# Руководство
# Программного обеспечения Domination Management Server
# (Центральный сервер управления)

Версия 1.1

[Документация, содержащая описание функциональных характеристик программного обеспечения и информацию, необходимую для установки и эксплуатации программного обеспечения]

# 1. Лицензионное соглашение

Настоящее Лицензионное соглашение является документом, регулирующим правила использования программного продукта Domination (далее «Программа») лицом, обладающим правомерно изготовленным и введенным в гражданский оборот экземпляром данного продукта («Лицензиатом»).

Настоящее Лицензионное соглашение действует в течение всего срока эксплуатации Лицензиатом Программы и/или нахождения у него экземпляров Программы. Устанавливая Программу, осуществляя ее запись в память ЭВМ, Лицензиат признает правила настоящего Лицензионного соглашения.

По настоящему Лицензионному соглашению Лицензиат получает право использовать Программу способами, описанными ниже.

**АВТОРСКИЕ ПРАВА**

Программа защищена национальными законами и международными соглашениями об авторском праве. Все исключительные авторские права на Программу принадлежат правообладателю. При распространении программы обязательно указывается имя правообладателя, его контактная информация и сайт правообладателя.

**ПРАВА УСТАНОВКИ И ИСПОЛЬЗОВАНИЯ**

Лицензиат имеет право устанавливать и использовать Программу на компьютерах:

– при приобретении Программы в комплекте с видеосервером на материальном носителе на неограниченном количестве компьютеров;

– при приобретении Программы через Интернет на неограниченном количестве компьютеров.

После установки Программы Лицензиат получает право использовать Программу и ее компоненты бесплатно, без лицензионных отчислений неограниченное время согласно условиям данного Лицензионного соглашения.

Программа поставляется «как есть».

Лицензиат обязуется не допускать нарушений исключительных прав правообладателя на Программу, в частности, не совершать и не допускать совершения следующих действий без специального письменного разрешения правообладателя:

1) распространять части программы, ее компоненты отдельно от остальных компонентов программы;

2) запрещено коммерческое распространение Программы (за распространение Программы запрещено брать деньги);

3) вносить какие-либо изменения в код Программы, за исключением тех, которые вносятся штатными средствами, входящими в состав Программы и описанными в сопроводительной документации;

4) осуществлять доступ к информационной базе Программы и построение систем на основе Программы с помощью средств и технологических решений, не предусмотренных в сопроводительной документации;

5) совершать действия, результатом которых является устранение или снижение эффективности технических средств защиты авторских прав, применяемых правообладателем Программы, включая применение программных и технических средств «мультиплексирования», средств, изменяющих алгоритм работы программных или аппаратных средств защиты Программы, а также использовать Программу с устраненными или измененными без разрешения Правообладателя средствами защиты;

6) восстанавливать исходный код, декомпилировать и/или деассемблировать программную часть системы, менять что-либо в ней и дополнять ее новыми функциями, за исключением тех случаев, и лишь в той степени, в какой такие действия специально разрешены действующим законодательством.

Программа может включаться в состав платных сборников, помещаться на сайтах, отличных от сайта правообладателя только с разрешения правообладателя.

**ОГРАНИЧЕНИЕ ГАРАНТИЙНЫХ ОБЯЗАТЕЛЬСТВ**

Программа может содержать ошибки. Правообладатель не несет ответственности за возможные ошибки Программы.

Правообладатель не гарантирует, что функции, содержащиеся в Программе, будут удовлетворять заявленным требованиям, или что работа Программы не прервется из-за ошибки.

Правообладатель намеренно отказывается от всех письменно заявленных и предполагаемых по умолчанию гарантийных обязательств, включая ограничения в применении гарантийных обязательств после определенного срока и годности Программы к продаже.

Ни при каких обстоятельствах правообладатель не несет обязательств перед пользователем за любой вред, физический или коммерческий, нанесенный данной Программой, включая упущенную прибыль, потерю данных, ущерб репутации или другой побочный, или косвенный вред, произошедший из-за использования или неспособности использования данной Программы. Также не принимаются иски на любые другие имущественные требования пользователя Программы.

**КОНТРОЛЬ НАД СОБЛЮДЕНИЕМ ОБЯЗАТЕЛЬСТВ**

Это Лицензионное соглашение соответствует национальным законам об авторском праве. Данное Лицензионное соглашение основано на новой редакции этих законов, что отменяет все остальные договоренности и соглашения, ранее применяемые по отношению к данной Программе.

Все спорные вопросы решаются по взаимной договоренности сторон, а если соглашения не было достигнуто, то в судебном порядке в порядке, предусмотренном действующим законодательством Российской Федерации.

**КОНТАКТНАЯ ИНФОРМАЦИЯ**

Правообладатель: ООО «ВИПАКС+»
Россия, г. Пермь, ул. Краснова, д. 24.
Тел. 8-800-700-20-95

http://vipaks.com
info@vipaks.com

# 2. Общие сведения

## 2.1. Полное наименование программного обеспечения

Полное наименование: Domination Management Server (Центральный сервер управления).

## 2.2. Краткое наименование программного обеспечения

Краткое наименование: ЦСУ или Центральный сервер управления.

## 2.3. Термины и сокращения

| **Сокращение/термин** | **Расшифровка сокращения/Описание термина** |
|---|---|
| ПК | Персональный компьютер |
| ПО | Программное обеспечение |
| АПК Domination | Аппаратно-программный комплекс Domination. Это решение, состоящее из видеосерверов, специализированного ПО и модулей видеоаналитики |
| Видеосервер | Видеосервер Domination – устройство для записи видеоданных |
| Конфигуратор видеосервера | ПО, предназначенное для настройки видеосервера Domination |
| Сервер аналитики | ПО, предназначенное для обработки и анализа изображения с камер, подключенных к видеосерверам Domination, без участия человека |
| Конфигуратор аналитики | ПО, предназначенное для настройки сервера аналитики |
| Клиент Domination (Domination Client) | Клиентское приложение, предназначенное для получения видеоданных и событий с видеосерверов Domination |
| ПКМ | Правая кнопка мыши |

# 3. Системные требования

## 3.1. Минимальные системные требования к ПК

Операционная система: Windows 10, Windows Server 2012 – 2019, Astra Linux 1.7.2 и выше.
Дополнительное ПО: Microsoft.NET 7.
Процессор: Intel i3 530.
Оперативная память: 4 GB.
Свободное место на диске для программы: не менее 5 GB.
Поддерживаемые web-браузеры: Google Chrome, Opera, Microsoft Edge, Mozilla Firefox.
Domination Client: версия 2.12 и выше.
При использовании сервера аналитики: версия 1.9 и выше.

## 3.2. Требование к видеосерверу Domination

Видеосервер Domination: версия 2.1.4.6 и выше.

# 4. Функциональные характеристики программного обеспечения

ЦСУ (Центральный сервер управления) – это ПО, которое устанавливается на выделенный сервер и позволяет администрировать системы видеонаблюдения, построенные на базе оборудования Domination.

Основные функции ЦСУ:

1) создание единого хранилища настроек;
2) управление учетными записями пользователей;
3) логирование действий пользователей;
4) резервное копирование каналов видеосерверов.

Для работы ПО ЦСУ с системой видеонаблюдения, построенной на базе видеосерверов Domination, требуется приобретение Лицензии в количестве, равном количеству каналов на видеосерверах Domination.

Для работы ЦСУ обязательно требуются «Лицензия ЦСУ для управления пользователями (базовая лицензия)» и ключ защиты «Ключ-USB электронный для лицензирования ПО ЦСУ Domination».

**Лицензии**:

- лицензия ЦСУ для управления пользователями (базовая лицензия);
- лицензия ЦСУ для мониторинга действий пользователей.

Если аппаратного USB-ключа с лицензией нет, то после установки ЦСУ открывается в демонстрационном режиме с демо-лицензией (далее по тексту – демо-режим). Демо-режим позволяет ознакомиться с основным функционалом системы.

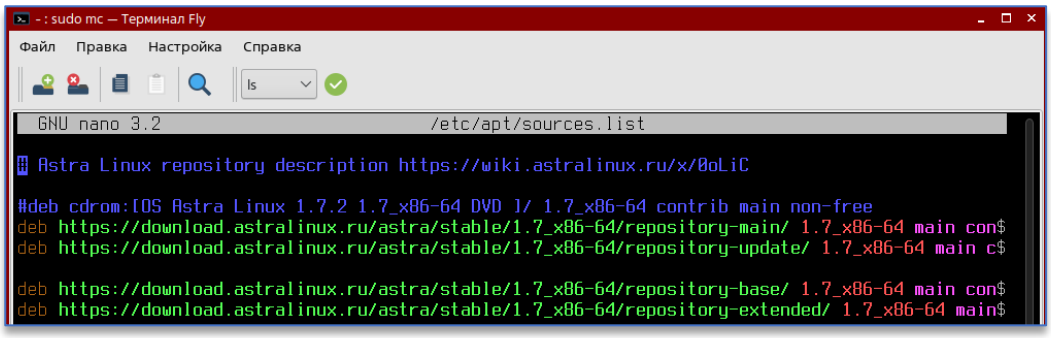
В демо-лицензии доступны:

- 16 каналов, которые можно назначить пользователям для просмотра;
- 1 канал для резервирования.

Запись лога действий пользователей в демо-режиме недоступна. Доступен только просмотр лога, который мог быть записан при наличии полноценной лицензии.

## 5. Установка Domination Management Server на Linux

Перед началом установки на Astra Linux следует обновить список пакетов. Для этого требуется закомментировать строки «deb cdrom: [OS Astra Linux …. DVD]» в файле **«/etc/apt/sources.list»** и раскомментировать все строки «deb https://download.astralinux.ru/.....».




После подключения репозитория обновить список пакетов командой:
sudo apt -y update

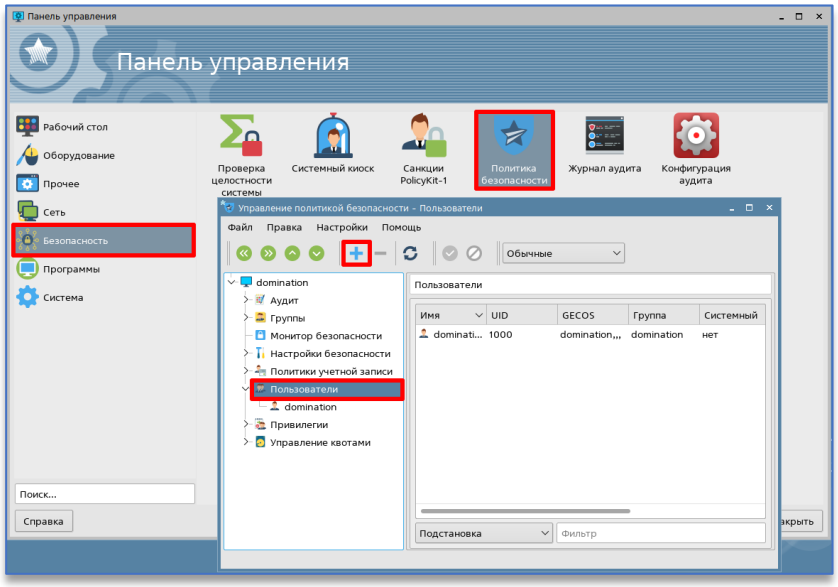
Для работы ключа защиты Guardant необходимо установить библиотеку:
sudo apt -y install libusb-1.0-0 libusb-0.1-4

Далее необходимо установить базу данных PostgreSQL командой:
sudo apt -y install postgresql

Если используется ОС Astra Linux «Смоленск», то после установки PostgreSQL необходимо:
Дать права PostgreSQL на чтение мандатов:
sudo usermod -a -G shadow postgres
sudo setfacl -d -m u:postgres:r /etc/parsec/macdb
sudo setfacl -R -m u:postgres:r /etc/parsec/macdb
sudo setfacl -m u:postgres:rx /etc/parsec/macdb
sudo setfacl -d -m u:postgres:r /etc/parsec/capdb
sudo setfacl -R -m u:postgres:r /etc/parsec/capdb

sudo setfacl -m u:postgres:rx /etc/parsec/capdb

Создать пользователя «enterprise» с паролем «enterprisePW» – «**Пуск – Панель управления – Безопасность – Политика безопасности – Пользователи**», нажать на кнопку  .




После установки базы данных нужно добавить роль:
sudo -u postgres psql -U postgres -c "CREATE ROLE enterprise WITH login createdb PASSWORD 'enterprisePW'"

Для установки deb пакета ЦСУ необходимо из консоли прописать:
sudo dpkg -i «путь до пакета»

Для проверки статуса службы Domination Management Server:
sudo systemctl status dms

После установки Domination Management Server обязательно надо настроить конфигурационный файл appsettings.json.

## 6. Расположение файлов

**Windows:**

- Программа (по умолчанию) – «C:\Program Files (x86)\Vipaks\Domination Management Server»,
- Конфигурационный файл appsettings.json – «C:\ProgramData\Vipaks\Domination Management Server»,
- Логи Domination Management Server – «C:\ProgramData\Vipaks\Domination Management Server\logs».

**Linux:**

- Программа – «/opt/DominationManagementServer»,
- Конфигурационный файл appsettings.json – «/var/cache/vipaks/DominationManagementServer»,
- Логи Domination Management Server – «/var/log/vipaks/DominationManagementServer».

# 7. Настройка программного обеспечения

## 7.1. Настройка Active Directory для работы с ЦСУ

Если не планируется использовать аутентификацию с помощью Active Directory, то пункты 5.1 и 5.2 нужно пропустить.

Для включения аутентификации через Active Directory необходимо добавить атрибуты пользователям на сервере Active Directory. А также создать пользователя домена (например: «dominationServiceAccount») и запомнить его пароль.

