ролью "Оператор" к обязательным полям добавляются поля "Сетевой домен" и "Сетевое имя" на вкладке "Аутентификация".

6.1.2. Создание пользователя по образцу

Доступно только в режиме DBI.

Для добавления нового пользователя по образцу от существующего необходимо открыть нужного пользователя на редактирование и через меню "Действия" выбрать функцию "Создание пользователя по образцу".

Перед открытием формы создания нового пользователя появится окно с чекбоксами "Копировать группы, включающие пользователя" и "Копировать меню пользователя". При необходимости выбрать один или оба.

6.1.3. Удаление пользователя

Для удаления пользователя необходимо открыть пользователя для редактирования и через меню "Действия" выбрать функцию "Удалить пользователя".

6.2. Изменение пароля пользователя

Для изменения пароля пользователя необходимо открыть пользователя для редактирования и нажать кнопку "Изменить пароль".

6.3. Назначение прав доступа пользователю

Назначение прав доступа пользователю выполняется на кладке "Права доступа" при просмотре информации о пользователе. На данной вкладке объекты системы представлены в виде дерева типов. Наименования объектов, к которым у пользователя отсутствует доступ, указаны серым шрифтом. Для назначения прав необходимо выбрать требуемый ТБП, отметить нужные экземпляры ТБП и нажать на кнопку "Разрешить" или "Запретить". Список объектов, к которым планируется предоставить или отозвать доступ за текущую итерацию, можно посмотреть и отредактировать по кнопке "Выбрано". После завершения редактирования прав доступа к объектам системы необходимо нажать на кнопку "Сохранить".

Кнопки "Разрешить" и "Запретить" только формируют список прав, которые будут добавлены/отозваны у субъекта, без нажатия кнопки "Сохранить" права выданы/отозваны не будут.

6.4. Добавление пользователя в группу

На вкладке "Группы" указаны группы в которых состоит пользователь. Добавить пользователя в группу можно через кнопку "+".

6.5. Как посмотреть суммарные права пользователя

Суммарные права пользователя можно посмотреть на вкладке "Суммарные права".

6.6. Как скопировать права пользователю

Для того чтобы скопировать права от другого пользователя, необходимо воспользоваться функцией "Копировать права", которая может быть активирована через кнопку "Действия".

6.7. Формирование отчёта по пользователям

Отчёт может быть сформирован как по одному пользователю, так и по нескольким. Для формирования отчёта необходимо выбрать "Отчёт", в меню "Действия", находясь в разделе "Пользователи" или просматриваю информацию по конкретному пользователю. Доступны следующие отчётов:

- Доступные ТБП, Операции, Представление, Переходы;
- Пользователи с правами администраторов;
- Пользователи, временно получившие права;
- Профили пользователей;
- Список групп, в которые включен пользователь.

6.8. Просмотр общих групп пользователей

Для просмотра общих групп пользователей необходимо в представлении "Пользователи" отметить нужных пользователей и выбрать операцию "Общие группы выбранных пользователей" в меню "Действия".

7. Группы доступа

7.1. Создание/удаление групп доступа

7.1.1. Создание группы доступа

Для добавления новой группы доступа необходимо перейти в раздел "Группы доступа" и нажать кнопку "Создать".

7.1.2. Удаление группы доступа

Для того, чтобы удалить группу доступа, необходимо открыть группу доступа для просмотра, затем в меню "Действия" выбрать "Удалить группу".

7.1.3. Создание группы по образцу пользователя

Для создания группы доступа, обладающей правами доступа как у конкретного пользователя, необходимо перейти в раздел "Пользователи", открыть пользователя, от которого планируется скопировать права, и выбрать операцию "Создание группы по образцу" в меню "Действия". В открывшемся окне необходимо указать короткое и полное имена создаваемой группы, выбрать одно или несколько значений и нажать кнопку "Создать":

- Копировать права на типы;
- Копировать права на представления;
- Копировать права на операции;
- Копировать права на переходы;
- Копировать права на экземпляры;
- Копировать права доступа по реквизиту.