В дальнейшем пароль потребуется прописать в файле конфигурации **appsettings.json.**

Путь до файла appsettings.json **на Windows**: C:\ProgramData\Vipaks\Domination Management Server

Путь до файла appsettings.json **на Linux**: /var/cache/vipaks/DominationManagementServer

**Лог-файлы** о работе ЦСУ находятся в той же директории в подпапке logs.

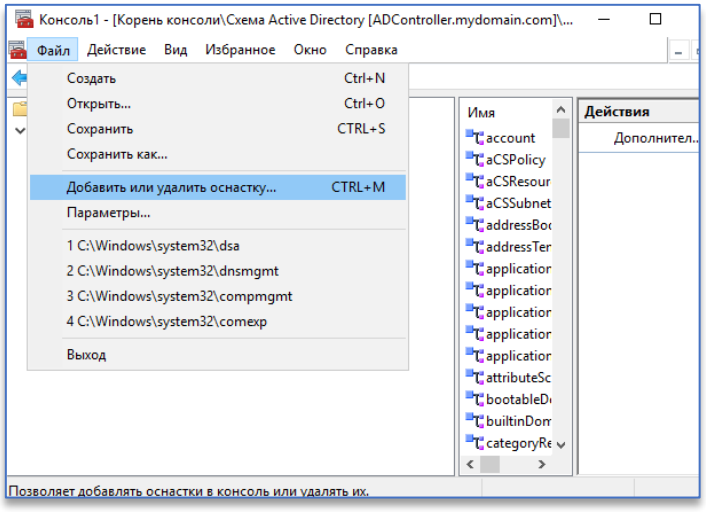
## 7.2. Создание атрибутов для Active Directory

Выполнить в cmd.exe команды:

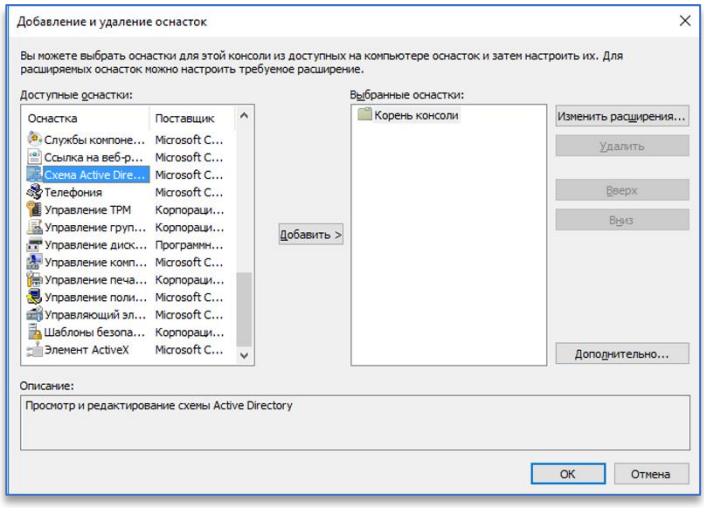
***regsvr32 schmmgmt.dll***

***mmc***

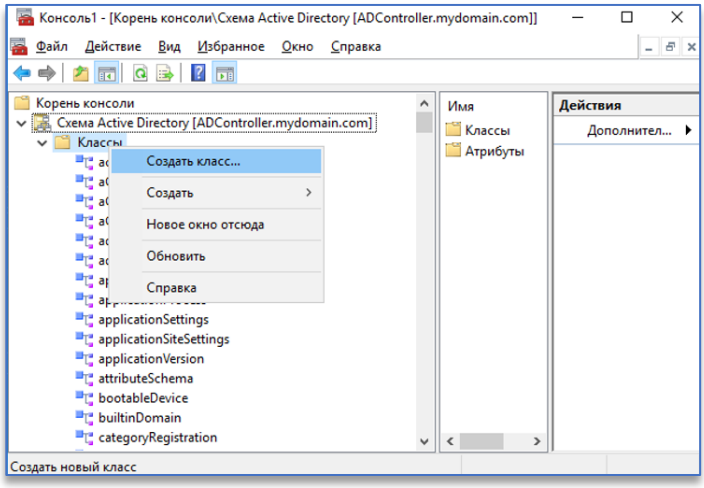
В открывшемся окне **«Консоль1 – Корень консоли»** выбрать «**Файл**» – «**Добавить или удалить оснастку**».




В окне **«Добавление и удаление оснасток»** найти **«Схема Active Directory»** и нажать **«Добавить >»**. Подтвердить действие, нажав на кнопку «**ОК**».

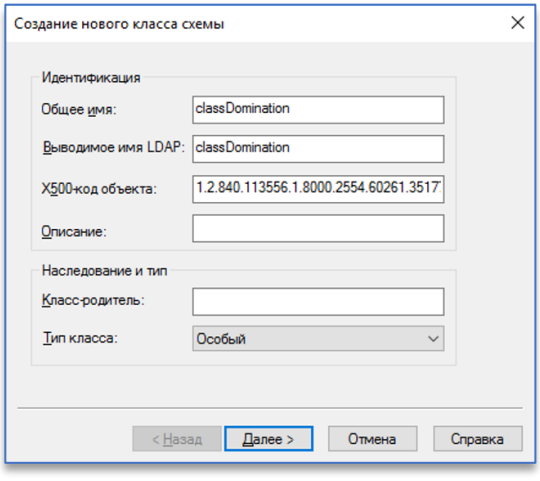



В окне «**Консоль1 – Корень консоли**» раскрыть «**Схема Active Directory**» и «**Классы**». Нажать ПКМ по директории «**Классы**», далее нажать «**Создать класс...**».

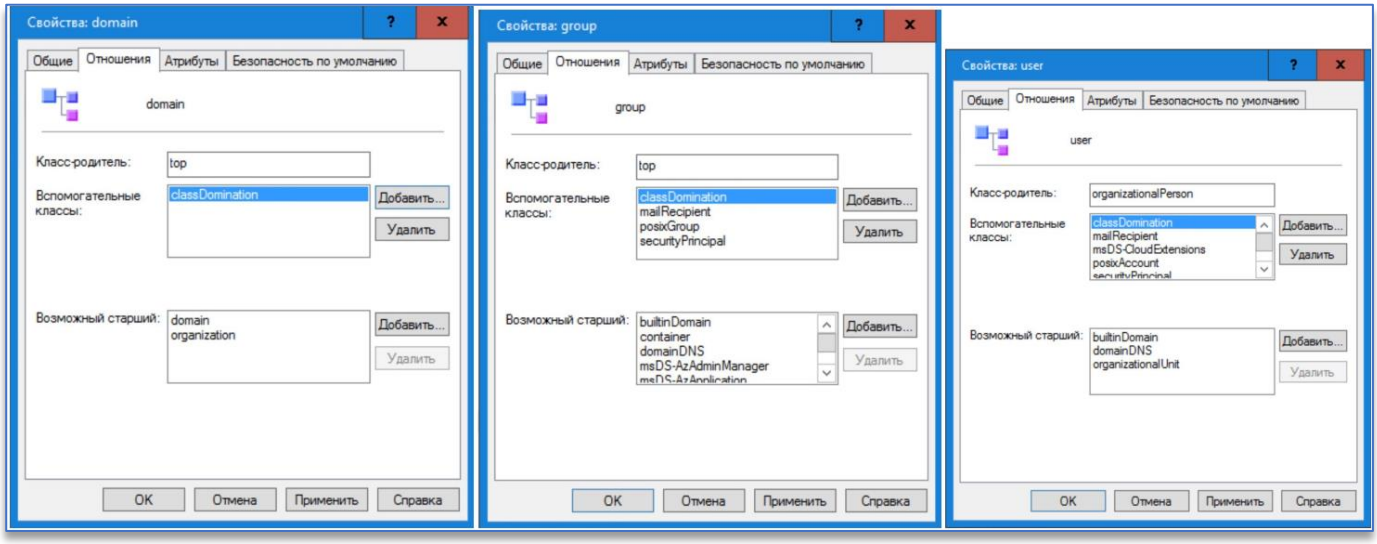



В окне «**Создание нового класса схемы**» необходимо ввести следующие данные:
*Общее имя: classDomination*
*X500-код объекта: 1.2.840.113556.1.8000.2554.60261.35177.16306.19442.40185.2384456.12562999.1.1*
*Тип класса: Особый*

Нажать «**Далее**», затем «**Готово**».
В списке «**Классы**» у классов «**domain**», «**user**» и «**group**»:
1) через ПКМ выбрать «**Свойства**»;

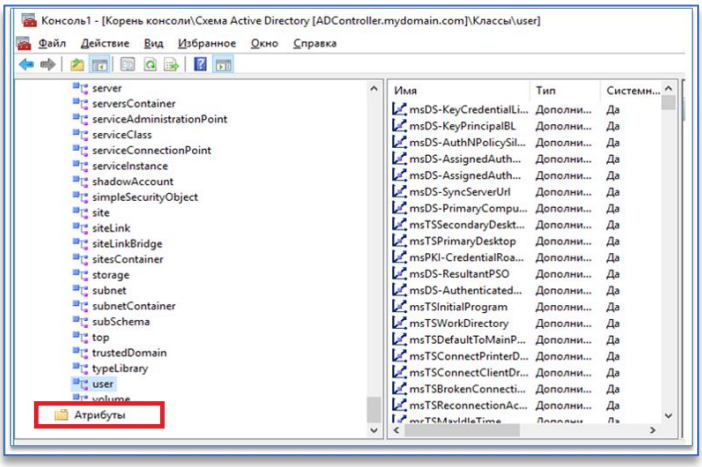


2) на вкладке «**Отношения**» напротив списка «**Вспомогательные классы:**» нажать «**Добавить...**»;
3) выбрать созданный ранее класс «**classDomination**»;
4) нажать **«ОК»**.

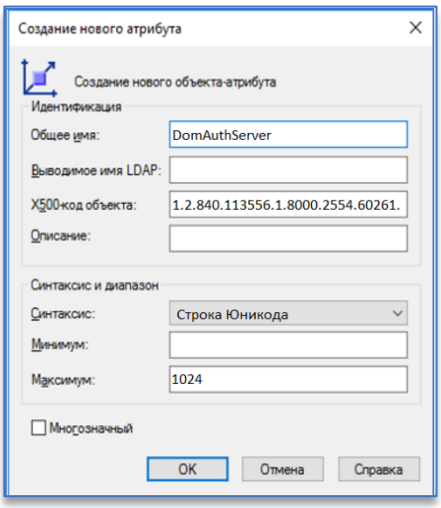



- *Атрибут «**DomAuthServer**».*

Нажать ПКМ по директории «**Атрибуты**», далее выбрать «**Создать атрибут...**».




В окне «**Создание нового атрибута**» ввести следующие данные:
*Общее имя: DomAuthServer*
*X500-код объекта: 1.2.840.113556.1.8000.2554.60261.35177.16306.19442.40185.2384456.12562999.2.1*



*Синтаксис: Строка Юникода*
*Максимум: 1024*
*Многозначный: Нет*

Для сохранения данных нажать на кнопку «**OK**».

- *Атрибут «**DomPermission**».*

Нажать ПКМ по директории «**Атрибуты**», далее выбрать «**Создать атрибут...**».

*Общее имя: DomPermission*
*X500-код объекта: 1.2.840.113556.1.8000.2554.60261.35177.16306.19442.40185.2384456.12562999.2.2*
*Синтаксис: Строка Юникода*
*Максимум: 4096*
*Многозначный: Да*

*! Обязательно нужно поставить галку «**Многозначный**».*
Для сохранения данных нажать на кнопку «**OK**».

- *Атрибут «**DomAnalyticsPermission**».*

Нажать ПКМ по директории «**Атрибуты**», далее выбрать «**Создать атрибут...**».

*Общее имя: DomAnalyticsPermission*
*X500-код объекта: 1.2.840.113556.1.8000.2554.60261.35177.16306.19442.40185.2384456.12562999.2.3*
*Синтаксис: Строка Юникода*
*Максимум: 4096*
*Многозначный: Да*

*! Обязательно нужно поставить галку «**Многозначный**».*
Для сохранения данных нажать на кнопку «**OK**».

- *Атрибут «**DomUseAuth**».*

Нажать ПКМ по директории «**Атрибуты**», далее выбрать «**Создать атрибут...**».

*Общее имя: DomUseAuth*
*X500-код объекта: 1.2.840.113556.1.8000.2554.60261.35177.16306.19442.40185.2384456.12562999.2.4*
*Синтаксис: Строка Юникода*
*Максимум: 1024*
*Многозначный: Нет*

Для сохранения данных нажать на кнопку «**OK**».

- *Атрибут «**DomSubjectProperties**».*

Нажать ПКМ по директории «**Атрибуты**», далее выбрать «**Создать атрибут...**».

*Общее имя: DomSubjectProperties*
*X500-код объекта: 1.2.840.113556.1.8000.2554.60261.35177.16306.19442.40185.2384456.12562999.2.5*
*Синтаксис: Строка Юникода*
*Максимум: 4096*

*Многозначный: Нет*

Для сохранения данных нажать на кнопку «**ОК**».

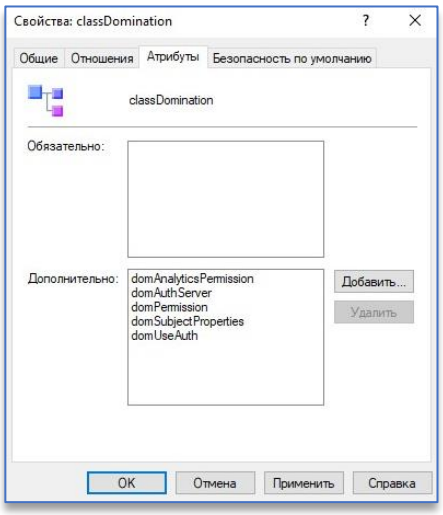
- *Атрибут «**DomProfile**».*

Нажать ПКМ по директории «**Атрибуты**», далее выбрать «**Создать атрибут...**».

*Общее имя: DomProfile*
*X500-код объекта: 1.2.840.113556.1.8000.2554.60261.35177.16306.19442.40185.2384456.12562999.2.6*
*Синтаксис: Строка Юникода*
*Максимум: 1024*
*Многозначный: Нет*

Для сохранения данных нажать на кнопку «**ОК**».

Далее необходимо вернуться в окно «**Консоль1 – Корень консоли**».
В директории «**Классы**» найти созданный класс «**classDomination**». Через ПКМ выбрать «**Свойства**», перейти на вкладку «**Атрибуты**».

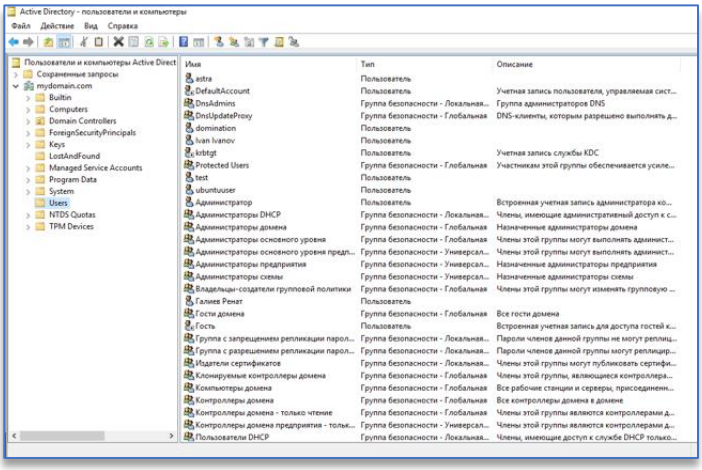



Напротив списка «**Дополнительно:**» нажать «**Добавить...**».

Добавить созданные ранее атрибуты **DomAuthServer, DomAnalyticsPermission, DomPermission, DomUseAuth, DomSubjectProperties, DomProfile**.

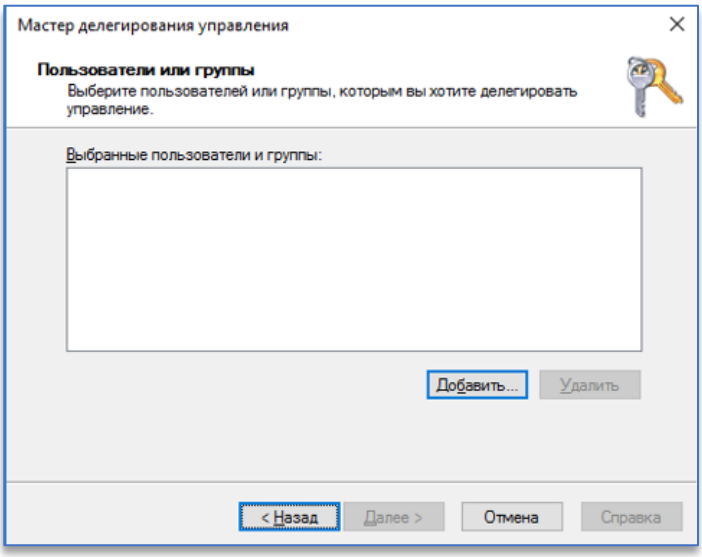
Нажать на кнопку «**ОК**» и **перезагрузить сервер для применения изменений.**

Далее необходимо открыть «**Active Directory – пользователи и компьютеры**».

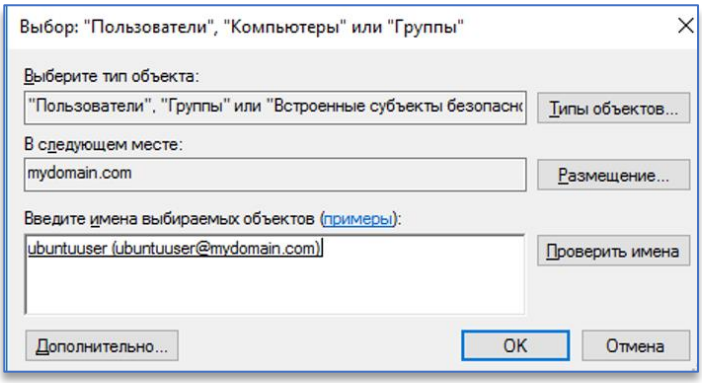


Найти в **домене** директорию «**Users**».

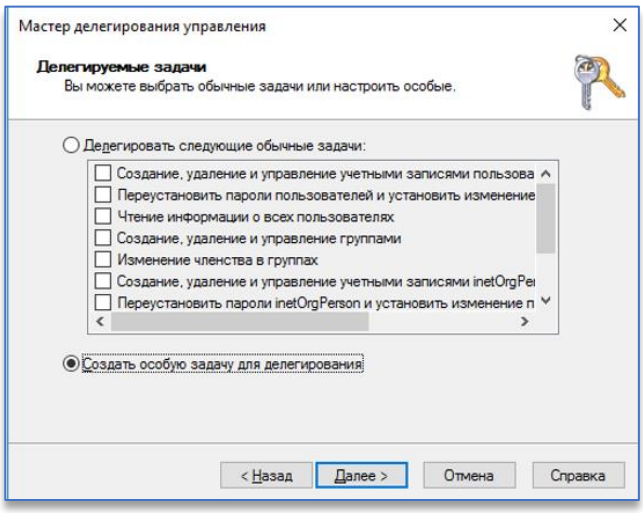
Через ПКМ выбрать «**Делегирование управления»**, в открывшемся окне нажмите «**Добавить...**».



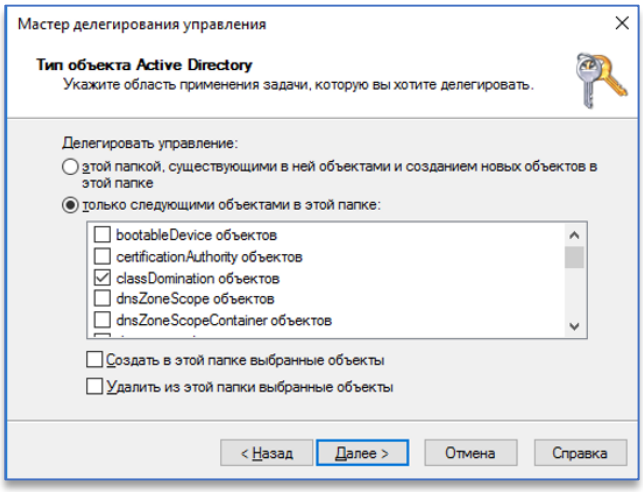

Вписать в поле имя «**Сервисного пользователя**» ЦСУ (если пользователь не создан, то создать пользователя домена; его название может быть произвольным, например: «dominationServiceAccount»). В примере это пользователь «ubuntuuser». Далее нажать «**ОК**».



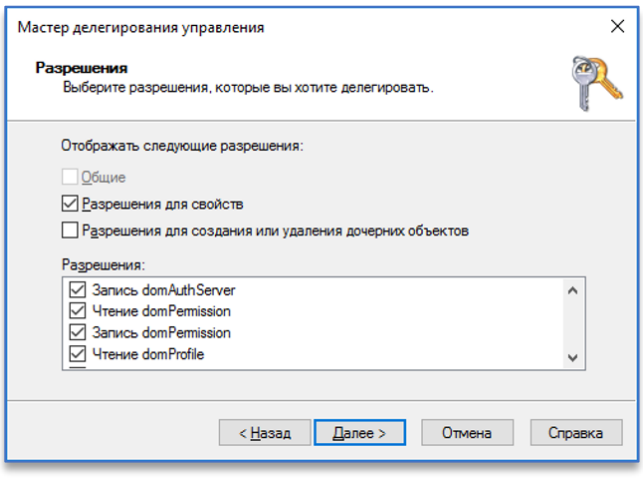
В окне «**Мастер делегирования управления**» в пункте «**Делегируемые задачи**» выбрать «**Создать особую задачу для делегирования**», нажать «**Далее**».




Выбрать пункт «**только следующими объектами в этой папке**» и отметить галочкой класс «**classDomination**». Затем нажать «**Далее**».




В следующем окне нужно отметить галочкой пункт «**Разрешения для свойств**», также установить галочки на «**Чтение**» и «**Запись**» для всех атрибутов. Затем нажать «**Далее**» и «**Готово**».




Таким образом были успешно добавлены атрибуты для работы ЦСУ и создан сервисный пользователь для работы с атрибутами.

## 7.3. Добавление правил в firewall

Чтобы разрешить сетевой доступ к экземпляру PostgreSQL и ЦСУ с других компьютеров, нужно создать правила в файрволе. Создать правила можно через «командную строку».

Для этого нужно запустить командную строку от имени администратора и ввести команды:

***netsh advfirewall firewall add rule name="Postgre Port" dir=in action=allow protocol=TCP localport=5432***

***netsh advfirewall firewall add rule name="ЦСУ Port" dir=in action=allow protocol=TCP localport=8000***

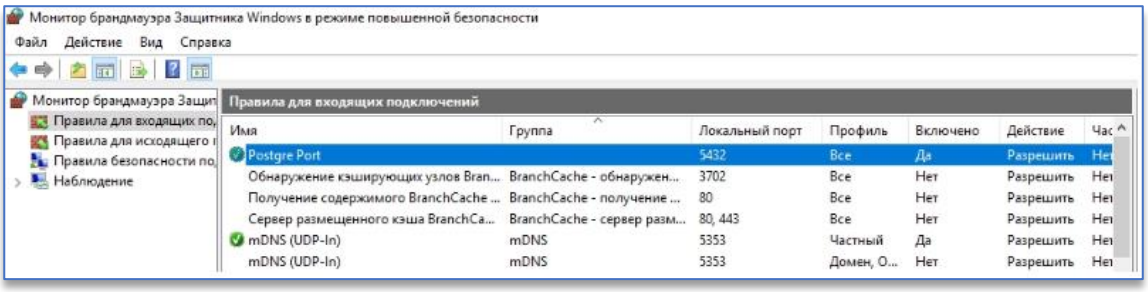
***netsh advfirewall firewall add rule name="ЦСУ Port" dir=in action=allow protocol=TCP localport=8001***

Где:

rule name – имя правила,

localport – разрешенный порт.

После применения команд в брандмауэре Windows появятся новые разрешающие правила для портов.




## 7.4. Настройка конфигурационного файла appsettings.json

Файл **appsettings.json** находится в корне папки с программой.

**Секция для настройки номера порта службы ЦСУ.**

По умолчанию указан порт 8001.

```
"Kestrel": {
  "EndPoints": {
   "Http": {
    "Url": "http://*:8001"
   }
  }
 }
```

**Секция для настройки номера порта, по которому видеосерверы Domination будут подключаться к службе ЦСУ.**

По умолчанию указан порт 8000, в большинстве случаев его можно оставить неизменным.

```
"DominationListener": {
  "Address": "*",
  "Port": 8000
 }
```

**Секция для настройки логина и пароля WEB интерфейса администратора службы ЦСУ.**

```
"Admin": {
  "Name": "admin",
  "Password": " admin "
 }
```

**Секция для настройки параметров подключения к домену предприятия.**

В инструкции используются следующие псевдонимы:

- cd.domain.com – контроллер домена,
- ServiceUser – пользователь с правами редактирования атрибутов в домене,
- ServiceUserPassword – пароль для подключения ServiceUser.

```
"LdapConnection": {
   "Address": "cd.domain.com",
   "Port": 389,
   "Name": "ServiceUser",
   "Password": "ServiceUserPassword",
   "Domain": "DOMAIN",
   "RootDistinguishedName": "DC=domain,DC=com",
   "RootGroup": "OfficeUsers"
 }
```

**Секция для настройки провайдера данных.**

Для работы с ролями и пользователями через Active Directory нужно указать для поля Users значение **AD**.

Для работы через базу данных PostgreSQL указать **DB**.

Поле Servers изменять не требуется.

UserCacheUpdateInterval отвечает за интервал обновления (в минутах) списка пользователей, ролей из Active Directory.

```
"StorageScheme": {
   "Users": "AD",
   "Servers": "DB",
   "UsersCacheUpdateInterval": "10"
 }
```

**Секция настройки параметров подключения к базе данных.**

```
"DataBaseConnection": {
   "DataBaseName": "ENTERPRISE_STORAGE",
   "User": "",
   "Password": "",
   "Port": 5432,
   "Host": "",
   "Logging": "false",
   "EnableSensitiveDataLogging": "false"
 }
```

Если база данных на сервер установлена впервые, то нужно задать следующие значения параметров:

- User = «postgres»,
- Password = пароль, который был указан при установке,
- Port = номер порта, который был указан при установке,
- Host = ip-адрес компьютера, на который была установлена СУБД.

Если база данных уже была установлена, то необходимо использовать имеющиеся учётные данные.

**Секция для настройки папки хранения профилей для видеоклиента.**
По умолчанию сохраняется в корень программы.

```
"ProfilesStorage": {
  "Folder": ""
 }
```

**Секция для настройки уровня логирования сообщений.**

```
"Serilog": {
  "Using": [ "Serilog.Sinks.Console" ],
  "MinimumLevel": {
   "Default": "Debug",
   "Override": {
    "Microsoft": "Warning",
    "System": "Warning"
   }
  },
  "WriteTo": [
   { "Name": "Console" }
  ],
  "Enrich": [ "FromLogContext" ]
 }
```

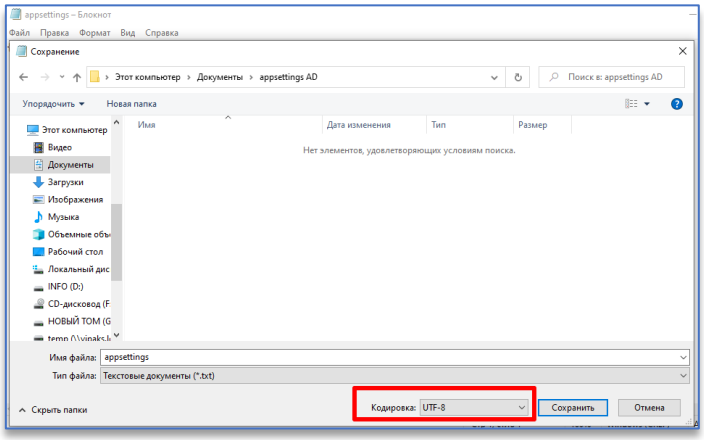
**Секция настройки сервиса Elastic.**

```
"ElasticConfiguration": {
  "Uri": "http://localhost:9200"
 }
```

**Секция настройки сервиса Swagger.**

```
"SwaggerConfiguration": {
  "UseSwagger": true
 }
```

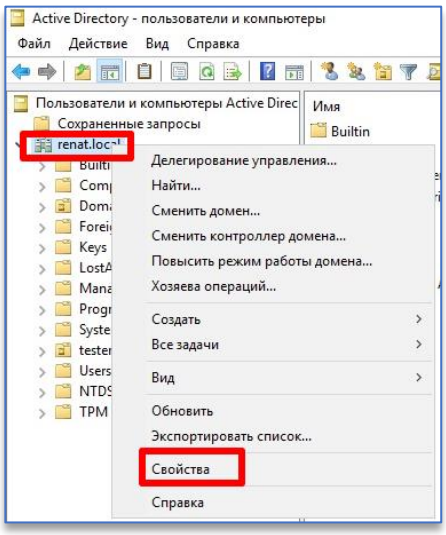
Файл конфигурации **appsettings.json** необходимо сохранять в кодировке UTF-8.