7.2. Импорт/экспорт групп доступа

7.2.1. Импорт группы доступа

Для выполнения импорта групп доступа необходимо нажать на кнопку "Загрузить" в разделе "Группы доступа". В окне импорта есть возможность установить признак "Заменить все права и подгруппы".

7.2.2. Экспорт группы доступа

Для экспорта группы доступа необходимо в разделе "Группы доступа" отметить необходимые группы доступа и выбрать операцию "Экспорт" в меню "Действия". Также экспорт может быть выполнен при просмотре группы доступа. Для этого необходимо перейти на вкладку "Текстовый вид" и нажать "Скачать".

7.3. Назначение прав доступа группе

Назначение прав группе доступа выполняется на кладке "Права доступа" при просмотре информации о группе доступа. На данной вкладке объекты системы представлены в виде дерева типов. Наименования объектов, к которым у группы отсутствует доступ, указаны серым шрифтом. Для назначения прав необходимо выбрать требуемый ТБП, отметить нужные экземпляры ТБП и нажать на кнопку "Разрешить" или "Запретить". Список объектов, к которым планируется предоставить или отозвать доступ за текущую итерацию, можно посмотреть и отредактировать по кнопке "Выбрано". После завершения редактирования прав доступа к объектам системы необходимо

нажать на кнопку "Сохранить".

Кнопки "Разрешить" и "Запретить" только формируют список прав, которые будут добавлены/отозваны у субъекта, без нажатия кнопки "Сохранить" права выданы/отозваны не будут.

7.4. Добавление группы в группу

Для того чтобы добавить одну группу доступа в другую, необходимо перейти на вкладку "Группы". Данный раздел содержит два представления:

- Входят в группу - здесь перечислены группы, которые входят в рассматриваемую группу доступа;
- Группы, включающие группу - здесь перечислены группы, в которые включена рассматриваемая группа доступа.

Используя кнопки "+" и "Удалить" в нужном представлении, можно настроить иерархию групп. Также в представлениях доступна выгрузка списка групп в CSV формате.

7.5. Список пользователей группы

Для того чтобы посмотреть список пользователей входящих в группу, необходимо перейти на вкладку "Пользователи". В данном представлении осуществляется добавление/удаление пользователей в рассматриваемую группу, также доступна функция выгрузки списка пользователей группы в CSV формате.

7.6. Выдача/копирование доступа по реквизиту

7.6.1. Выдача доступа по реквизиту

Настройка доступа по реквизиту производится на вкладке "Доступ по реквизиту". На первом этапе необходимо выбрать ТБП, в котором будет проверяться доступ. Для этого в блоке "ТБП, в котором проверяется доступ" вызываем операцию "Добавить доступ" нажатием на "+". В открывшемся окне выбираем ТБП и нажимаем "Далее", выполнится переход ко второму этапу. На втором этапе необходимо выбрать ТБП, на который ссылается реквизит, и нажать кнопку "Далее", выполнится переход к третьему этапу. На третьем этапе необходимо выбрать экземпляры ТБП и нажать кнопку "Добавить".

7.6.2. Копирование прав доступа по реквизиту

Для копирования прав доступа по реквизиту необходимо использовать операцию "Копировать права" в меню "Действия".

7.7. Поэкземплярный доступ

Настройка доступа по экземпляру осуществляется на вкладке "Доступ по экземпляру". Для настройки доступа необходимо выбрать нужный ТБП в колонке слева. В колонке справа отобразятся экземпляры выбранного ТБП с отметкой наличия/отсутствия доступа. Для редактирования доступа к экземплярам необходимо нажать на кнопку "Редактировать права на экземпляры". Откроется окно выбора экземпляров, в котором представлены две колонки: "Недоступные экземпляры" и "Доступные экземпляры". Чтобы предоставить доступ, отмечаем требуемые экземпляры в колонке "Недоступные экземпляры" и нажимаем кнопку "+" ("Разрешить доступ"). Выбранные экземпляры переместятся в колонку "Доступные экземпляры", далее нажать "Сохранить".

Настройка правил доступа по экземпляру осуществляется на вкладке "Доступ по экземпляру". Для

просмотра правил доступа необходимо выбрать нужный ТБП в колонке слева. В колонке справа отобразятся экземпляры выбранного ТБП, с отметкой наличия/отсутствия доступа, а в таблице внизу отобразятся правила доступа, если они настроены. Для добавления нового правила необходимо выбрать реквизит, нажав на "Добавить реквизит", а затем, нажатием на "+", создать правило.