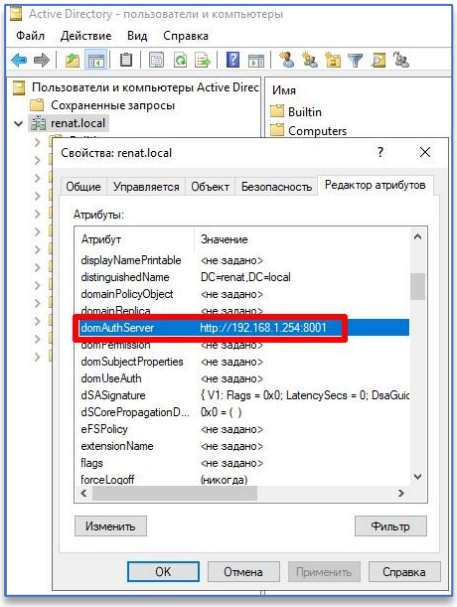
## 7.5. Настройка автоматического входа в Domination Client через Active Directory

Для включения автоматического входа в Domination Client с помощью учетной записи Active Directory необходимо выполнить следующее:

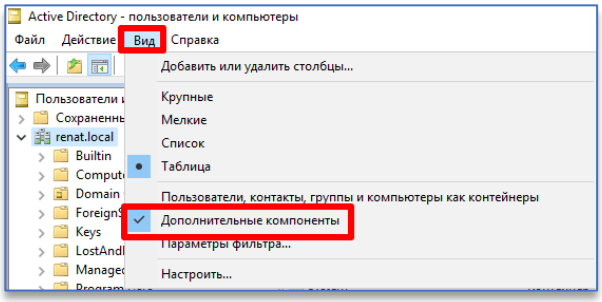
1. Зайти в «**Active Directory – пользователи и компьютеры**». Через ПКМ по названию домена выбрать «**Свойства**».



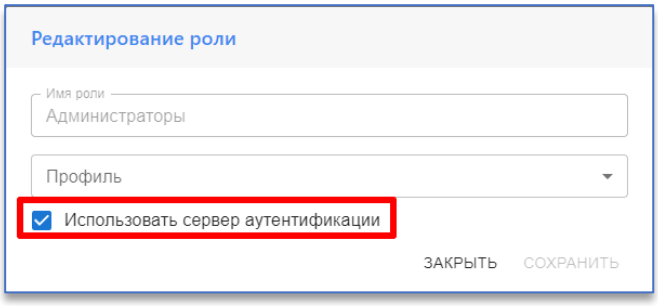

2. Во вкладке «**Редактор атрибутов**» найти атрибут «**domAuthServer**» и прописать IP-адрес ЦСУ.




Если в свойствах нет **«Редактора атрибутов»**, то нужно выбрать **«Вид»** – **«Дополнительные компоненты»**



3. В ЦСУ навести курсор на нужного пользователя или роль и нажать  . Выбрать «**Изменить**» или «**Редактировать роль**» и поставить галочку в чекбоксе напротив «**Использовать сервер аутентификации**».




Добавление пользователя и роли в ЦСУ производится через Active Directory.

## 8. Установка программного обеспечения на Windows

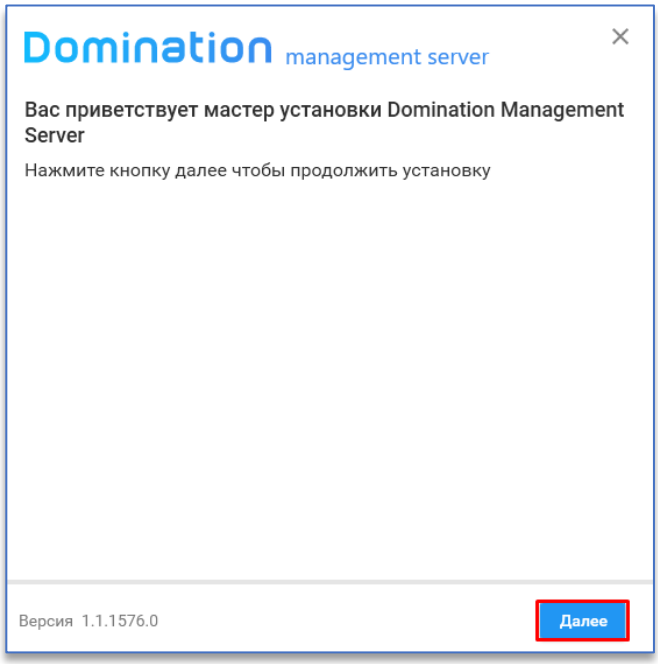
Для установки ЦСУ необходимо:

1. Скачать дистрибутив по ссылке:

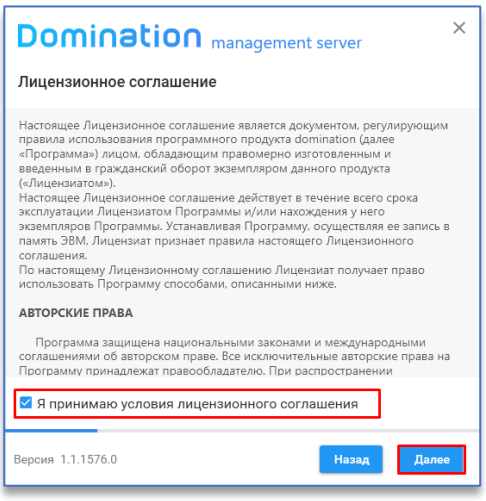
https://domination.one/upload/domination/DCCS_Windows.zip

2. Распаковать полученный архив.
3. Запустить файл установки **Domination Management Server.**

Откроется окно мастера установки, для продолжения установки необходимо нажать «**Далее**».

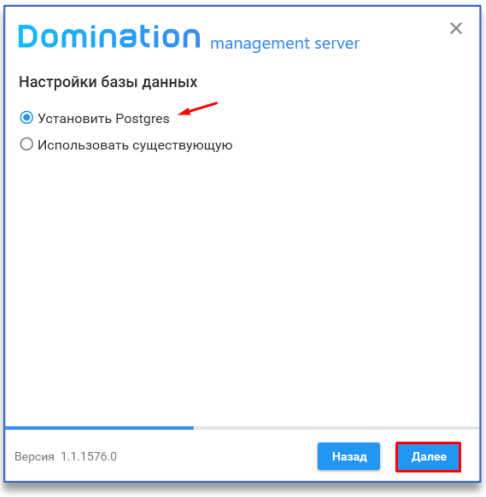


После этого потребуется ознакомиться и принять условия лицензионного соглашения, потом нажать «**Далее**».

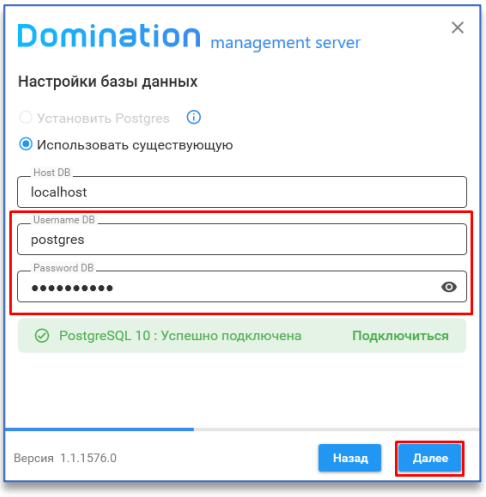



Дальнейшие действия по установке будут зависеть от того, установлена или нет база данных PostgreSQL на компьютере.

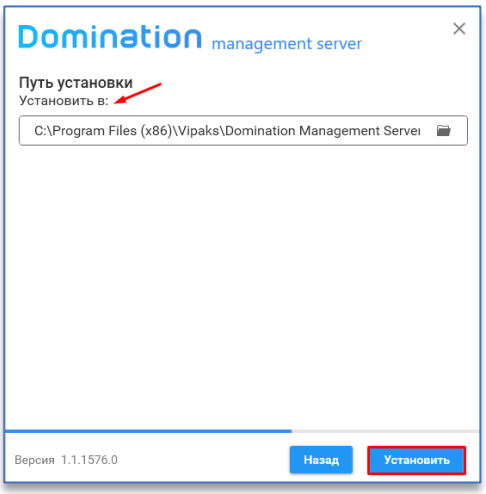
В случае если база данных Postgresql **не установлена** на компьютере, необходимо выбрать пункт «**Установить Postgres**» и нажать «**Далее**».



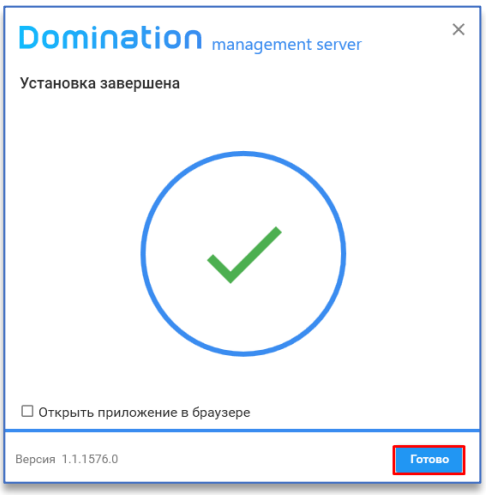

В случае если база данных Postgresql **уже установлена** на компьютере, необходимо выбрать пункт «**Использовать существующую**», ввести учётные данные и нажать «**Далее**».

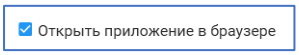


Далее нужно указать путь установки и нажать на кнопку «**Установить**».




По завершению установки в окне установки появится сообщение «Установка завершена». Для закрытия окна нужно нажать на кнопку «**Готово**».




При необходимости можно установить галочку в поле 

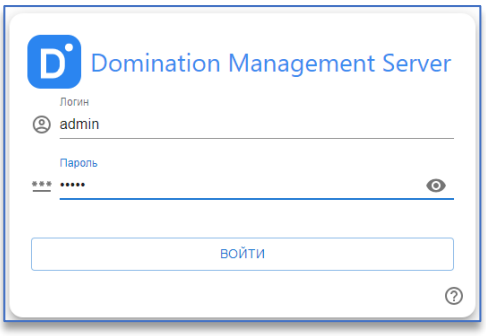
. В этом случае панель администратора ЦСУ откроется в web-браузере.

## 9. Вход в панель администратора

Для входа в панель администратора ЦСУ необходимо открыть на устройстве web-браузер и в поле адреса ввести http://localhost:8001/.

Стандартный порт для подключения – 8001.

При успешном соединении откроется меню авторизации «Domination Management Server».



В окне авторизации необходимо указать логин и пароль и нажать кнопку «**Войти**».

По умолчанию логин и пароль: admin/admin.

Чтобы поменять логин и/или пароль нужно внести изменение в конфигурационный файл (см. раздел «Настройка конфигурационного файла appsettings.json»).

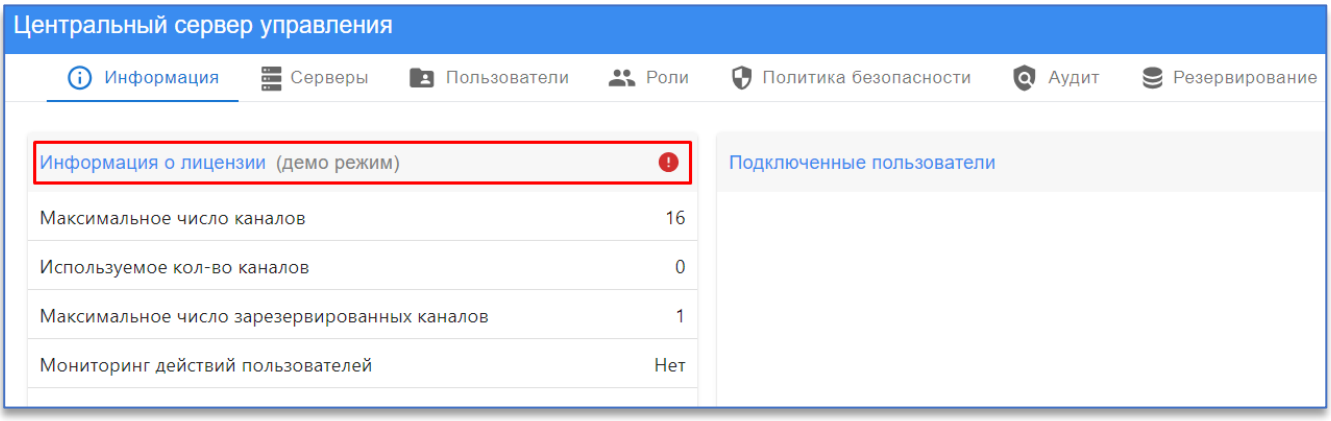
Кнопка  в строке, где указывается пароль, служит для просмотра введённого пароля.

После авторизации откроется стартовая страница – панель администратора ЦСУ.

## 10. Вкладка «Информация»

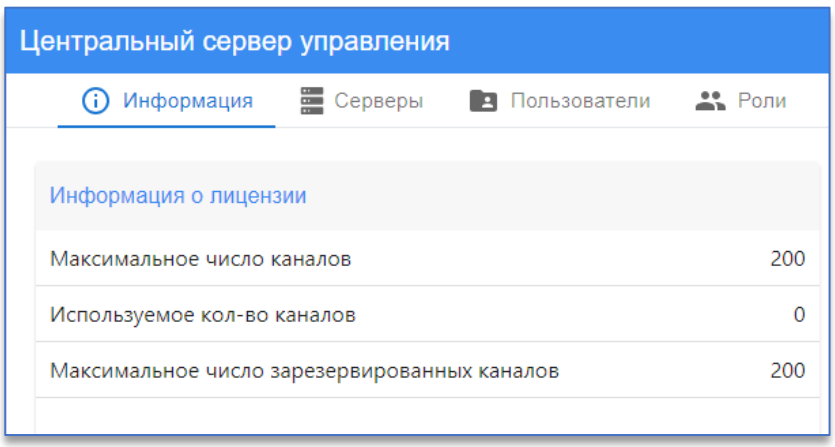
На стартовой странице ЦСУ указана информация о лицензии и подключенных пользователях.

Если аппаратного USB – ключа защиты нет, то ЦСУ откроется в демо-режиме.

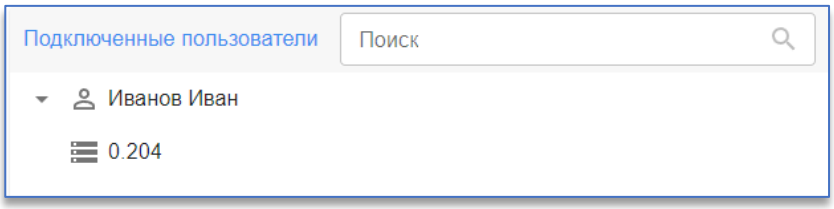



Необходимо вставить аппаратный USB-ключ защиты в USB-порт компьютера.

После успешной инициализации USB-ключа защиты в разделе «**Информация о лицензии**» отобразится максимальное число каналов, а также те возможности, которые будут доступны в рамках приобретённой лицензии.




В разделе **«Подключенные пользователи»** отображаются те пользователи, которые в данный момент подключены к серверам.



# 11. Вкладка «Серверы»

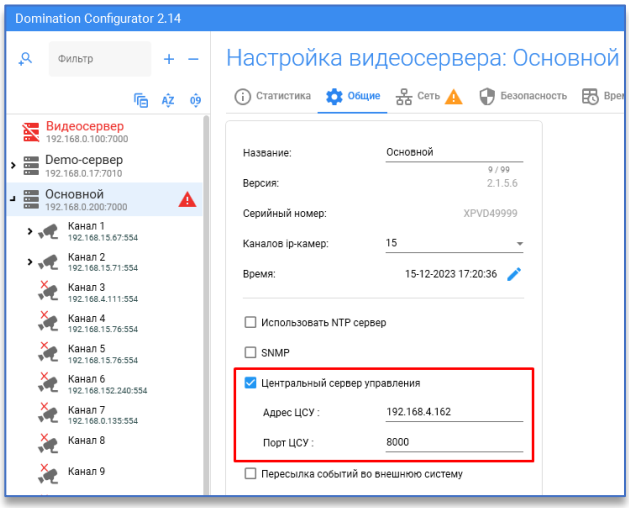
На вкладке **«Серверы»** можно управлять видеосерверами и серверами аналитики.

## 11.1. Вкладка «Видеосерверы»

Даная вкладка отображает входящие запросы на подключение и информацию о подключенных видеосерверах.

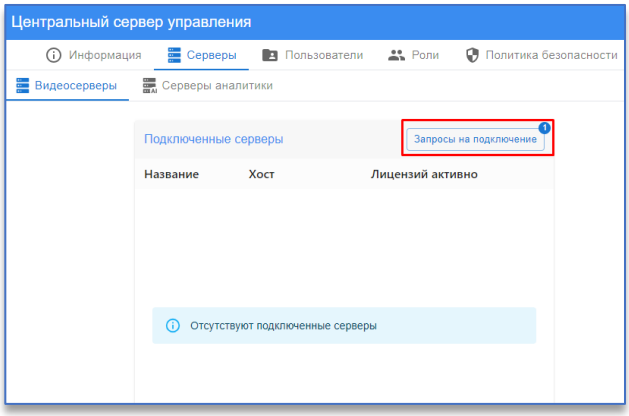
Для добавления видеосервера в ЦСУ нужно сначала перейти в Конфигуратор видеосервера и выполнить его настройку:

1) добавить или выбрать видеосервер, работа с которым планируется через ЦСУ;
2) на вкладке «Общие» установить галочку в разделе «Центральный сервер управления» и прописать в поле «Адрес ЦСУ» IP-адрес того сервера, где запущен ЦСУ;
3) нажать на кнопку «Сохранить» в правом нижнем углу.

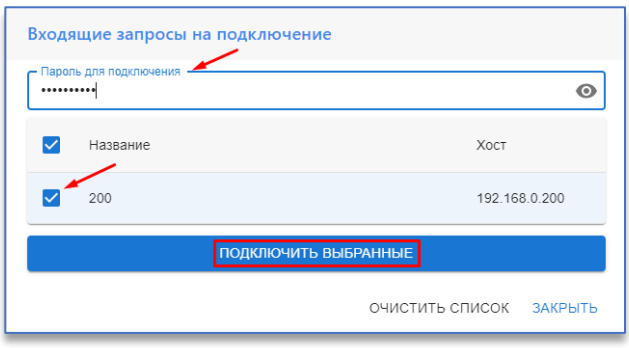



После этого в ЦСУ придёт запрос на подключение выбранного видеосервера.

Нужно перейти в ЦСУ в раздел «**Видеосерверы**» и нажать на кнопку «**Запросы на подключение**».

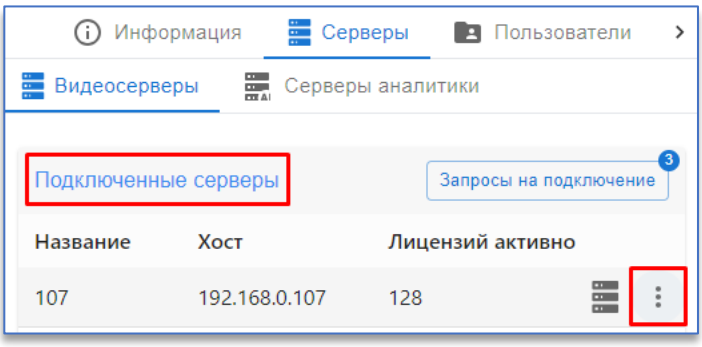



Далее нужно выбрать в списке видеосервер, ввести пароль для подключения и нажать на кнопку «**Подключить выбранные**».

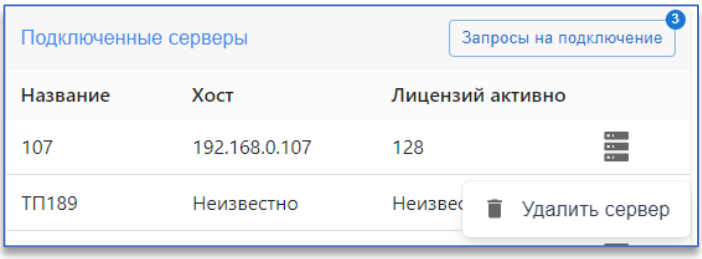


Кнопка  в строке, где указывается пароль, служит для просмотра введённого пароля.

После подключения видеосервер отобразится в разделе «Подключенные серверы».



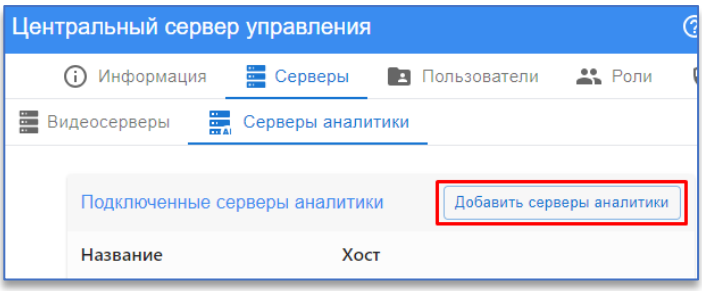

Чтобы удалить сервер нужно навести курсор мыши на нужный видеосервер и нажмите на кнопку  . В отрывшемся меню выбрать «**Удалить сервер**».



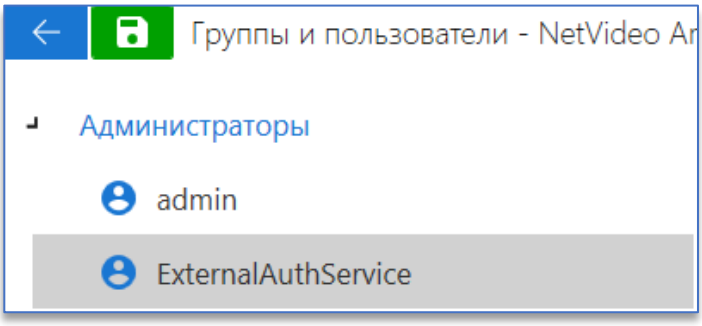

## 11.2. Вкладка «Серверы аналитики»

Данная вкладка содержит информацию о подключенных серверах аналитики.

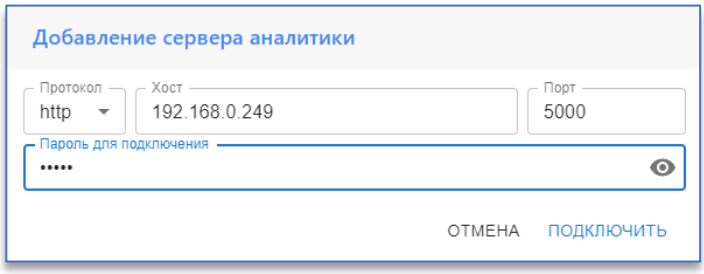
Для подключения сервера аналитики нужно нажать на кнопку **«Добавить сервер аналитики»**.




Для подключения сервера аналитики в ЦСУ требуется создать пользователя **«ExternalAuthService»** с любым паролем в Конфигураторе аналитики в разделе **«Пользователи»**.

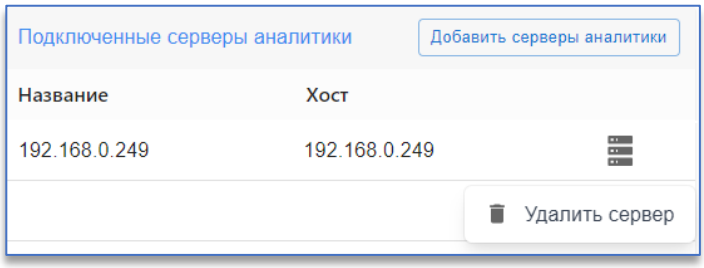


В ЦСУ в открывшемся окне нужно выбрать протокол, ввести IP-адрес, порт сервера аналитики и пароль от пользователя **«ExternalAuthService»**.

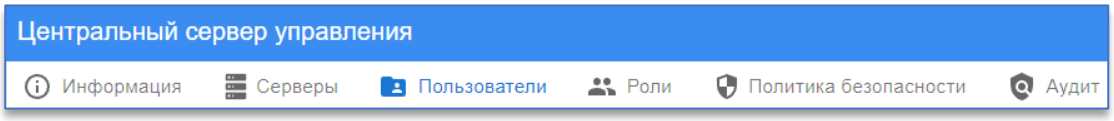



Кнопка  в строке, где указывается пароль, служит для просмотра введённого пароля.

Чтобы удалить сервер нужно навести курсор мыши на нужный сервер аналитики и нажмите на кнопку 




## 12. Пользователи

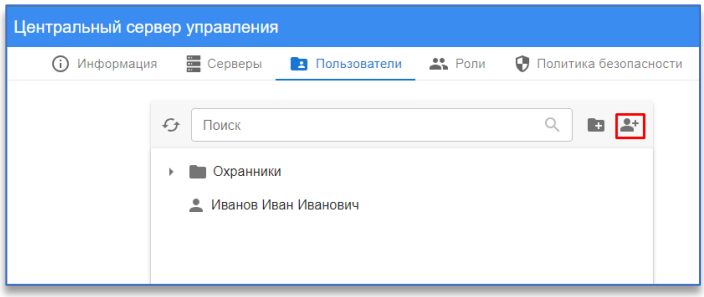



Вкладка «**Пользователи**» предназначена для управления пользователями и группами пользователей, заведённых в ЦСУ, а именно:

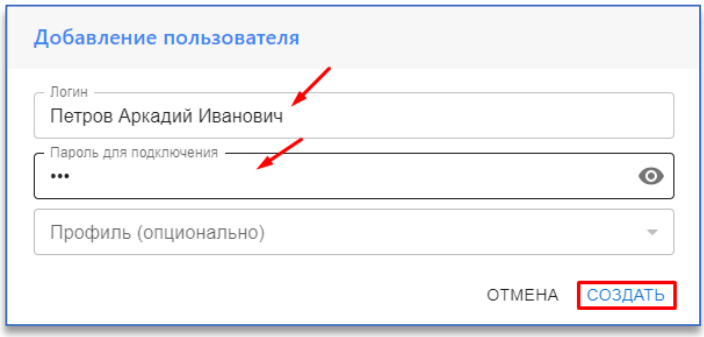
- создания нового пользователя;
- создания группы пользователей;
- распределения пользователей по группам;
- редактирования данных пользователей;
- редактирования данных групп пользователей;
- удаления пользователей;
- удаления групп пользователей.

При использовании Active Directory отображаются пользователи, занесённые в службу каталогов. Добавление и редактирование данных у таких пользователей через ЦСУ невозможно.

Чтобы добавить нового пользователя, нажмите на кнопку  .

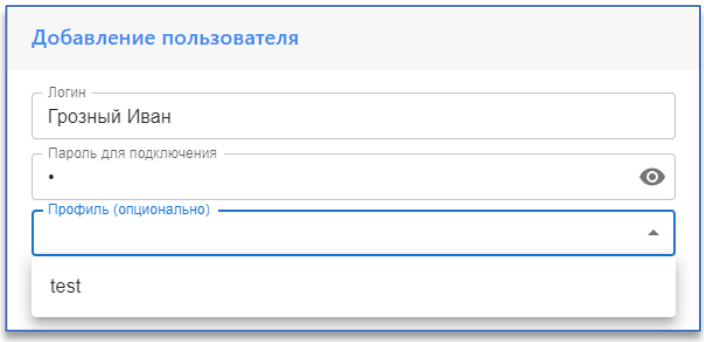


Откроется окно добавления нового пользователя. Необходимо задать логин и пароль пользователя, после чего нажать кнопку «**Создать**».



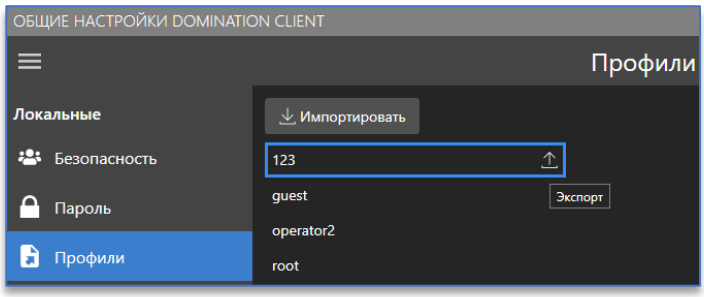

Кнопка  в строке, где указывается пароль, служит для просмотра введённого пароля.

В поле «**Профиль**» можно указать заранее настроенный профиль, который будет использоваться при открытии клиента Domination (Domination Client).