7.8. Копирование прав группе доступа

7.8.1. Копирование прав группе

Чтобы скопировать права группе доступа от другой группы, необходимо перейти в группу доступа, которой планируется скопировать права, и выбрать операцию "Копировать права от группы" в меню "Действия". В открывшемся окне необходимо выбрать группу доступа, от которой будут скопированы права, и нажать кнопку "Дальше". На втором шаге необходимо выбрать одно или несколько значений и нажать кнопку "Копировать":

- Копировать группы;
- Копировать права на типы;
- Копировать права на представления;
- Копировать права на операции;
- Копировать права на переходы;
- Копировать права на экземпляры;
- Копировать права доступа по реквизиту.

7.8.2. Копирование прав от группы

Чтобы скопировать права от группы доступа другой группе или нескольким группам, необходимо перейти в группу доступа, от которой планируется скопировать права, и выбрать операцию "Копировать права" в меню "Действия". В открывшемся окне необходимо: * Выбрать одну или несколько групп доступа, в которые будут скопированы права, и нажать кнопку "Дальше"; * Выбрать группы, которые будут скопированы грппе/группам доступа, и нажать кнопку "Дальше" (по умолчанию группы не копируются); * Выбрать права, которые будут скопированы, и нажать кнопку "Дальше" (по умолчанию права не копируются). * Копировать доступ по экземплярам (по умолчанию доступ не копируется). * Копировать доступ по реквизиту (по умолчанию доступ не копируется). Если необходимо скопировать доступ по реквизиту на новый экземпляр для текущей группы, на этапе выбора групп доступа активируйте переключатель "Использовать текущую группу".

7.9. Формирование отчёта по группам доступа

По группам доступа есть возможность формирования следующих отчётов:

- Доступ к экземплярам системы;
- Доступ по реквизиту;
- Доступные ТБП, Операции, Представления, Переходы;
- Список пользователей группы.

Операция "Отчёт" может быть вызвана из меню "Действия" в разделе "Группы доступа" или при просмотре информации по группе доступа. Для того, чтобы сформировать отчёт, в разделе "Группы доступа" необходимо выбрать требуемые группы и вызвать операцию "Отчёт". Если вызвать отчёт без выбора групп, то отчёт будет сформирован по всем группам.

7.10. Суммарные права группы доступа

Во вкладке "Суммарные права" есть возможность посмотреть все права на объекты доступа, принадлежащие группе доступа, включая права, наследуемые от групп доступа, в которые группа доступа была включена.

Для вкладки "Суммарные права" доступна выгрузка объектов в формате CSV с параметрами фильтра:

- Типы данных;
- Операции;
- Представления;
- Переходы.

8. Объекты доступа

В разделе "Объекты доступа" представлены объекты доступа в виде дерева типов с возможностью поиска и фильтрацией по типу объекта. Для просмотра объекта доступа, необходимо перейти по короткому имени объекта из окна поиска или дерева типов. В открывшемся представлении доступны следующие вкладки:

- Основная информация;
- Имеют доступ - группы, имеющие доступ к объекту, представлены в виде иерархии групп;
- Группы - группы, имеющие доступ к объекту, представлены в плоском виде;
- Доступ по реквизиту.

8.1. Добавление доступа к объекту

Для добавления доступа к объекту, необходимо перейти на вкладку "Группы" и нажать на "+", в открывшемся окне можно выбрать группы, которым необходимо предоставить доступ к объекту.

8.2. Копирование доступа

Для того, чтобы скопировать доступ от одного объекта доступа другому, необходимо выполнить операцию "Копировать доступ" в меню "Действия". В открывшемся окне необходимо выбрать объекты, которым требуется скопировать доступ.

9. Профили пользователей

Добавление, удаление и редактирование профилей пользователей осуществляется в разделе "Профили".