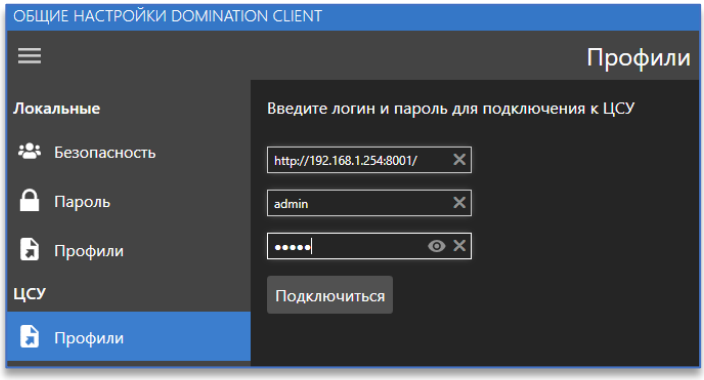



Чтобы экспортировать настроенный профиль в ЦСУ, необходимо:

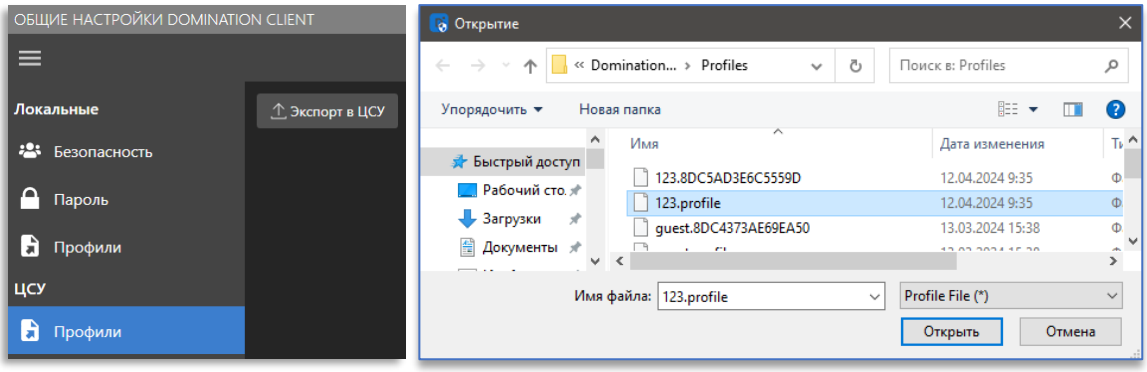
1. Зайти в «**Общие настройки**» Domination Client, выбрать «**Профили**», выделить нужный профиль пользователя и нажать на кнопку «**Экспорт**».



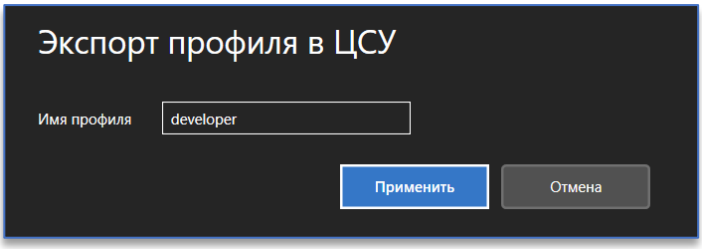

2. Далее зайти в раздел «**ЦСУ – Профили**».
3. Ввести адрес, порт, логин и пароль ЦСУ. Нажать «**Подключиться**».



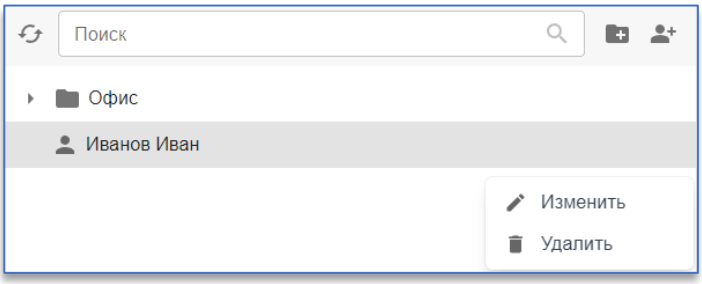
4. После успешного подключения к ЦСУ нажать на кнопку **«Экспорт в ЦСУ»**, выбрать нужный профиль и нажать «**Открыть**».



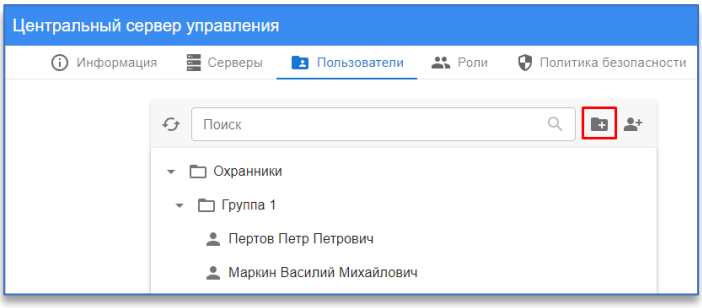

5. При необходимости можно изменить имя профиля и нажать «**Применить**».



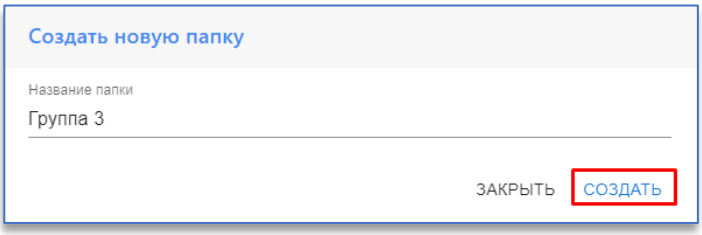

Чтобы «**Изменить**» или «**Удалить**» пользователя, нужно навести курсор на нужного пользователя и нажать  .



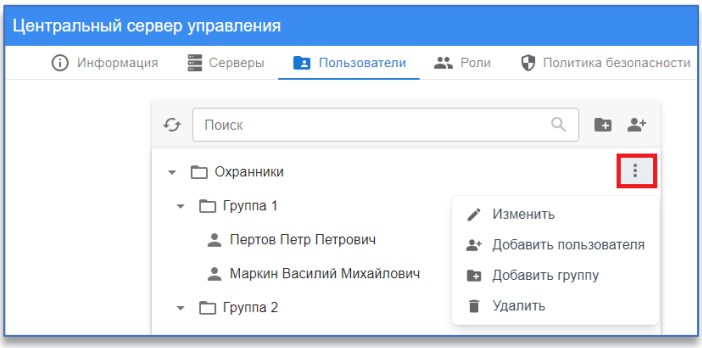

Чтобы создать «**Группу**», нужно нажать на кнопку  .




Откроется окно создания новой группы, в нём нужно указать название группы и нажать на кнопку **«Создать»**.



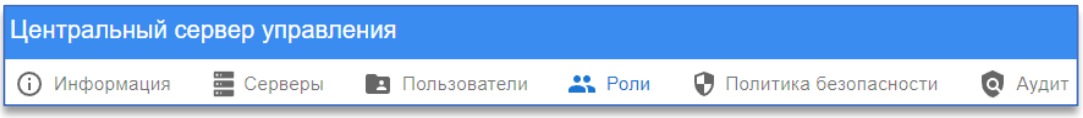
Чтобы «**Изменить**» название группы, «**Добавить пользователя**» в группу, «**Добавить группу**» и «**Удалить**» группу, нужно навести курсор мыши на нужную группу и нажать  , откроется меню, из которого необходимо выбрать нужное действие.




Переместить пользователя из одной группы в другую можно путем перетаскивания. Для этого необходимо выбрать нужного пользователя, зажать его имя левой кнопкой мыши и перетащить в нужную группу (при этом наводить курсор мыши нужно на название группы, в которую необходимо переместить пользователя).

## 13. Роли

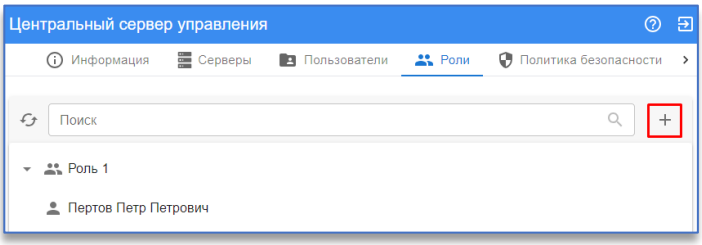
Роли позволяют группировать пользователей по общей принадлежности к одной категории для более удобной и единовременной настройки политики безопасности выбранных групп.



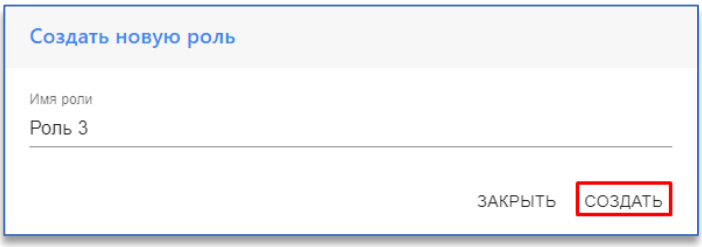

На вкладке **«Роли»** можно управлять ролями пользователей:

- создавать новую роль;
- назначать пользователей на роли;
- редактировать роли;
- редактировать локальную политики безопасности;
- удалять роли.

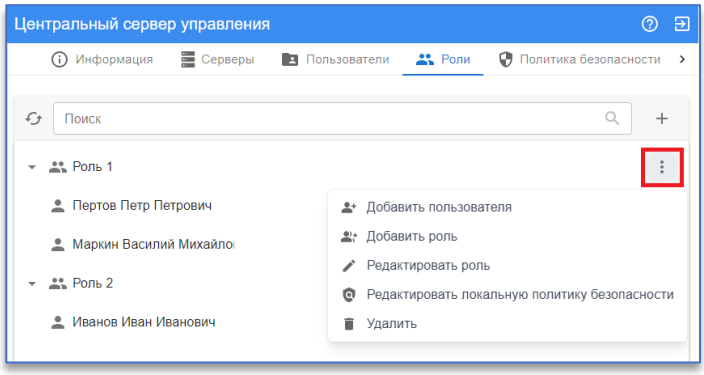
Чтобы добавить новую роль, нужно нажать на кнопку  .



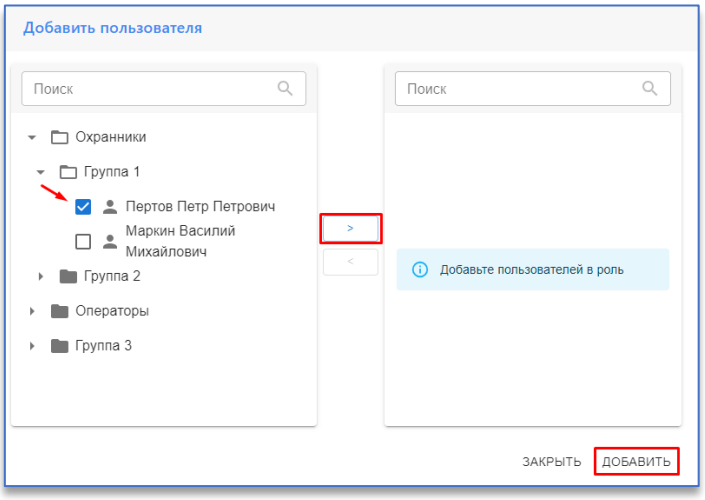

Откроется окно создания новой роли. Необходимо указать имя роли и нажать на кнопку «**Создать**».



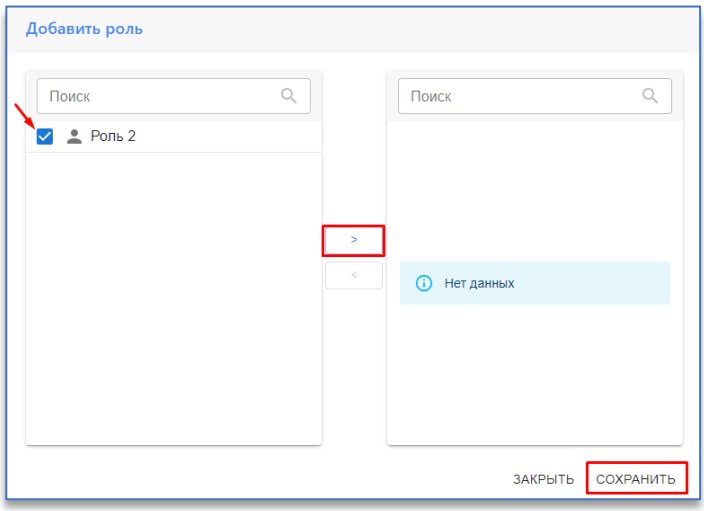
Чтобы «**Добавить пользователя**», «**Добавить роль**», «**Редактировать роль**», «**Редактировать локальную политику безопасности**» и «**Удалить**» роль, требуется навести курсором мыши на нужную роль и нажать  , откроется меню, из которого необходимо выбрать нужное действие.




Чтобы добавить пользователя в роль, нужно нажать «**Добавить пользователя**», выбрать пользователя  и переместить его в правую колонку кнопкой  , после чего нажать кнопку «**Добавить**».

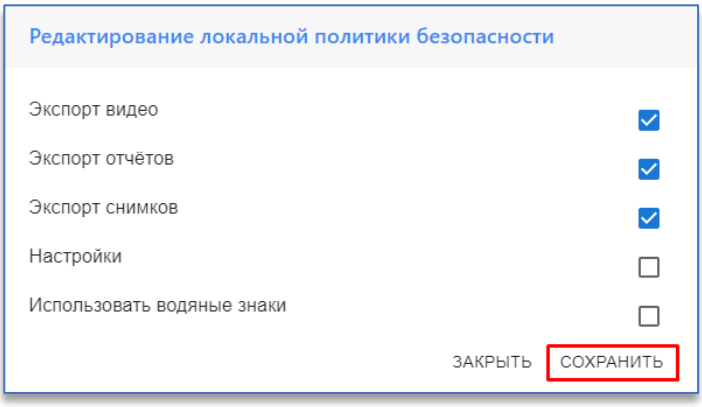



Чтобы добавить роль в роль нужно нажать «**Добавить роль**», выбрать роль  и переместить её в правую колонку кнопкой  , после чего нажать кнопку «**Сохранить**».



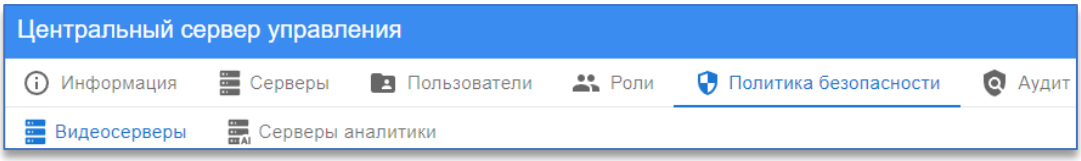
Редактирование локальной политики безопасности относится к правам роли пользователя в клиенте Domination («Domination Client»).

Чтобы настроить политику безопасности (права) у роли, необходимо нажать «**Редактировать локальную политику безопасности**», выбрать нужные настройки  и нажать на кнопку «**Сохранить**».




## 14. Политика безопасности

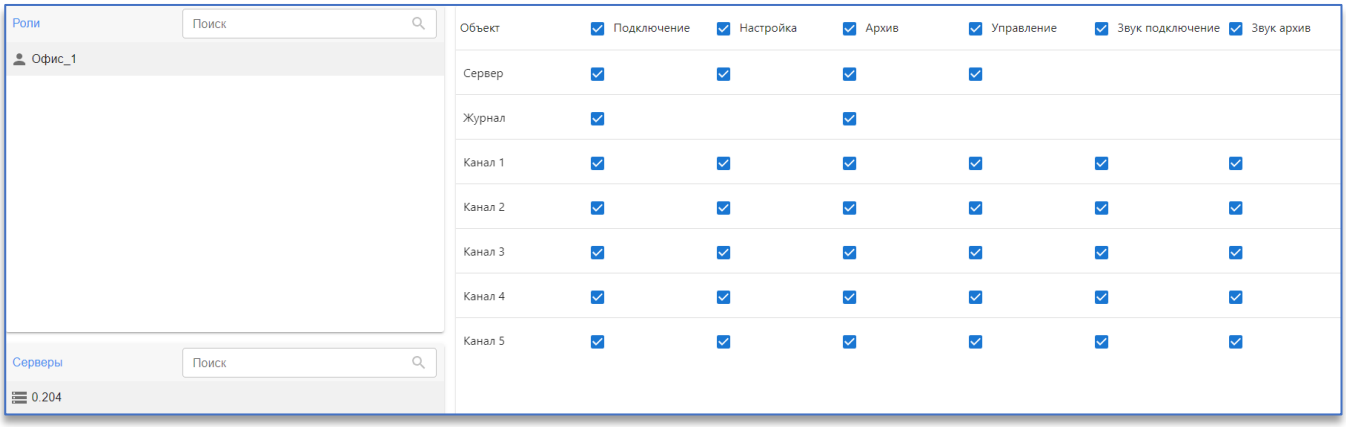
На вкладке «**Политика безопасности**» можно настроить доступ пользователей, которые входят в определённую роль, к различным функциям видеосервера и сервера аналитики.



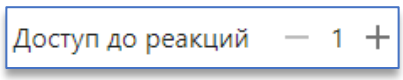

### 14.1. Политика безопасности видеосерверов

Чтобы предоставить/убрать доступ роли до нужного ресурса, необходимо:

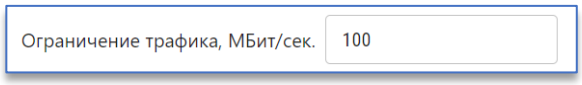
1) выбрать роль;
2) выбрать видеосервер;
3) поставить/снять соответствующую галочку в необходимом пункте.




Для настройки «**Доступа до реакции**» нужно указать уровень доступа для роли. Если уровень у роли ниже, чем выставленный уровень в событии, то запустить реакцию данные пользователи не смогут.



Для ограничения скорости трафика для данной роли требуется указать ограничение в поле «**Ограничение трафика**». Ограничение трафика начинает действовать для вновь установленных соединений.




## 14.2. Политика безопасности серверов аналитики

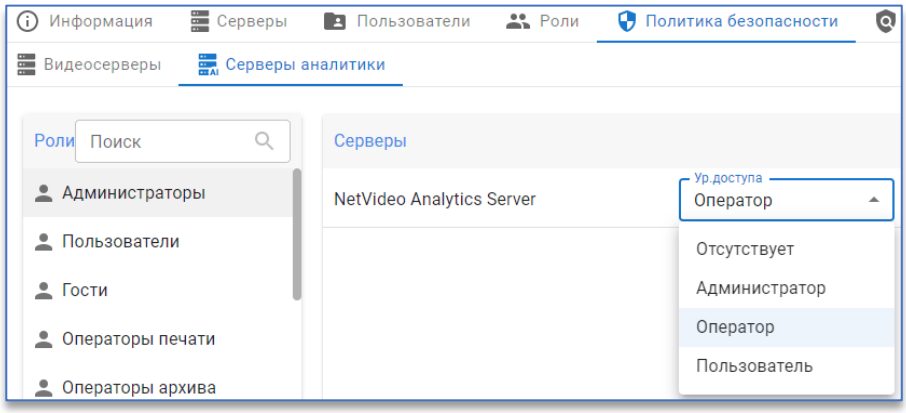
Роль, обладающая уровнем доступа **«Администратор»**, имеет право:

1) подключаться к серверу аналитики для его настройки;
2) получать и редактировать события аналитики через Domination Client;
3) добавлять автомобили и персоны в базу.

Роль, обладающая уровнем доступа **«Оператор»**, имеет право:

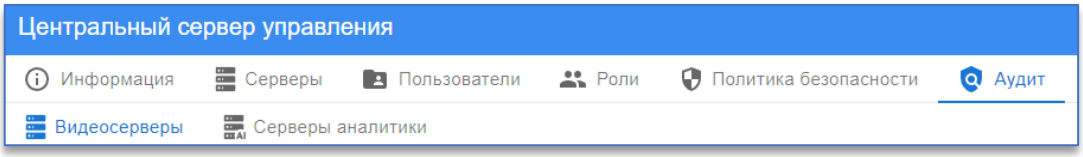
1) получать и редактировать события аналитики через Domination Client;
2) добавлять автомобили и персоны в базу.

Роль, обладающая уровнем доступа **«Пользователь»**, имеет право только подключаться к серверу аналитики для получений событий в клиенте Domination.




# 15. Аудит

Каждый пользователь может обладать несколькими ролями. На вкладке **«Аудит»** можно проверить, какими ролями обладает пользовать и какие итоговые права он имеет.

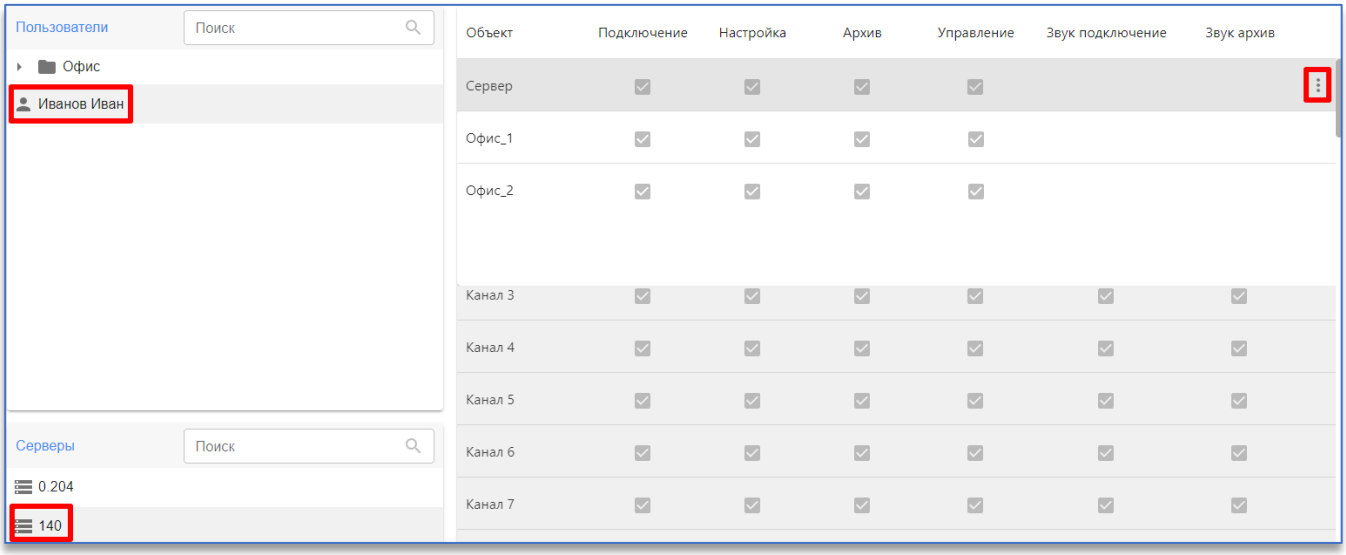



## 15.1. Аудит видеосервера

Чтобы посмотреть, какими правами обладает пользователь, нужно выбрать:

1) пользователя,
2) видеосервер.

В результате будет отображена сводная таблица, которая покажет права пользователя. В таблице будут отображены данные с названием сервера или канала и правами пользователя (подключение, настройка, архив, управление, звук подключение, звук архив).

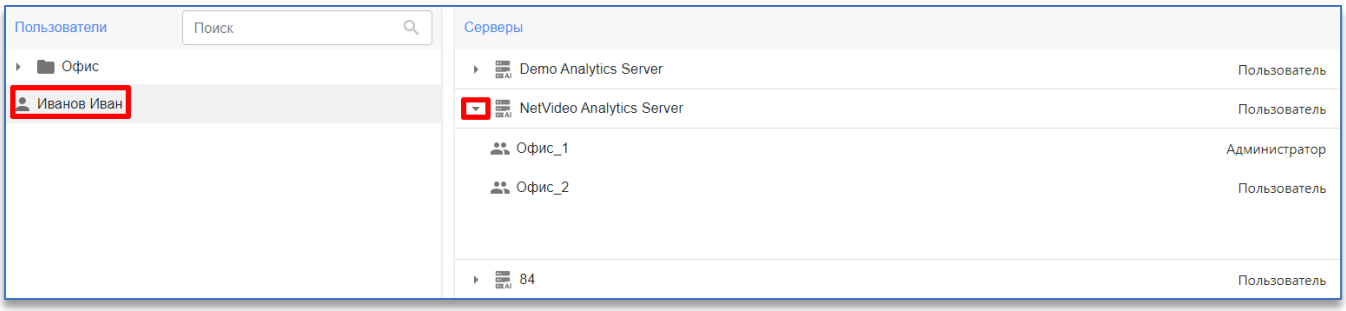



Чтобы проверить, в какие роли входит пользователь, нужно навести курсор мыши на нужный сервер/канал и нажать на кнопку «**Зависимость ролей**»  .

Рядом с названием разделов «Пользователи» и «Серверы» доступно окно **поиска**. При введении названия или его части данные будут отсортированы, регистр букв при вводе не учитывается.

### 15.2. Аудит серверов аналитики

Чтобы посмотреть, какими правами обладает пользователь на конкретном сервере аналитики, нужно выбрать пользователя и развернуть информацию по интересующему серверу аналитики с помощью кнопки  .




Если у пользователя несколько уровней доступа, то в приоритете будет тот уровень, что выше.

Рядом с названием раздела «Пользователи» доступно окно **поиска**. При введении названия или его части данные будут отсортированы, регистр букв при вводе не учитывается.

## 16. Логирование действий пользователей

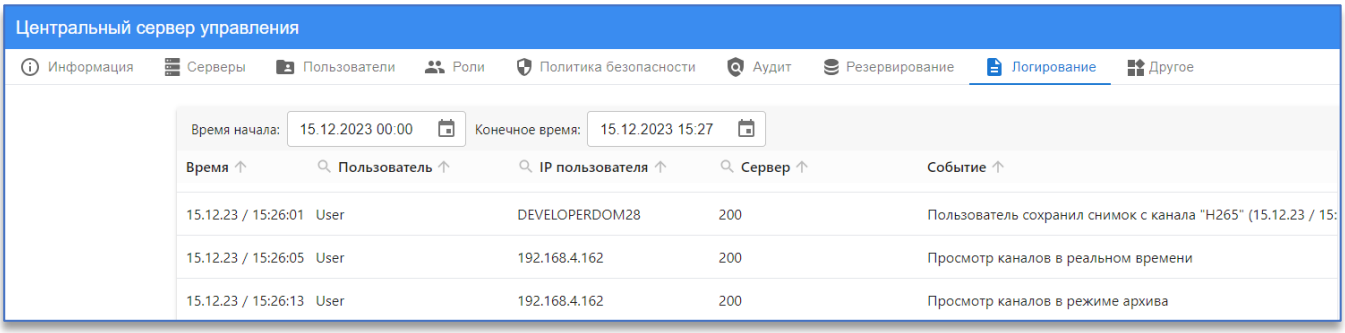
### 16.1. Описание раздела «Логирование»

Вкладка **«Логирование»** позволяет осуществлять мониторинг взаимодействия пользователей с видеосервером, позволяет узнать кем и когда вносились какие-либо изменения. Журнал содержит в себе следующую информацию:

- время взаимодействия;
- какой пользователь осуществлял действие;
- IP-адрес пользователя, совершившего действие;
- с каким сервером взаимодействовал пользователь;
- тип события.

Список возможных действий пользователя:

- подключение к серверу или видеосерверу, отключение аналитики;
- просмотр и/или закрытие камеры, учитывая вывод звука (как в режиме реального времени, так и в архиве);
- снимок изображения камеры;
- экспорт видео, включая звук;
- управление PTZ камерой;
- замыкание/размыкание контакта IP-устройства;
- запуск макросов по клавише;
- редактирование событий аналитики;
- поиск событий/запуск отчёта (аналитики/системных событий);
- изменение настроек клиента;
- открытие/закрытие программы.



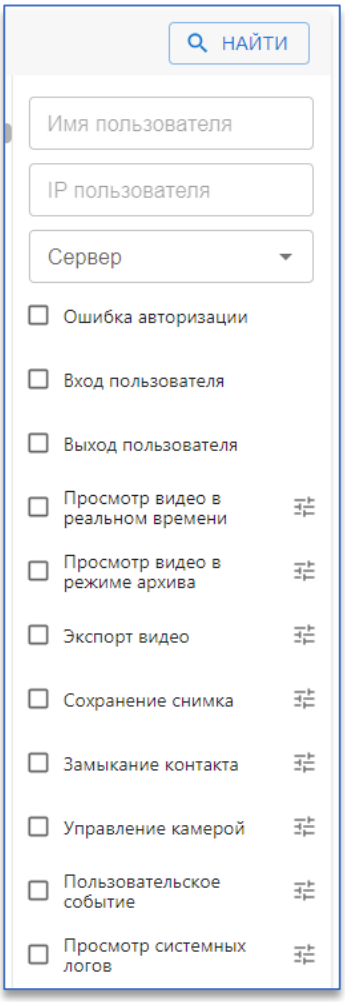

## 16.2. Фильтрация журнала

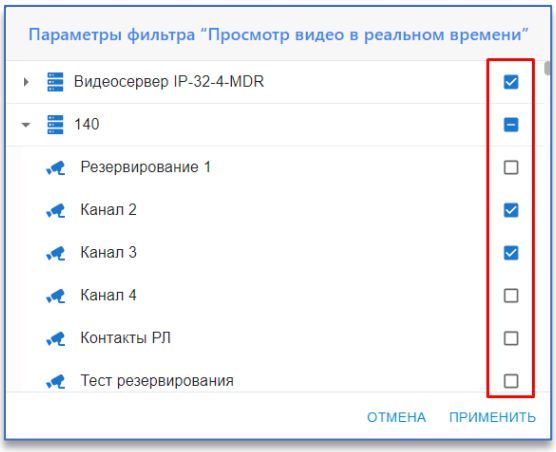
С помощью фильтров можно выгрузить информацию по определенным действиям за интересующий промежуток времени.