9.1. Свойства пользовательских профилей

Профили пользователей могут иметь свойства:

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]".
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. Примечание Свойство поддерживается на схемах с версией ТЯ 7.6.1.0 и выше.
ALTER_SESSION	Описание параметров в виде "параметр=значение" через пробел	Параметры пользовательских сессий, использующих текущий профиль.
AUD.NAV.VW.STATES	YES/NO	Флаг определяет доступность пользователю функции «Просмотр журнала состояний» в АРМ «ЦФТ – Навигатор»: YES - функция доступна; NO - функция недоступна. Примечание Свойство поддерживается АРМом «ЦФТ – Навигатор» версии 6.0.121.36 и выше.

Наименование свойства	Возможные значения	Описание
AUD.NAV.VW.VALUES	YES/NO	Флаг определяет доступность пользователю функции «Просмотр истории изменений» в АРМ «ЦФТ – Навигатор»: YES - функция доступна; NO - функция недоступна. Примечание Свойство поддерживается АРМом «ЦФТ – Навигатор» версии 6.0.121.36 и выше.
AUD.OPEN_VIEW	YES/NO	Флаг необходимости журналирования открытия представлений для конкретного пользователя: YES – все открытые пользователем представления всегда журналируются; NO – значение по умолчанию, необходимость журналирования определяется настройками представлений в АРМе «Администратор словаря данных». Примечание Свойство поддерживается на схемах с версией ТЯ 7.4.2.5 и выше АРМом «ЦФТ – Навигатор» версии 6.0.118.30 и выше, Сервером Приложений 2 МСА версии 2.42.19 и выше.
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, необходимость журналирования параметров операций определяется настройками операций в АРМе «Администратор словаря данных» и настройками формы журналирования параметров операций в АРМе «Рабочее место ревизора». Примечание Свойство поддерживается на схемах с версией ТЯ 7.4.2.5 и выше АРМо«м ЦФТ – Навигато»р версии 6.0.118.30 и выше, Сервером Приложений 2 МСА версии 2.42.19 и выше.

Наименование свойства	Возможные значения	Описание
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; Примечание Свойство поддерживается на схемах с версией ТЯ 7.4.9.0 и выше, АРМо«м ЦФТ – Навигато»р версии 6.0.119.28 и выше.
CREATE_SYNONYMS	YES/NO	Режим инициализации сессий пользователей для отчётов: YES – синонимы создаются по существующим зависимостям отчётов; NO – синонимы не создаются. Примечание Если в профиле пользователя CREATE_SYNONYMS = NO, то при любом выборе действия в окне команды «Пересоздание синонимов для отчетов» будут удалены все синонимы пакетов и представлений пользователя, в том числе созданные DBA.
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.

Наименование свойства	Возможные значения	Описание
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).

Наименование свойства	Возможные значения	Описание
IDE_ADMIN_READ_ONLY	YES/NO	Режим модификации модели в сессии: YES – запрет на модификацию модели пользователем, NO – модификация модели пользователем разрешается. Значение параметра учитывается только в соединении в CFT Platform IDE со схемой. По умолчнию NO. Примечание Свойство поддерживается CFT Platform IDE версии 2.36.43 и выше.
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.FILTER.EXT.ENABLED	YES/NO	Определяет возможность использовать пользовательский фильтр, указанный в поле Дополнительно в окне формирования фильтра (2MCA_PROXY - по умолчанию YES, 2MCA и 2MCA DBI - по умолчанию NO).
NAV.VW.FILTER.SECURITY_CHECK	YES/NO	Включает проверку полей с дополнительными фильтрами на соответствие политики безопасности (2MCA_PROXY - по умолчанию NO, 2MCA и 2MCA DBI - по умолчанию YES).
NAV.VW.REFCING	YES/NO	Флаг определяет доступность функции «Поиск ссылок на экземпляр» в АРМ «ЦФТ – Навигатор»: YES - функция доступна; NO - функция недоступна. Примечание Свойство поддерживается АРМом «ЦФТ – Навигатор» версии 6.0.121.36 и выше.

Наименование свойства	Возможные значения	Описание
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_CHARACTERS	Разделители, например: '.,'	Настройка разделителей в клиентской сессии.
NLS_SETTINGS	NLS-параметры и их значения. Например: NLS_LANGUAGE=RUSSI AN NLS_SORT=BINARY NLS_NUMERIC_CHARAC TERS='.,' NLS_TERRITORY=CIS NLS_DATE_FORMAT='DD /MM/YY'	Возможность задать NLS-параметры одной строкой.
NLS_SORT		Настройка сортировки в клиентской сессии.
NLS_TERRITORY		Установка региональных настроек в клиентской сессии.
NOVO.3L.LOCK_SESSION	YES/NO	Включает режим перманентной блокировки 3L-сессий (YES – 3L- сессия перманентно блокируется, NO – значение по умолчанию, не блокируется).
NOVO.3L.FORBID_PASSWORD_ CHANGE	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). Примечание Свойство поддерживается АРМом "ЦФТ – Навигатор" начиная со 116 версии.
NOVO.START_METHOD	Операция для запуска в формате <ТБП>.<Короткое имя операция>	При соединении со схемой через АРМ "ЦФТ – Навигатор" автоматически запускается операция, указанная в параметре.
NOVO.REPORT_SCHEDULE	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".

Наименование свойства	Возможные значения	Описание
NOVO.FORBID_VIEW_COPY_ROWS	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". Примечание Свойство поддерживается на схемах с версией ТЯ 7.4.9.0 и выше, АРМо«м ЦФТ – Навигато»р версии 6.0.119.28 и выше.
OOXML_EXPORT	YES/NO	Флаг определяет возможность печати в файл формата Office Open XML (*.xlsx). YES – разрешено, NO – значение по умолчанию, запрещено. Примечание Свойство поддерживается АРМом "ЦФТ – Навигатор" начиная с версии 6.0.121.28.
OOXML_USER	YES/NO	Флаг определяет возможность использования стороннего ПО (не MS Office) для работы с отчётами, выполненными в формате OOXML. YES – разрешено, NO – значение по умолчанию, запрещено. Примечание Механизм действует на схемах с версией ТЯ 7.3.8.0 или выше. Свойство поддерживается АРМом "ЦФТ – Навигатор" начиная со 117 версии.

Наименование свойства	Возможные значения	Описание
PLP_READ_ONLY_ON_START	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. Механизм действует на схемах с версией ТЯ 7.3.6.2 или выше.
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. Подробности см. далее, после таблицы.
SHOW_LEGAL_NOTICE	YES/NO	Показ уведомления об ответственности при входе в АРМ "ЦФТ – Навигатор".
SHOW_LOGINS_HISTORY	YES/NO	Показ истории входов пользователей в случае обнаружения попыток несанкционированного доступа. Подробности см. далее, после таблицы.
USER_CONTEXT	Название функции	Функция инициализации пользовательского контекста (должна возвращать строку).
USER_LOCK_OPEN	Название функции	Функция инициализации пользовательского сеанса (должна возвращать строку).

Наименование свойства	Возможные значения	Описание
VIEWPRINTLOCK	YES/NO	Определяет доступность печати представлений пользвателю. При отсутствии параметра печать представлений разрешена. Примечание Свойство поддерживается АРМом "Администратор доступа" версии 6.86.0.72 и выше и АРМом « ЦФТ – Навигато»р версии 6.0.121.13 и выше.

9.1.1. Ограничение количества сессий

При использовании свойств SESSIONS_PER_USER и SESSIONS_PER_USER_MODE следует помнить их особенности. Значение SESSIONS_PER_USER=0 означает полный запрет на подключение. Значение SESSIONS_PER_USER='пусто', или SESSIONS_PER_USER='UNLIMITED', или отсутствие параметра SESSIONS_PER_USER означает отсутствие ограничения. Для каждого из АРМов подсчет количества сессий ведется отдельно. Таким образом, пользователь может одновременно зайти в несколько АРМов "Администратор проектов" и несколько АРМов "Администратор словаря данных", даже в том случае, если суммарно их количество будет превышать установленный лимит сессий. Каждое подключение АРМов системы считается одной сессией. Т.е., при SESSIONS_PER_USER=2 пользователь может подключиться к схеме двумя идентичными АРМами одновременно. Параметр SESSIONS_PER_USER может быть определен в профиле пользователя Oracle непосредственно в базе данных. При этом взаимодействие со значением параметра в профиле пользователя "ЦФТ – Платформа Развития" происходит следующим образом:

- если значение параметра SESSIONS_PER_USER в профиле пользователя Oracle (определяется непосредственно в БД) задано как 'UNLIMITED', то при любом значении параметра SESSIONS_PER_USER_MODE в профиле пользователя "ЦФТ – Платформа Развития" (задающемся в АРМе "Администратор доступа") количество АРМов, которое данный пользователь может одновременно запустить, ограничивается параметром SESSIONS_PER_USER в профиле пользователя "ЦФТ – Платформа Развития";
- если значение параметра SESSIONS_PER_USER в профиле пользователя Oracle есть некоторое число, то:
  - если значение параметра SESSIONS_PER_USER_MODE в профиле пользователя "ЦФТ – Платформа Развития" есть USE_PROFILE, то количество идентичных АРМов, которое данный пользователь может одновременно запустить, ограничивается параметром SESSIONS_PER_USER в профиле пользователя "ЦФТ – Платформа Развития";
  - при любых других значениях параметра SESSIONS_PER_USER_MODE в профиле пользователя "ЦФТ – Платформа Развития" количество АРМов, которое данный пользователь может одновременно запустить, ограничивается параметром SESSIONS_PER_USER в профиле пользователя Oracle.
- если на уровне базы данных включена обработка параметра SESSIONS_PER_USER, то одновременно запустить можно не больше АРМов, чем указано в параметре SESSIONS_PER_USER в профиле пользователя Oracle.

Важно! *Для пользователей, работающих в **CFT Platform IDE**, минимальне значение параметра SESSIONS_PER_USER - **4**, что соответствует минимальному количеству активных соединений для одного запущенного CFT Platform IDE. Для корректной работы IDE (в зависимости от режима) значение данного параметра должно быть согласовано с установленными на схеме системными параметрами IDE.MAX_CONNECTIONS и IDE.CLM.MAX_CONNECTIONS, подробнее см. документацию CFT Platform IDE.*

9.1.2. Показ истории входов пользователей

Если в профиле пользователя указано SHOW_LOGINS_HISTORY = YES, то в АРМе "ЦФТ – Навигатор" при успешном подключении к БД, в случае если до этого были зафиксированы несанкционированные попытки доступа, поднимается окно **"История подключений"**, в котором демонстрируются последнее успешное подключение и последующие попытки несанкционированного подключения. Также в окне имеется возможность сообщить об обнаруженных попытках несанкционированного доступа администратору системы.

Примечание *Для включения механизма показа истории входов пользователей необходимо на схеме включить активный аудит и выполнить скрипт регистрации событий CR_MAIL.SQL. Скрипт CR_MAIL.SQL входит в комплект Серверной Части ТЯ.*

9.1.3. Наследование значений свойств профиля

Если параметр не задан для конкретного профиля, то будет использовано значение из профиля DEFAULT. Это верно для всех свойств профиля, кроме случаев, оговоренных далее. Если следующие параметры не заданы в конкретном профиле, то будет использовано умолчательное значение, а не значение, указанное в профиле DEFAULT:

Наименование свойства	Умолчательное значение
FIO_MAKE_DIR	NO
NLS_DATE_FORMAT	'DD/MM/YYYY'
NLS_LANGUAGE	'RUSSIAN'
NLS_NUMERIC_CHARACTERS	'.,'
NLS_SORT	'BINARY'
NLS_TERRITORY	'CIS'
NOVO.REPORT_SCHEDULE	'NO'

Не наследуется параметр IDLE_TIME. АРМы получают его значение через вызов функции utl_file.get_resource(), которая читает значение из профиля пользователя. Значения нижеследующих свойств всегда берутся из профиля DEFAULT, даже если они заданы в конкретном профиле:

Наименование свойства
FIO_HOME_DIR
FIO_REPLACE_DIR
FIO_TEMP_DIR
FIO_LOG_FILE

Для параметра FIO_BASE_DIR происходит объединение значений, указанных в профиле DEFAULT и в текущем профиле пользователя.

10. Журнал действий

Просмотр журнала действий осуществляется в разделе "Журнал действий".