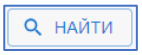
Есть возможность отфильтровать список событий по следующим характеристикам:

- имя пользователя,
- IP-адрес пользователя,
- сервер,
- события.

Также для некоторых событий существует возможность дополнительной фильтрации по серверу/каналу, для этого необходимо нажать на кнопку  рядом с интересующим событием, после чего откроется окно с дополнительными фильтрами. В окне можно выбрать один или несколько серверов/каналов для фильтрации, отметив их в списке.



После указания параметров фильтрации необходимо нажать кнопку 

.

Дополнительно в каждой колонке с информацией в строке заголовков доступны кнопки **сортировки** значений по возрастанию и убыванию  .

Также в колонках «Пользователь», «IP пользователя» и «Сервер» доступна функция **поиска** по введённому значению. Для этого нужно нажать на кнопку  в строке заголовков и ввести необходимо значение, регистр букв при этом не учитывается.

## 17. Подтверждение событий

Функция «**Подтверждение событий**» позволяет направить событие с сервера аналитики в Domination Client, каждому событию присваивается приоритет и устанавливается таймер на его обработку. Операторы, назначенные для обработки событий, обязаны подтвердить их получение в течение установленного времени, в случае если оператор не успевает обработать событие в срок, событие переходит на обработку к другому оператору.

### 17.1. Сценарии реагирования

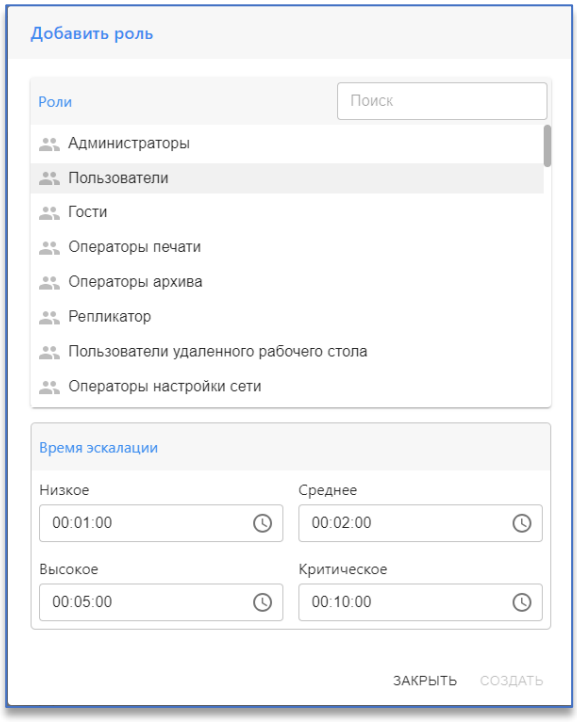
Для начала работы необходимо создать сценарий, для этого нужно нажать на кнопку  , справа от названия списка «**Сценарии**», после чего задать название группы и нажать кнопку 

.

#### 17.1.1. Настройка ролей

Роли необходимы для того, чтобы обозначить, какой группе операторов будет поступать событие на обработку.

Для добавления роли необходимо нажать на кнопку  справа от названия списка «**Роли**», после чего откроется окно для добавления операторов.




Для добавления операторов необходимо выделить название группы нажатием левой кнопки мыши. Также есть возможность редактировать «**Время эскалации**» в зависимости от приоритета. Параметр «**Время эскалации**» отвечает за то, сколько времени будет предоставлено оператору на взаимодействие с событием (в зависимости от приоритета). По истечении заданного времени событие перейдет на обработку в следующую группу операторов.

Для завершения настройки необходимо нажать кнопку 

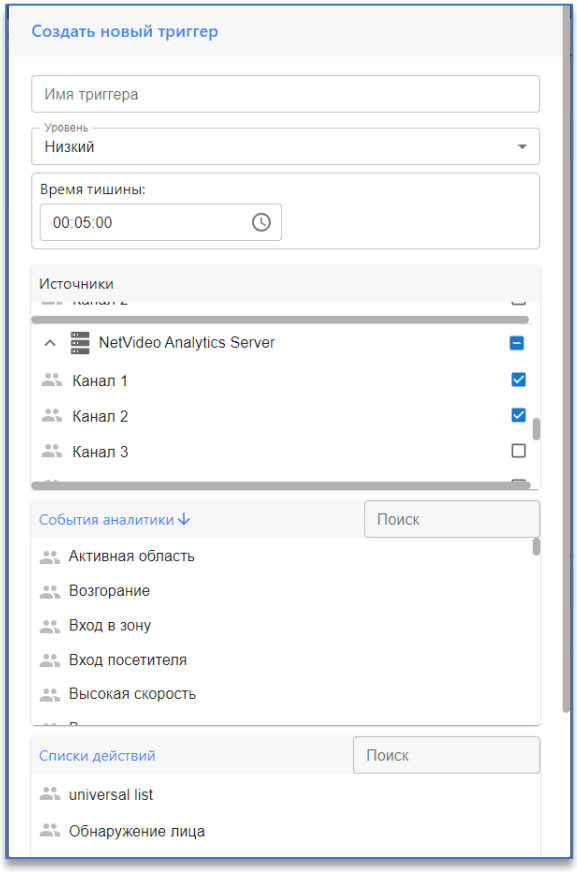
.

Приоритет роли можно задать в самом списке, для этого следует нажать по кнопке  слева от названия и, удерживая, перенести на необходимое место в списке. Событие поступит в первую очередь той группе операторов, которая находится в верху списка.

Удалить или изменить роль в списке можно по кнопке  , которая становится активной при наведении курсора мыши на строку с названием роли.

### 17.1.2. Настройка триггеров

Настройка триггеров сценария необходима для того, чтобы обозначить, какие события должны поступать операторам. Для перехода в настройки необходимо нажать на кнопку + справа от названия списка «**Триггеры**».




В настройках триггера можно задать его название, уровень (приоритет), «Время тишины» и источники

«**Время тишины**» – этот параметр необходим для того, чтобы некоторое время после обработки события, не поступало событий того же типа (срабатывает только в случае, если событие достоверное).

«**Источники**» – параметр, который позволяет указать, с каких каналов и серверов требуется присылать события. Развернуть список каналов можно по кнопке ⌄, доступной рядом с наименованием сервера.

«**События аналитики**» – параметр, позволяющий выбрать событие аналитики, которое будет отправлено оператору на обработку. Для удобства выбора события аналитики можно отсортировать по возрастанию или убыванию, а также найти их через функцию поиска. Для этого достаточно ввести часть названия, значения будут автоматически отсортировываться в соответствии с условиями поиска, регистр букв при этом не учитывается.

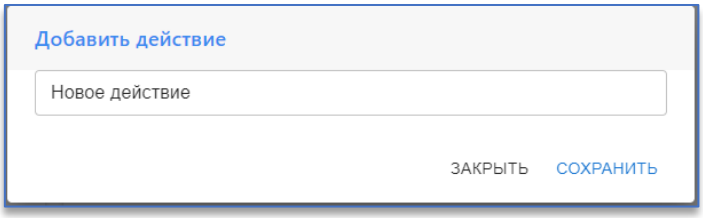
«**Список действий**» – позволяет выбрать список действий, который поступит оператору при срабатывании события.

Для завершения и сохранения настройки необходимо нажать кнопку СОЗДАТЬ.

## 17.2. Настройка списка действий

Список действий необходим для того, чтобы при обработке событий оператор сразу получал инструкцию для той или иной ситуации.

Для того чтобы создать список действий, необходимо нажать на кнопку +, задать имя списка и нажать кнопку СОЗДАТЬ. Далее выбрать созданный список действий, нажав по его называнию левой кнопкой мыши. После чего справа станет доступна кнопка +, с её помощью можно добавлять действия в список.



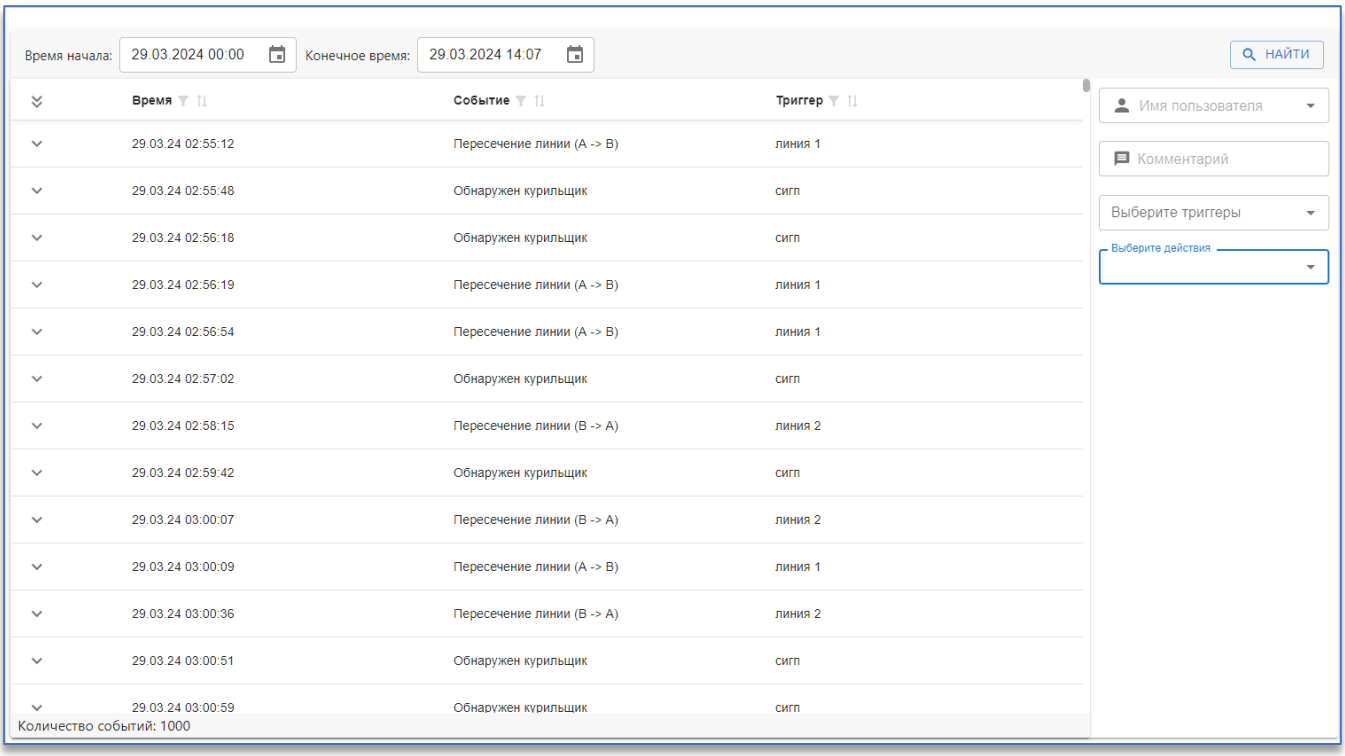

Редактировать или удалять созданные списки можно с помощью кнопки ⋮, которая становится активной при наведении курсора мыши на строку с названием списка.

## 17.3. Логирование

Журнал логирования предназначен для того, чтобы отслеживать отработку событий. В нем фиксируются все события, их дата и время, действие оператора и его комментарий.

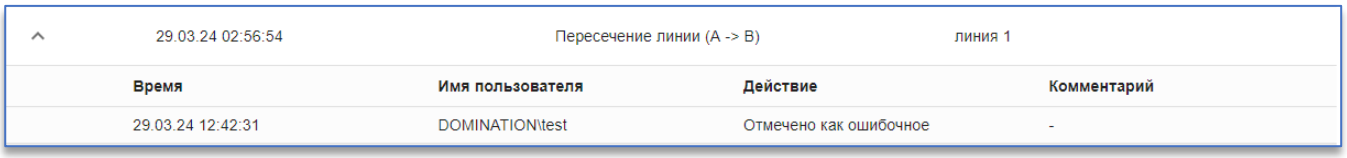
События в журнале можно отфильтровать по следующим характеристикам:

- дата и время;
- имя пользователя, обработавшего события;
- комментарий;
- триггер;
- действие оператора.




Более детальный отчет можно увидеть, нажав на кнопку  .

Кнопка  развернет весь список событий, повторное нажатие на кнопку скроет все данные.




Поиск по списку событий можно настроить в меню с правой стороны от списка. Можно настроить поиск по имени пользователя, его комментарию, выбрать нужный триггер и действие из выпадающего меню, после нажать на кнопку «**Найти**». Также можно настроить время начала события и его конечное время.

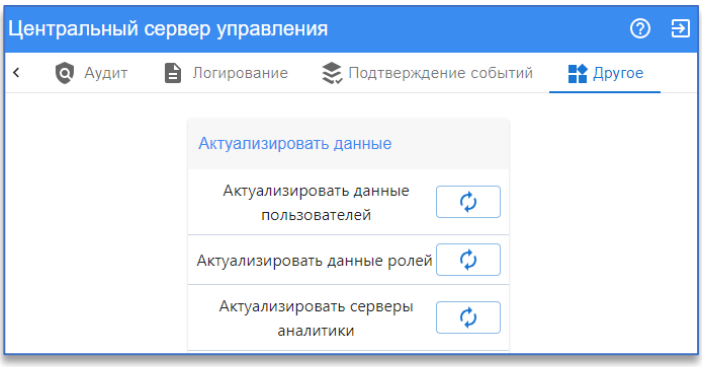
Также отфильтровать события можно с помощью кнопки фильтра  , доступной в строке заголовков. После ее нажатия откроется строка, в которую можно ввести необходимое значение или его часть и события автоматически будут отфильтрованы по введённым данным, регистр букв при вводе не учитывается. Для скрытия фильтра необходимо нажать на клавишу Esc на клавиатуре.

Дополнительно доступна кнопка сортировки значений  . При нажатии на неё появляется возможность отсортировать значения по возрастанию или убыванию.

## 18. Другое

Функции в данном разделе имеют смысл только при использовании Active Directory. Если администратор вносил изменения в Active Directory в части пользователей, ролей и серверов аналитики, то ЦСУ не узнает об этих изменениях пока данные не будут актуализированы.

Для того чтобы актуализировать данные пользователей, ролей и серверов аналитики необходимо нажать кнопку  напротив нужного пункта.




После нажатия в правом углу экрана появится сообщение об успешной актуализации данных.

Например: