



Руководство Domination Central Control Server (Центральный сервер управления)

Версия 1.0.0

Оглавление

1.	Лицензионное соглашение	2
2.	О программе	3
3.	Минимальные системные требования	3
4.	Установка .NET 5	3
5.	Настройка Active Directory для работы с ЦСУ	4
5.1.	Создание атрибутов для Active Directory	4
6.	Установка PostgreSQL на Windows	11
7.	Добавление правил в firewall	14
8.	Установка драйвера для ключа защиты Guardant	15
9.	Настройка конфигурационного файла appsettings.json	15
10.	Настройка автоматического входа в Domination Client через Active Directory	17
11.	Установка DCMServer на Windows	19
12.	Подключение и авторизация через web браузер	19
13.	Подключение и авторизация через Domination Client	19
14.	Информация	20
15.	Серверы	21
15.1.	Видеосерверы	21
15.2.	Серверы аналитики	22
16.	Пользователи	23
17.	Роли	24
18.	Политика безопасности	25
18.1.	Политика безопасности видеосерверов	25
18.2.	Политики безопасности серверов аналитики	26
19.	Аудит	26
19.1.	Видеосерверы	27
19.2.	Серверы аналитики	27

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 ответственность 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 письменных 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.

К Контактная информация

ООО «ВИПАКС+»

Юридический адрес: 115162, г. Москва, вн. тер. г. муниципальный округ Якиманка, ул. Мытная, д.40, к.4, кв. 135

Фактический адрес: 614015, г. Пермь, ул. Краснова, 24

Почтовый адрес: 614015, г. Пермь, а/я 1662

Тел. 8-800-101-01-32

E-mail: info@vipaks.com

Сайт: <https://vipaks.com/>

2. О программе

ПО «Domination Central Control Server» (ЦСУ) позволяет создать единое хранилище настроек и централизованно управлять пользователями масштабной системы видеонаблюдения. Процесс смены настроек или сценариев становится автоматизированным, администратору больше не нужно вручную подключаться к каждому устройству – видеосерверу, серверу видеоаналитики, чтобы добавить нового пользователя или поменять его права доступа.

Для настройки и администрирования ПО ЦСУ имеет встроенный веб-интерфейс, работающий на Linux и Windows. В качестве хранилища данных используется PostgreSQL. В случае, если имеется Active Directory (либо другое LDAP-хранилище) с уже введенными пользователями, то можно использовать его для аутентификации и хранения настроек пользователей.

3. Минимальные системные требования

Операционная система: Windows 10, Windows Server 2012 - 2019

Дополнительное ПО: Microsoft .NET 5

Процессор: Intel i3 530

Оперативная память: 4 GB

Свободное место на диске для программы: не менее 5 GB

Поддерживаемые браузеры: Google Chrome, Opera, Microsoft Edge, Mozilla Firefox

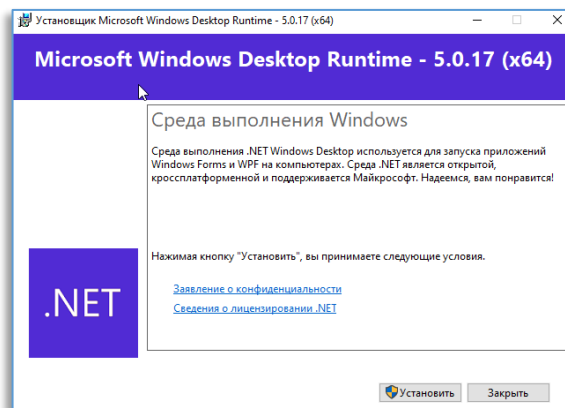
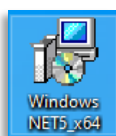
Domination Client: версия 2.12 и выше

Видеосервер Domination: версия 2.1.4.6 и выше

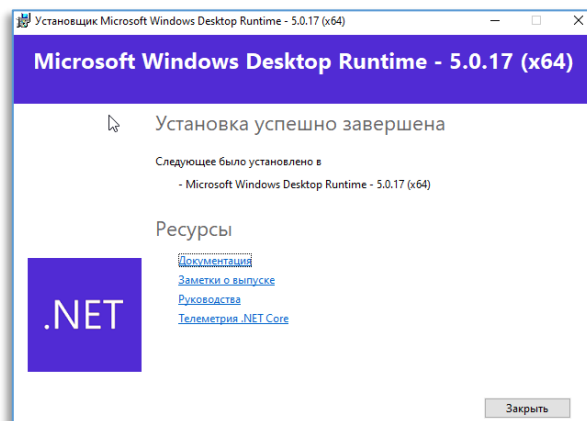
Сервер аналитики: версия 1.9 и выше

4. Установка .NET 5

Для установки программы используется дистрибутив Windows NET5_x64.exe из архива. После запуска нажмите «Установить».



Далее, нужно дождаться завершения установки.
Для завершения установки требуется нажать на кнопку «Закреть».



5. Настройка Active Directory для работы с ЦСУ



Если не планируется использовать авторизацию с помощью Active Directory, то пункты 5 и 5.1 нужно пропустить.

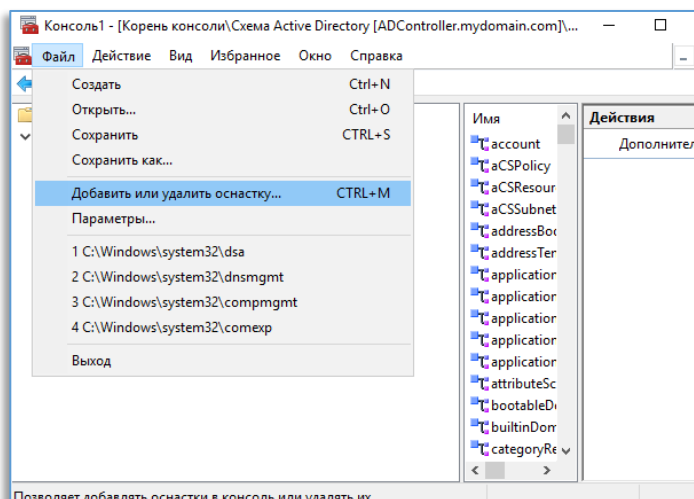
Для работы авторизации через доменных пользователей необходимо добавить атрибуты пользователям. Нужно создать пользователя домена и запомнить его пароль. (Задать имя, например: "dominationServiceAccount"). В дальнейшем пароль потребуется прописать в файле конфигурации **appsettings.json**.

5.1. Создание атрибутов для Active Directory

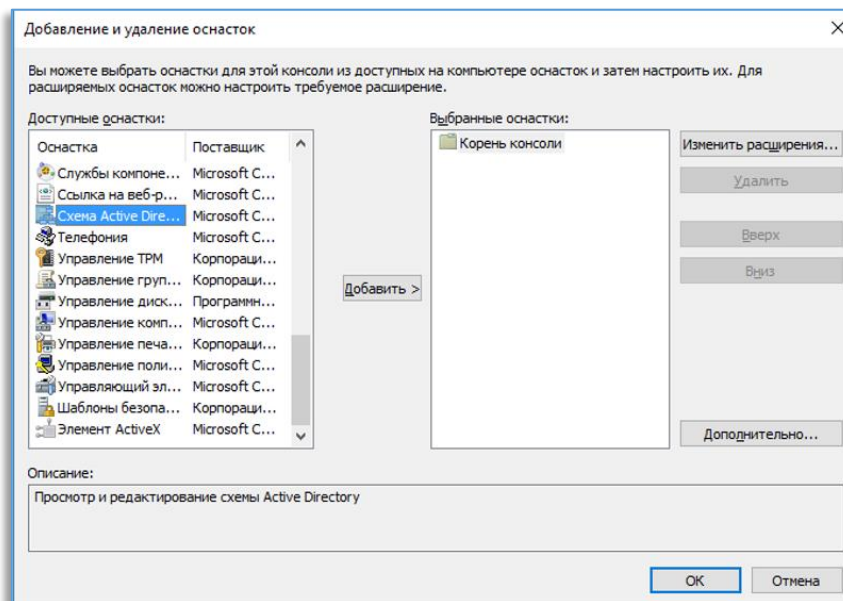
Потребуется добавить атрибуты и назначить делегирование этими атрибутами сервисному пользователю. Выполнить в cmd.exe команды:

```
regsvr32 schmmgmt.dll
mmc
```

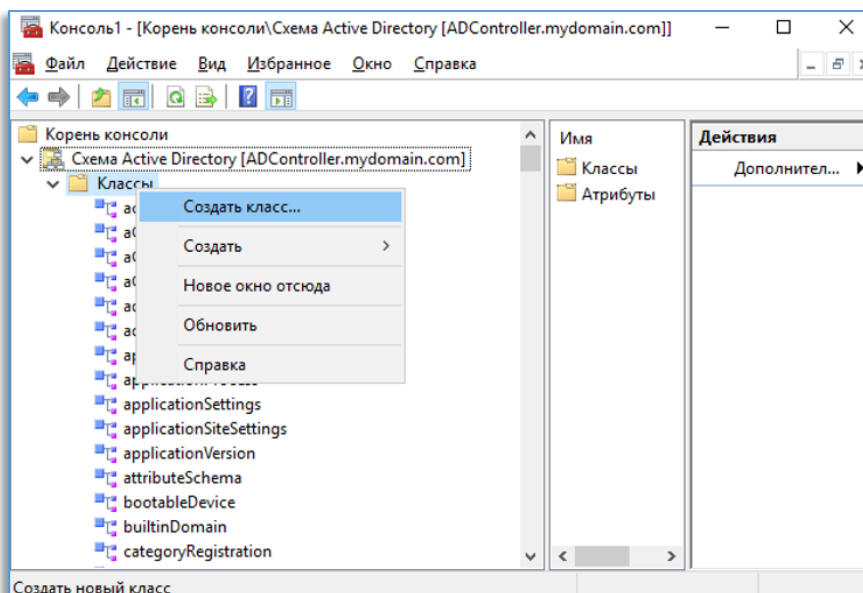
В открывшемся окне "Консоль1 - Корень консоли" нажимаем «Файл» -> «Добавить или удалить оснастку».



В окне "Добавление и удаление оснасток" находим "Схема Active Directory" и нажимаем "Добавить>". Затем "ОК".



В окне "Консоль1 - Корень консоли" раскрываем "Схема Active Directory" и "Классы". Нажимаем ПКМ по директории "Классы", нажимаем "Создать класс...".



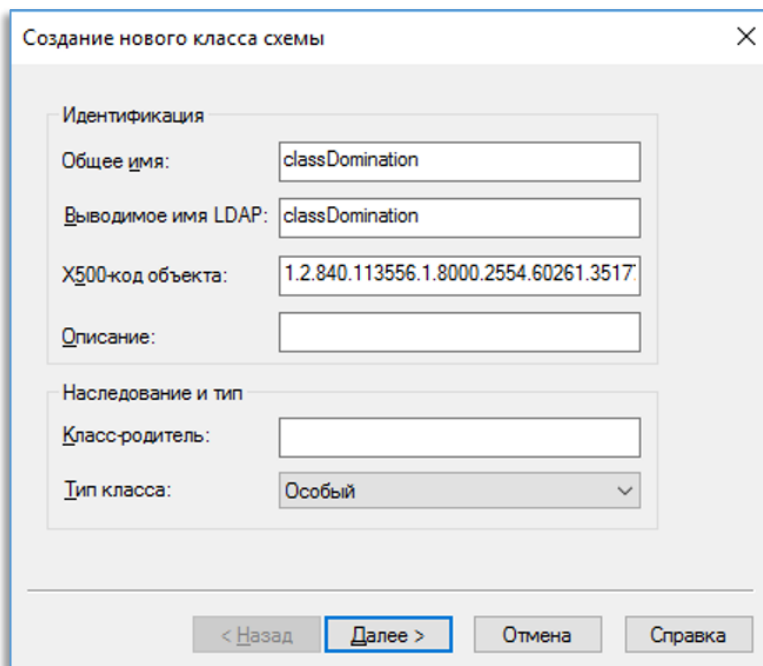
В окне «Создание нового класса схемы» вводим следующие данные:

Общее имя: classDomination

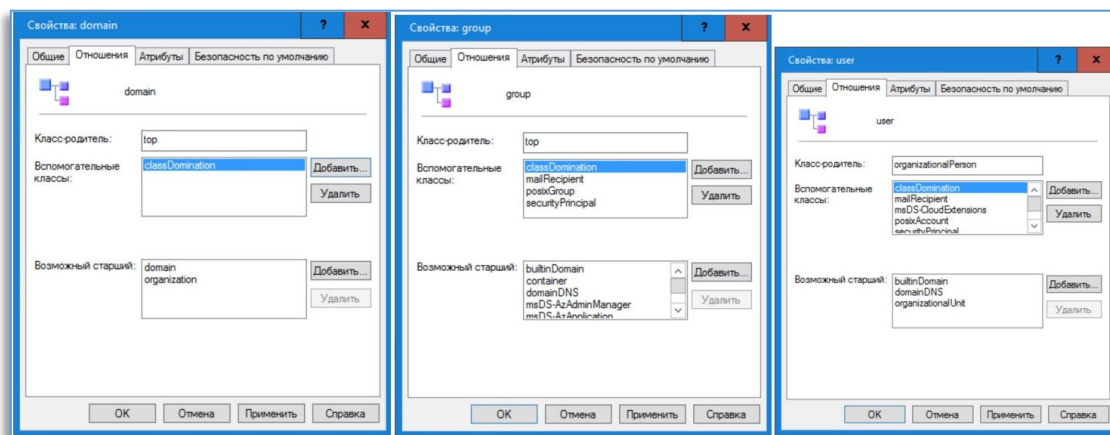
X500-код объекта: 1.2.840.113556.1.8000.2554.60261.35177.16306.19442.40185.2384456.12562999.1.1

Тип класса: Особый

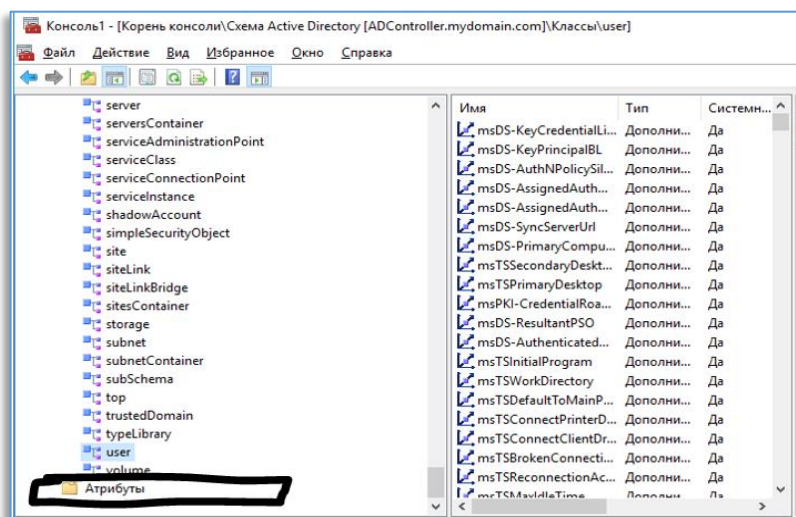
Нажимаем "Далее" и "Готово".



В списке "Классы" у классов "domain", "user" и "group" делаем следующее: ПКМ -> "Свойства". Далее нажимаем вкладку "Отношения". Напротив списка "Вспомогательные классы:" нажимаем "Добавить...". Выбираем созданный ранее класс "classDomination" и нажимаем "OK".



Нажимаем ПКМ по директории "Атрибуты", нажимаем "Создать атрибут...".



В окне «Создание нового атрибута» вводим следующие данные:

Атрибут "DomAuthServer"

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

Нажимаем "ОК". Нажимаем ПКМ по директории "Атрибуты", нажимаем "Создать атрибут...". Атрибут "DomPermission". Не забудьте здесь поставить галку "Многозначный".

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

Не забудьте здесь поставить галочку "Многозначный". Нажимаем "ОК" Нажимаем ПКМ по директории "Атрибуты", нажимаем "Создать атрибут..." Атрибут "DomAnalyticsPermission". Не забудьте здесь поставить галку "Многозначный".

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

Нажимаем "ОК" Нажимаем ПКМ по директории "Атрибуты", нажимаем "Создать атрибут..." Атрибут "DomUseAuth".

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

Нажимаем "ОК" Нажимаем ПКМ по директории "Атрибуты", нажимаем "Создать атрибут..." Атрибут "DomSubjectProperties".

Общее имя: DomSubjectProperties

X500-код объекта: 1.2.840.113556.1.8000.2554.60261.35177.16306.19442.40185.2384456.12562999.2.5

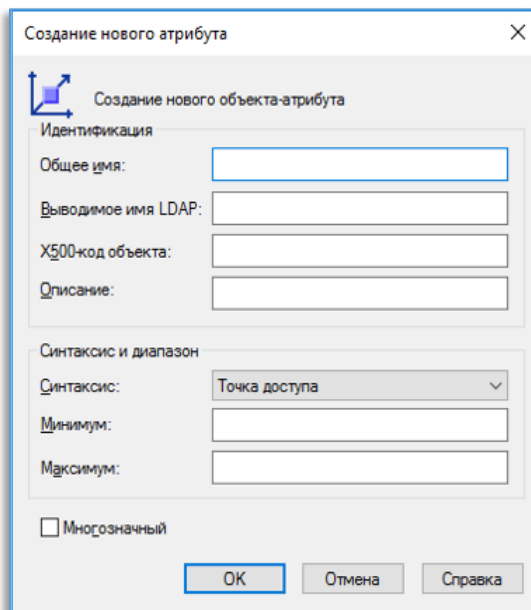
Синтаксис: Строка Юникода

Максимум: 4096
 Многозначный: Нет
 Нажимаем "OK"

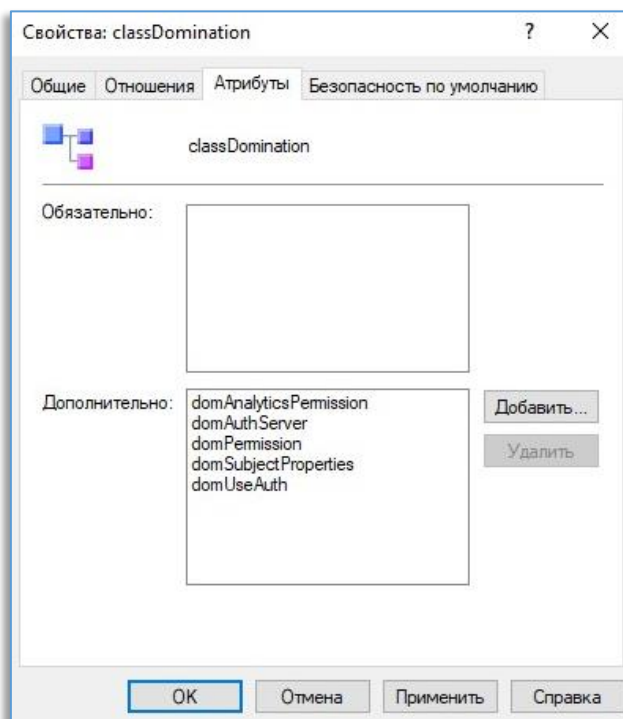
Нажимаем "OK" Нажимаем ПКМ по директории "Атрибуты", нажимаем "Создать атрибут..." Атрибут "DomProfile".

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

Нажимаем "OK".

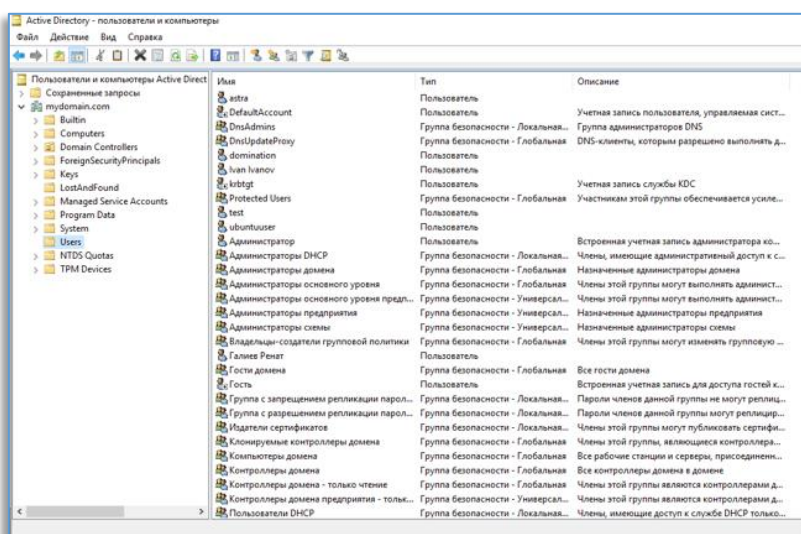


Возвращаемся в окно "Окно "Консоль1 - Корень консоли"". В директории "Классы" находим наш класс "classDomination". ПКМ -> "Свойства". Вкладка "Атрибуты". В "Дополнительно:" нажимаем "Добавить...". Добавляем наши атрибуты **DomAuthServer, DomAnalyticsPermission, DomPermission, DomUseAuth, DomSubjectProperties, DomProfile**. Нажимаем "OK" и перезагружаем компьютер для применения изменений.

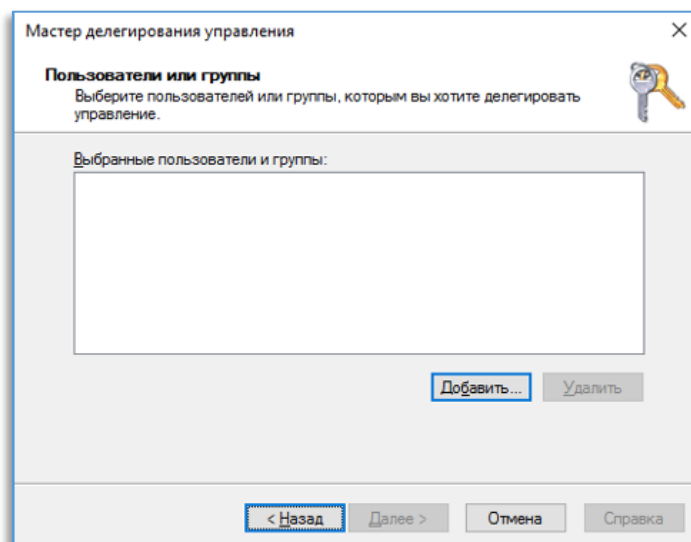


Далее
пользователи и компьютеры".

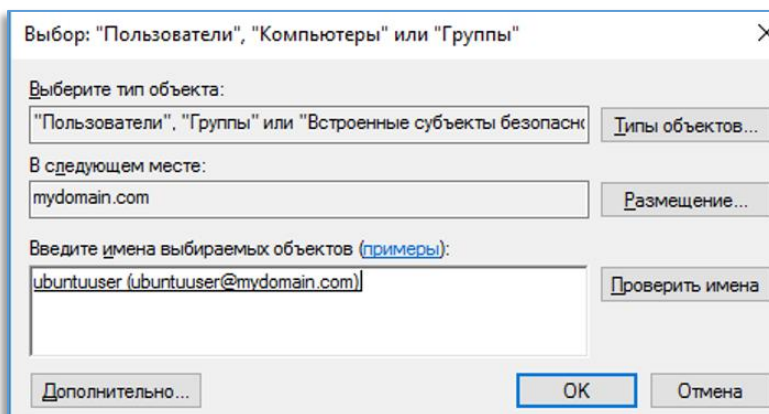
открываем "Active Directory –



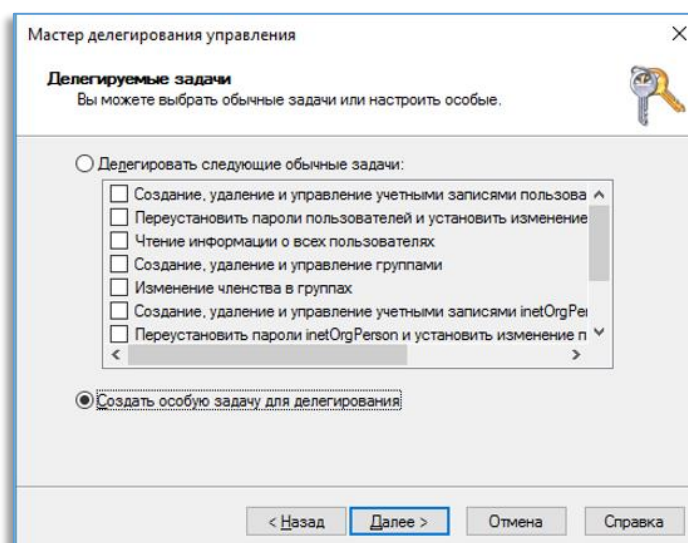
Находим в домене директорию "Users". Нажимаем ПКМ -> "Делегирование управления" Нажимаем "Добавить...".



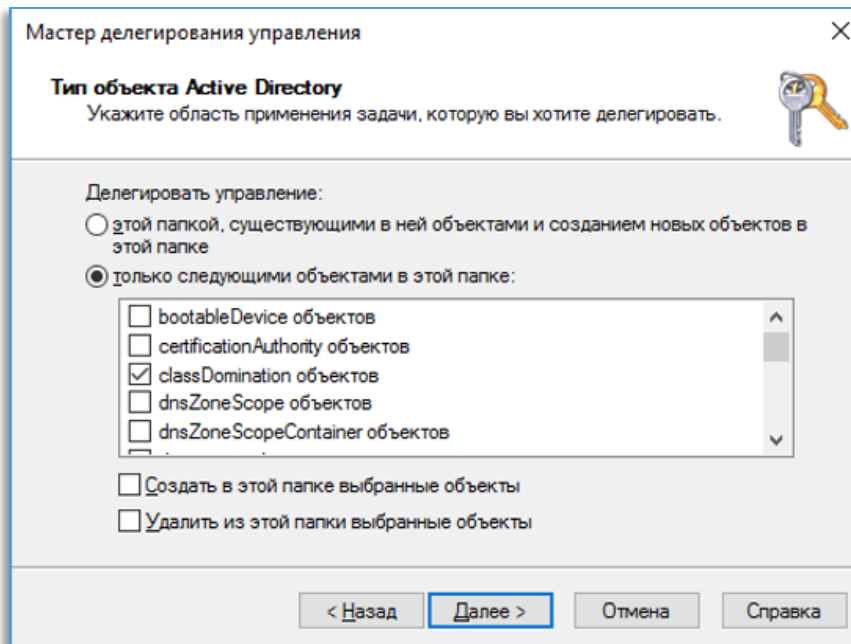
Вписываем в поле имя "Сервисного пользователя" DCMServer'a. (Его нужно создать если этого еще не сделали. Это обычный пользователь домена, назовите как хотите. Например: "dominationServiceAccount"). В примере это пользователь "ubuntuuser". Нажимаем "OK".



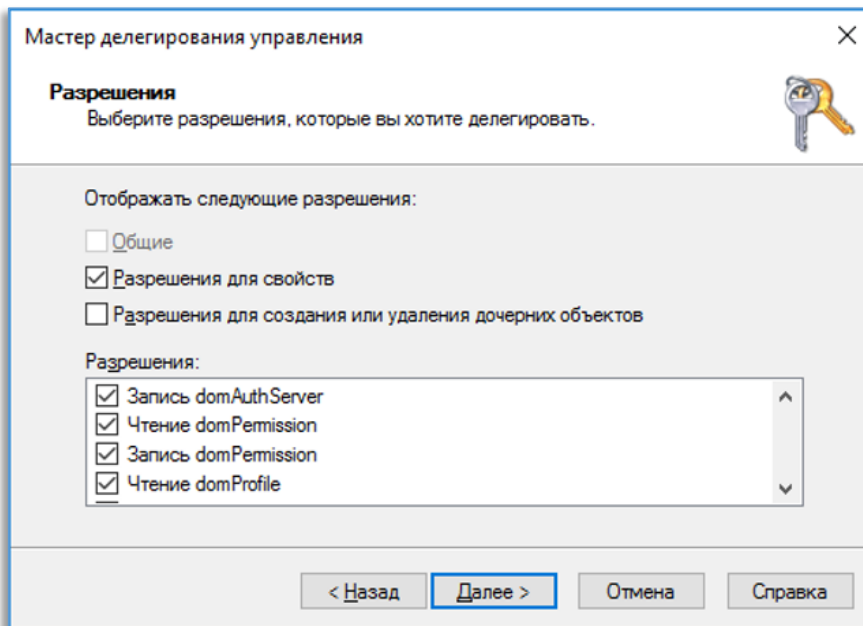
В окне "Мастер делегирования управления" в пункте "Делегируемые задачи" выбрать "Создать особую задачу для делегирования". Нажимаем "Далее".



Выбрать "Только следующими объектами в этой папке" и выбираем наш класс "classDomination" Нажимаем "Далее".



Выбрать "Разрешения для свойств". Выбрать "чтение" и "запись" для всех свойств нажимаем "Далее" Нажимаем "Готово".

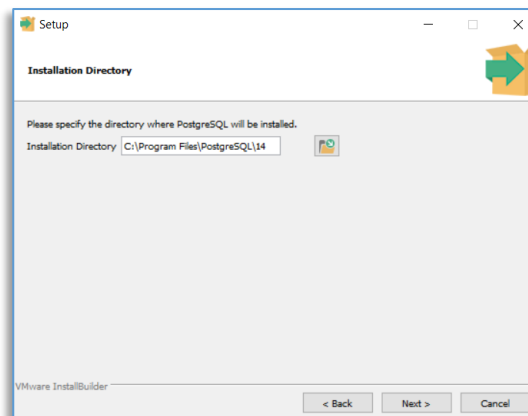


Мы успешно добавили атрибуты для работы DCM сервера и создали сервисного пользователя для работы с атрибутами.

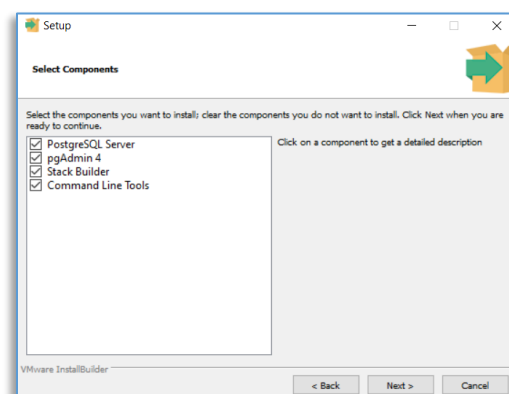
6. Установка PostgreSQL на Windows

Скачать PostgreSQL версии 14.3 для Windows с сайта <https://www.enterprisedb.com/downloads/postgres-postgresql-downloads> или использовать из комплекта поставки программы. Запустить скаченный файл, должно появиться окно установки.

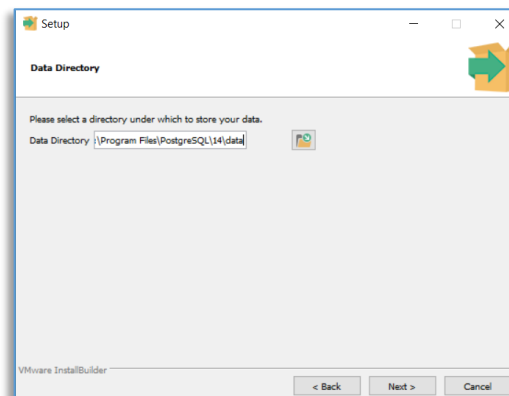
Нажать кнопку «Next». В директории установки СУБД оставить по умолчанию.



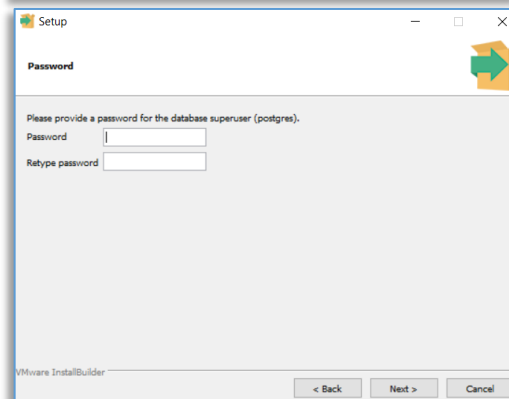
Нажать кнопку «Next». В окне выбора компонентов проверить, что отмечены галочками «Все» компоненты.



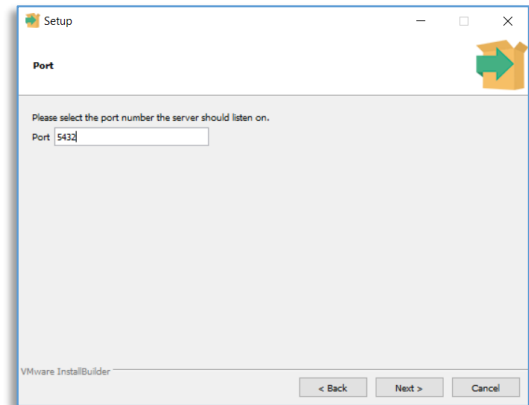
Нажать кнопку «Next». В директории файлов самой базы данных оставить по умолчанию. Запомнить эту директорию.



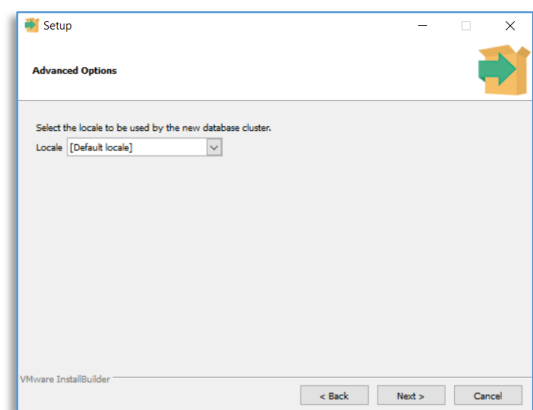
Нажать кнопку «Next». В окне придумать и установить пароль для суперпользователя postgres. Данный пароль нужно запомнить, так как его следует указать в конфигурационном файле **appsettings.json**.



Нажать кнопку «Next». В окне номер порта оставить по умолчанию (5432).



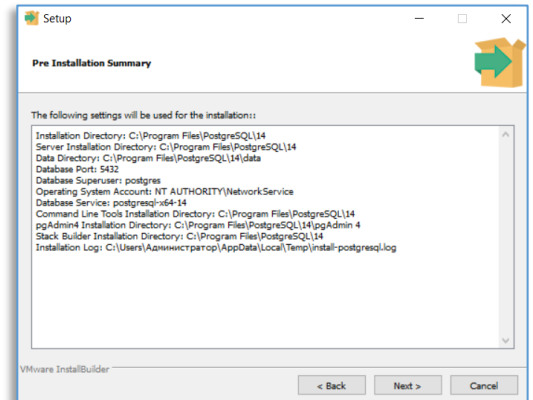
Нажать кнопку «Next». В окне настройки локализации оставить по умолчанию.



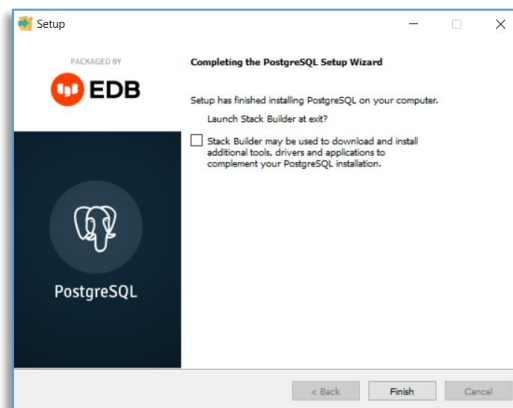
Нажать кнопку «Next». Появится окно с предварительным просмотром сделанных настроек.

Нажать кнопку «Next». В окне для запуска процесса установки снова нажать кнопку «Next».

Должно появиться окно процесса установки. Дождаться окончания процесса установки.



В окне снять галочку напротив пункта «Stack Builder...» и нажать кнопку «Finish».



Перейти в директорию файлов базы данных (путь был выбран ранее в окне). Открыть файл pg_hba.conf, найти фрагмент и заменить 127.0.0.1/32 на 0.0.0.0/0. Сохранить и перезагрузить компьютер.

```
# IPv4 local connections:
host      all             all             127.0.0.1/32    scram-sha-256
```

7. Добавление правил в firewall

Чтобы разрешить сетевой доступ к вашему экземпляру PostgreSQL и ЦСУ с других компьютеров, вам нужно создать правила в файрволе. Вы можете создать правило через «командную строку».

Запустите командную строку от имени администратора. Введите команду:

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

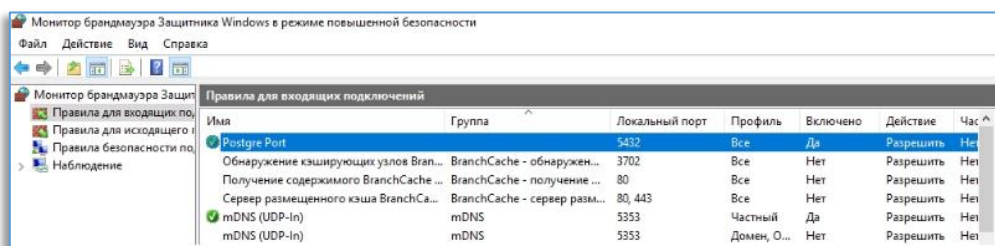
netsh advfirewall firewall add rule name="ЦСУ Port" dir=in action=allow protocol=TCP localport=8000

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 команды в брандмауэре Windows появится новое разрешающее правило для порта Postgres.



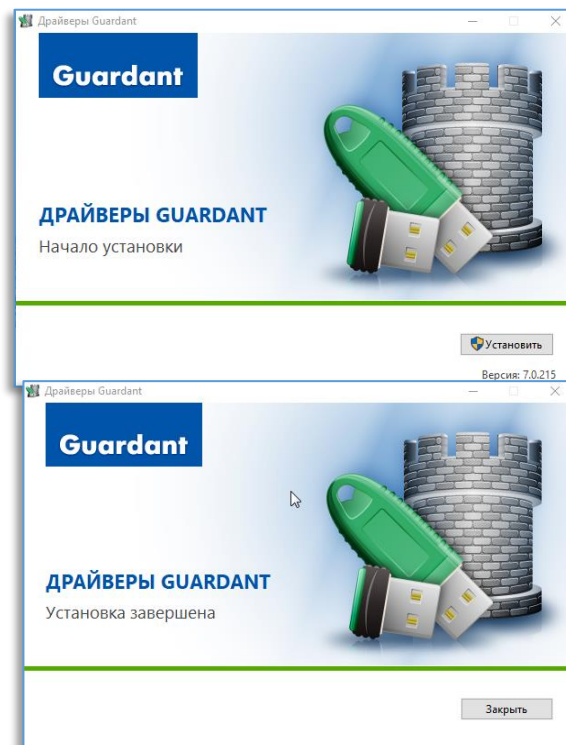
8. Установка драйвера для ключа защиты Guardant

Для установки программы используется дистрибутив GrdDrivers.exe из архива. После запуска нажмите «Установить».

Далее, нужно установить. Требуется нажать



дождаться завершения. Для завершения установки на кнопку «Закреть».



9. Настройка конфигурационного файла appsettings.json

Файл **appsettings.json** находится в корне папки с программой. Секция для настройки номера порта службы DCMServer. По умолчанию указан порт 8001.

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

Секция для настройки номера порта, по которому видеосервера Domination будут подключаться к службе DCMServer. 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 DCMServer.

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

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 выбора провайдера данных. Для работы с ролями и пользователями через Active Directory укажите для поля Users значение AD, если через базу данных PostgreSQL, то 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 компьютер установлена впервые, то 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 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" ]
}
```

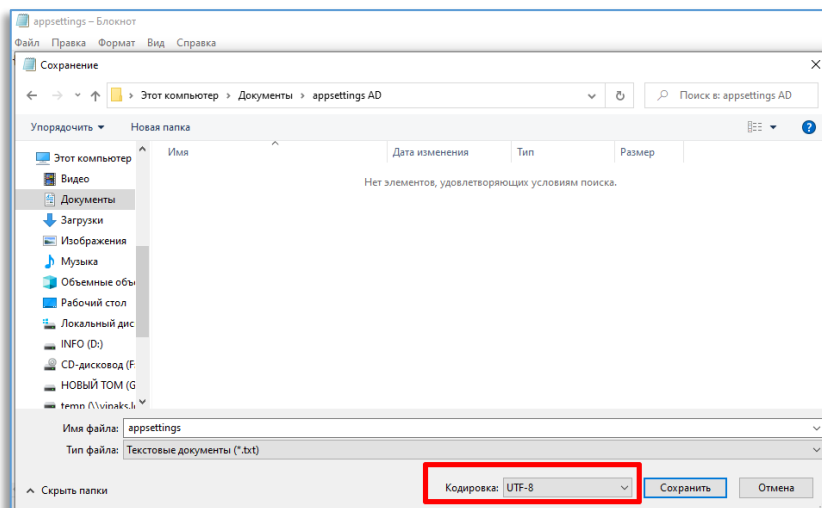
Секция настройки сервиса Elastic.

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

Секция настройки сервиса Swagger.

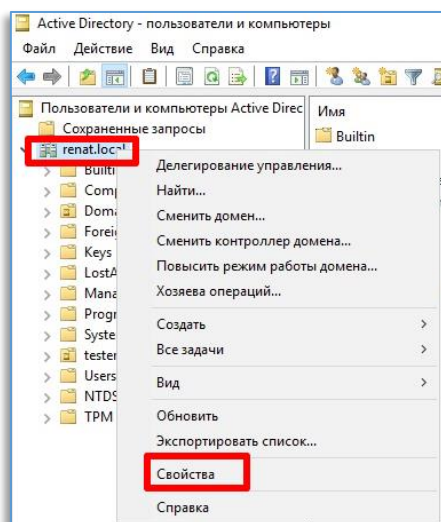
```
"SwaggerConfiguration": {
  "UseSwagger": true
}
```

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

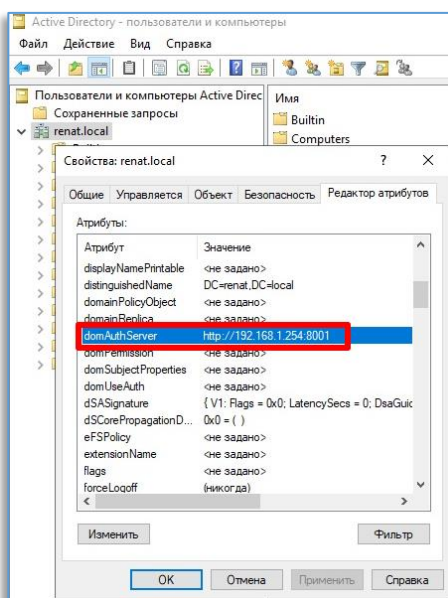


10. Настройка автоматического входа в Domination Client через Active Directory

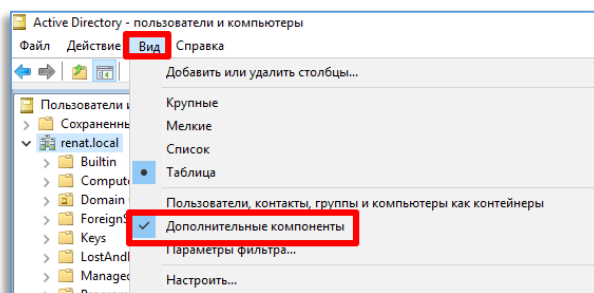
Для автоматического входа в Domination Client требуется зайти в «Active Directory – пользователи и компьютеры». Нажать ПКМ по названию домена – «Свойства».



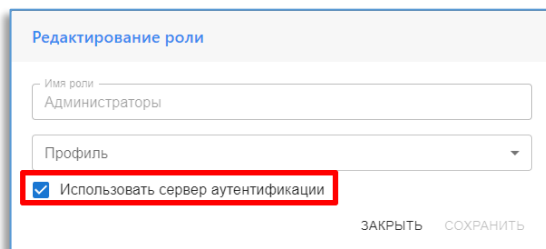
Во вкладке «Редактор атрибутов» найти атрибут «domAuthServer» и прописать IP адрес ЦСУ.



Если в свойствах нет «Редактора атрибутов», то нажмите «Вид» - «Дополнительные компоненты».



В ЦСУ наведите на нужного пользователя или роль и нажмите . Выберите «Изменить» или «Редактировать роль» и поставьте  на против «Использовать сервер аутентификации».



Добавление пользователя и роли в ЦСУ производится через Active Directory.

11. Установка DCMServer на Windows

Извлеките из архива программу в удобное место. Потребуется зарегистрировать приложение в виде службы. Для этого потребуется указать аргументы командной строки:

install - зарегистрировать приложение (например: C:\win-x64\NetVideo.Enterprise.AuthService.exe install)

start – запустить сервис (например: C:\win-x64\NetVideo.Enterprise.AuthService.exe start)

stop - остановить сервис (например: C:\win-x64\NetVideo.Enterprise.AuthService.exe stop)

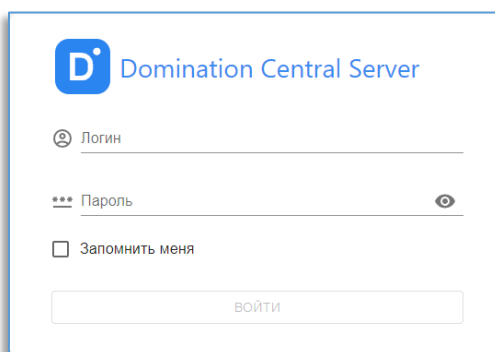
uninstall - удалить регистрацию сервиса (например: C:\win-x64\NetVideo.Enterprise.AuthService.exe uninstall)

12. Подключение и авторизация через web браузер


Для подключения к ЦСУ необходимо открыть на устройстве web браузер и в поле адреса ввести адрес компьютера, где установлен ЦСУ, например: 192.168.0.248:8001.

Стандартный порт для подключения используется: 8001.

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





В окне авторизации указываем логин и пароль, который прописали в файле конфигурации **appsettings.json**.

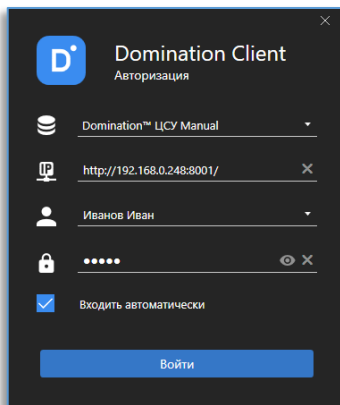
Кнопка  в строке, где указывается пароль, служит для просмотра введённого пароля.

Чтобы в дальнейшем при открытии меню авторизации больше не появлялось, необходимо поставить «галку» в поле «**Запомнить меня**».

13. Подключение и авторизация через Domination Client

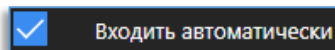
Для подключения к ЦСУ необходимо запустить «**Domination Client**». В меню авторизации в поле «**Тип профиля**»  выберите «**Domination ЦСУ Manual**», если используется база данных (не служба каталогов). В поле «**Адрес сервера**» укажите адрес компьютера, где установлен ЦСУ и порт ЦСУ, например: <http://192.168.0.248:8001>. В поле логин и пароль указываете учетные данные из ЦСУ.

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



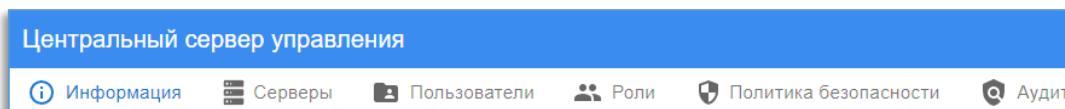
Если вход в Windows был выполнен, используя Active Directory, то вход в программу будет выполнен автоматически при условии, что данному пользователю разрешено авторизоваться через ЦСУ.

Чтобы в дальнейшем при запуске клиента Domination меню авторизации больше не появлялось, необходимо поставить «галку» в поле «**Входить автоматически**».



14. Информация

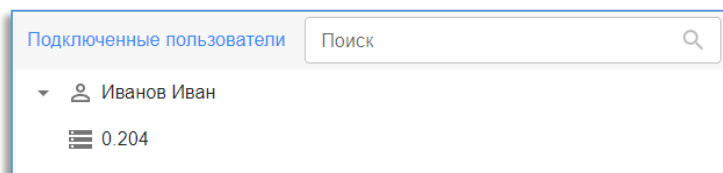
После авторизации отображается страница информации о лицензии и подключенных пользователях.



Информация о лицензии отображает максимальное и используемое количество каналов.

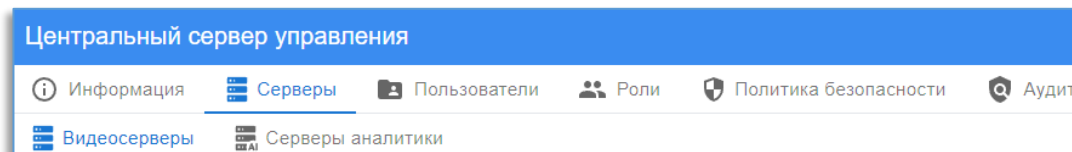
Информация о лицензии	
Максимальное число каналов	130
Используемое кол-во каналов	5

В подключенных пользователях отображаются те пользователи, которые в данный момент подключены к серверам.



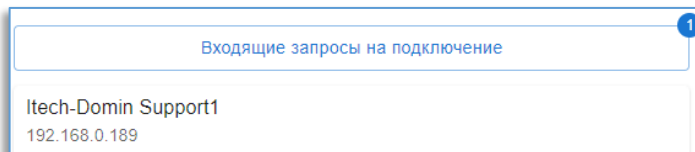
15. Серверы

На вкладке «Серверы» доступно добавление серверов в ЦСУ.

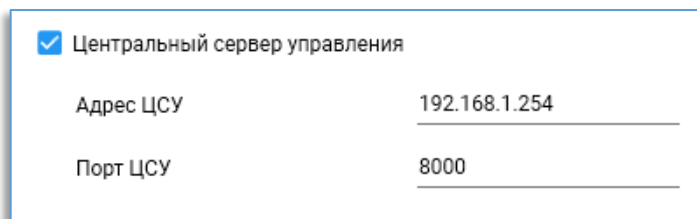


15.1. Видеосерверы

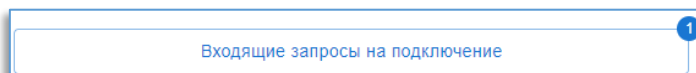
Данная вкладка отображает входящие запросы на подключение и информацию о подключенных видеосерверах.




Для подключения видеосервера в ЦСУ, откройте конфигуратор Windows/WEB, зайдите во вкладку «Общие», поставьте галочку напротив «Центральный сервер управления». Далее требуется указать IP адрес и порт ЦСУ.

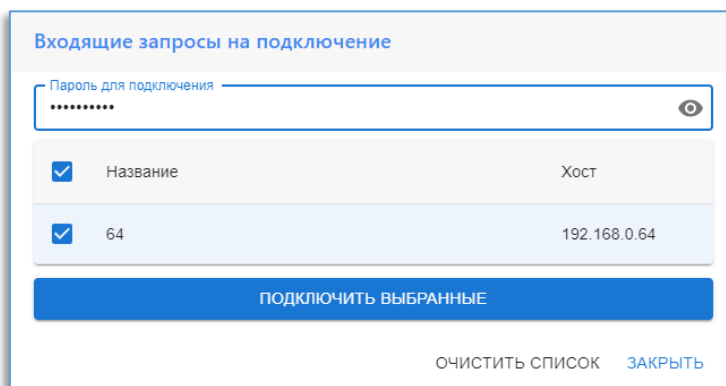


В ЦСУ нажимаете на «Входящие запросы на подключения».

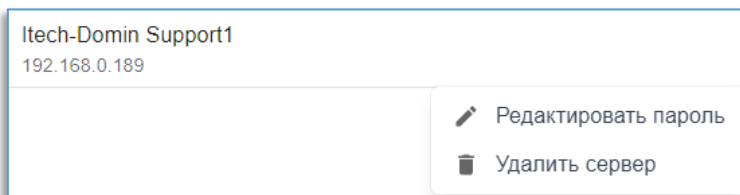


Выберите видеосервер , введите пароль от пользователя «root» видеосервера в строке «Пароль для подключения» и нажимаете «Подключить выбранные».

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

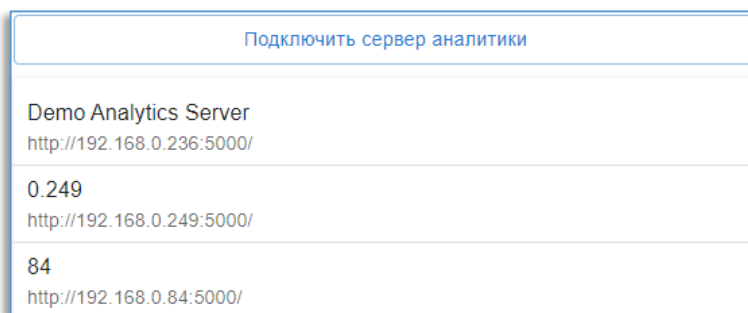


Чтобы «**Редактировать пароль**» или «**Удалить сервер**» наведите на нужный видеосервер и нажмите .

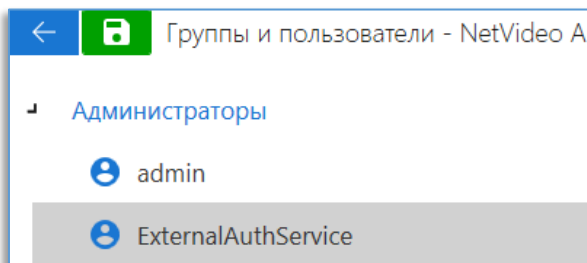


15.2. Серверы аналитики

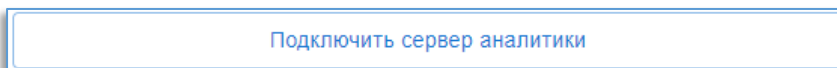
Данная вкладка отображает информацию о подключенных серверах аналитики и «**Подключить сервер аналитики**».



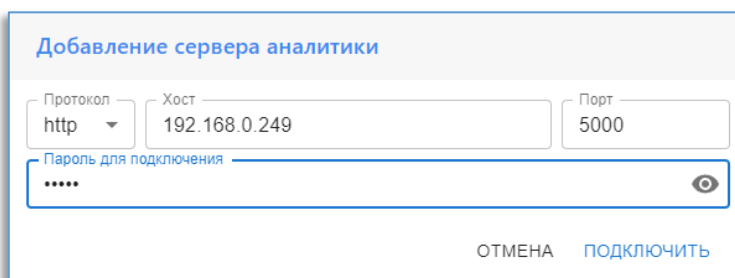
Для подключения сервера аналитики в ЦСУ требуется создать пользователя «**ExternalAuthService**» с любым паролем в конфигураторе аналитики в разделе «**Пользователи**».




Чтобы подключить сервер аналитики нажмите на «**Подключить сервер аналитики**».

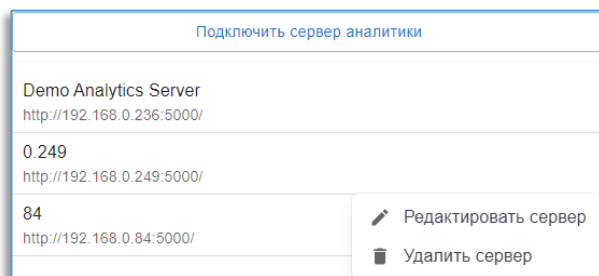


Выберите протокол, введите IP адрес, порт сервера аналитики и пароль от пользователя «**ExternalAuthService**».

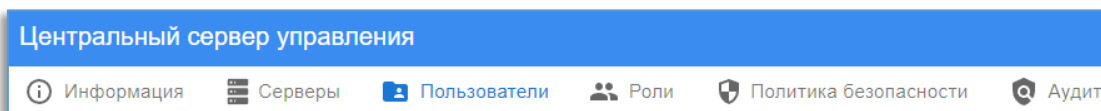


Кнопка  в строке, где указывается пароль, служит для просмотра введённого пароля.

Чтобы «**Редактировать сервер**» или «**Удалить сервер**» наведите на нужный сервер аналитики и нажмите  .



16. Пользователи



На вкладке «**Пользователи**» доступен список всех пользователей, заведённых в ЦСУ.

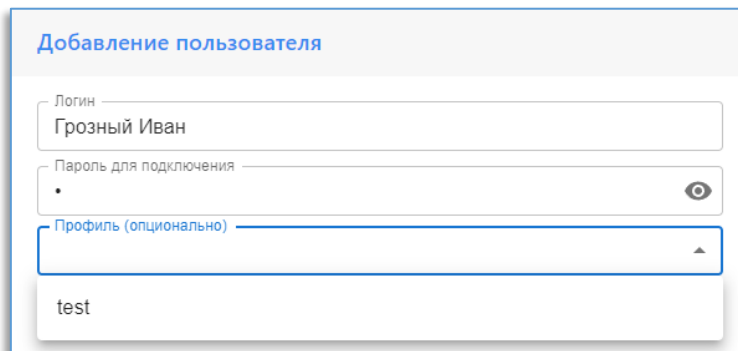


При использовании AD отображаются пользователи, занесённые в службу каталогов. Добавить и редактировать через ЦСУ невозможно.

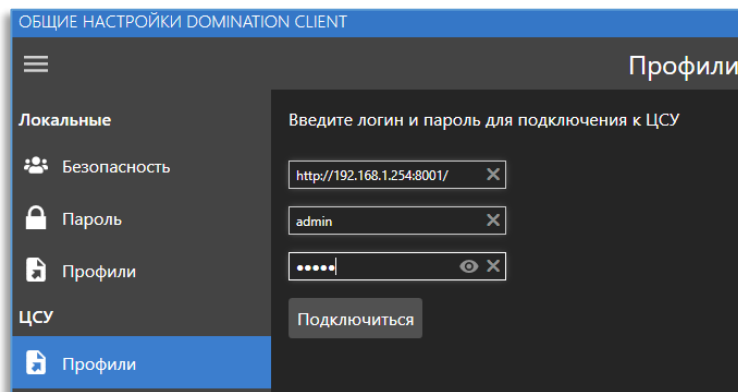
Чтобы добавить нового пользователя, нужно нажать на кнопку  .

В появившемся окне требуется указать логин и пароль.

В «**Профиле**» можно указать заранее настроенный профиль, который будет использоваться при открытии клиента Domination.

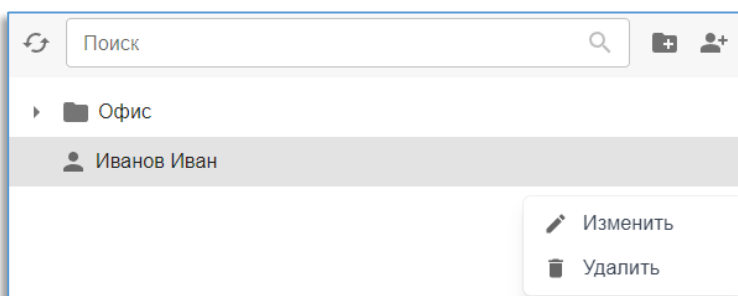



Чтобы экспортировать профиль в ЦСУ потребуется зайти в «**Общие настройки**» Domination Client, выбрать ЦСУ профиль. Ввести адрес, порт, логин и пароль ЦСУ.




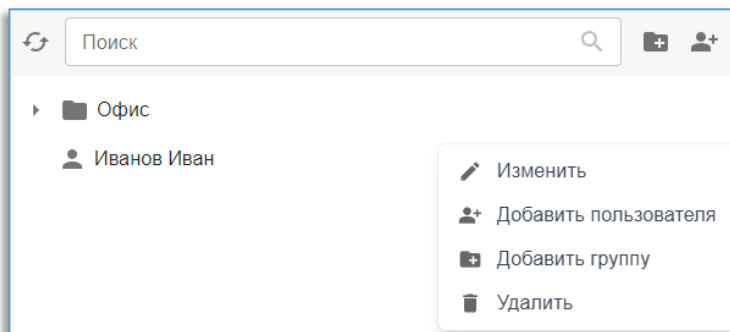
После подключения нажмите «Экспорт в ЦСУ» и выберите нужный профиль.

Чтобы «Изменить» или «Удалить» пользователя наведите на нужного пользователя и нажмите .



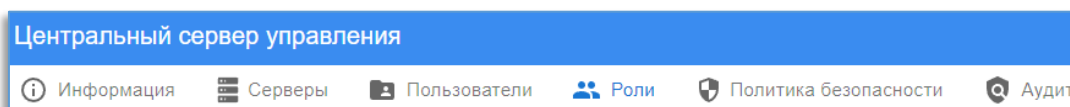
Чтобы добавить «Группы» нужно нажать на кнопку .


Чтобы «Изменить», «Добавить пользователя», «Добавить группу» и «Удалить» группу наведите на нужную группу и нажмите .






17.Роли

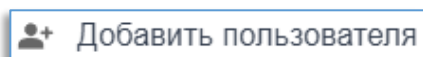
Роли позволяют группировать пользователей по общей принадлежности к одной категории для более удобной и единовременной настройки политики безопасности выбранных групп.





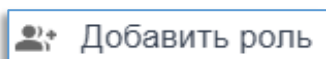
Чтобы добавить новую роль нужно нажать на кнопку .

Чтобы «Добавить пользователя», «Добавить роль», «Редактировать роль», «Редактировать локальную политику безопасности» и «Удалить» роль наведите на нужную роль и нажмите .

Чтобы добавить пользователя в роль нажмите «Добавить пользователя», выберите пользователя  и перенесите его в правую колонку, кнопкой .

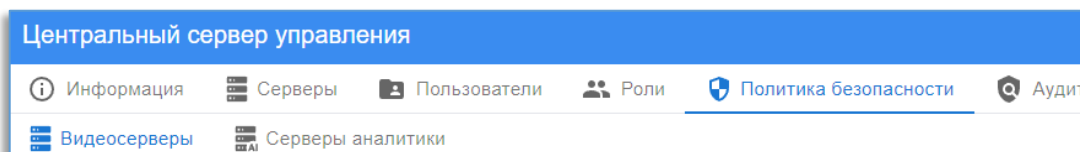


Чтобы добавить роль в роль нажмите «Добавить роль», после этого, выберите роль  и перенесите в правую колонку кнопкой .



Чтобы добавить пользователя в роль нажмите «Редактировать политику безопасности», выберите нужные настройки .

18. Политика безопасности



В разделе политики безопасности можно настроить доступ пользователей, которые входят в определённую роль, к различным функциям видеосервера и сервера аналитики.

18.1. Политика безопасности видеосерверов

Чтобы предоставить/убрать доступ роли до нужного ресурса, необходимо поставить/снять соответствующую «галку» в необходимом пункте, предварительно выбрав видеосервер в столбце слева.

Роль	Объект	<input checked="" type="checkbox"/> Подключение	<input checked="" type="checkbox"/> Настройка	<input checked="" type="checkbox"/> Архив	<input checked="" type="checkbox"/> Управление	<input checked="" type="checkbox"/> Звук подключения	<input checked="" type="checkbox"/> Звук архив
Офис_1	Сервер	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
	Журнал	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>			
	Канал 1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Канал 2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Канал 3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Канал 4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
	Канал 5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

У «Доступа до реакции» требуется указать уровень доступа для роли, пользователи смогут запустить привязанную к событию реакцию. Если уровень у роли ниже, чем выставленный уровень в событии, то запустить реакцию данные пользователи не смогут.

Доступ до реакций — 1 +

В «Ограничении трафика» указывается ограничение на получение трафика в мегабитах для указанной роли. Ограничение трафика начинает действовать для вновь установленных соединений.

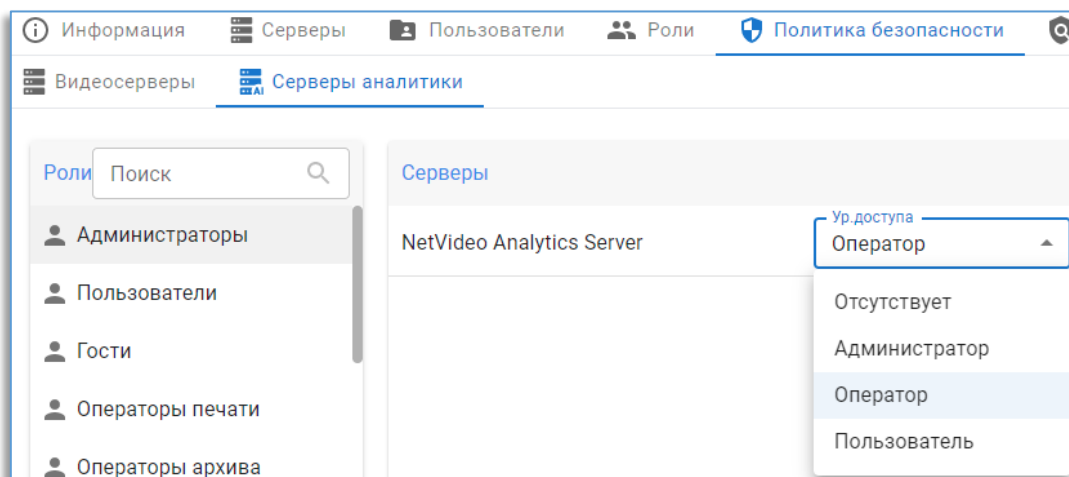
Ограничение трафика, МБит/сек.

18.2. Политики безопасности серверов аналитики

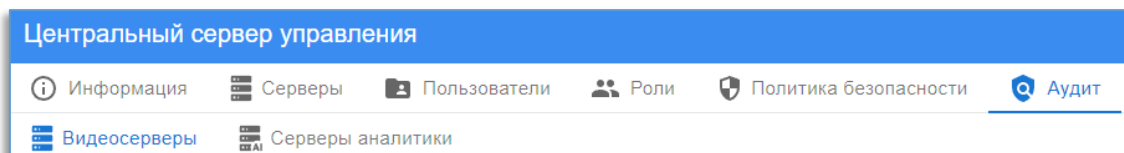
Роли, добавленные в группу «Администраторы», имеют право подключаться к серверу аналитики для его настройки, получать и редактировать события аналитики через «Domination Client», добавлять автомобили и персоны в базу.

Роли, добавленные в группу «Операторы», имеют право получать и редактировать события аналитики через «Domination Client», добавлять автомобили и персоны в базу.

Роли, добавленные в группу «Пользователи», имеют право только подключаться к серверу аналитики для получения событий в клиенте Domination.



19. Аудит

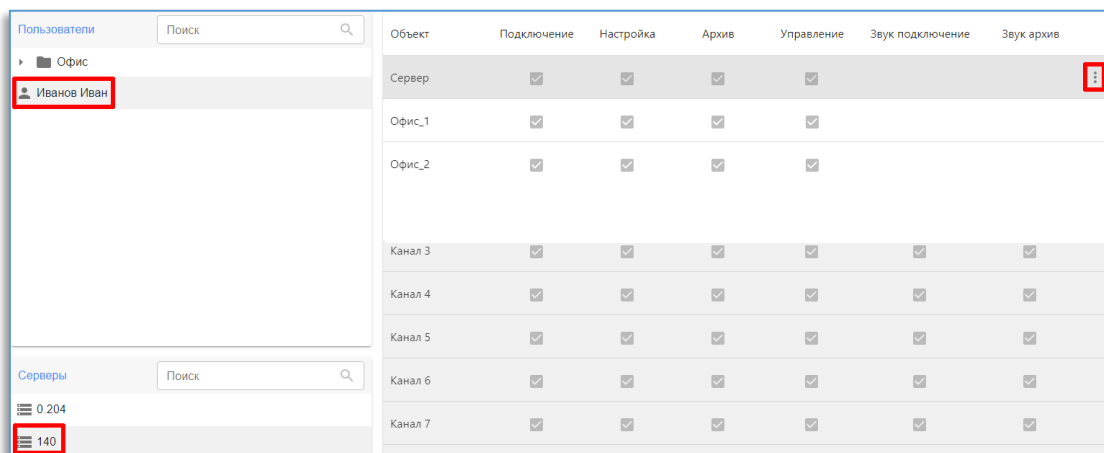


Во вкладке аудит можно просмотреть информацию прав доступа до видеосервера и сервера аналитики, по каждому пользователю, а также в каких ролях состоит пользователь.

19.1. Видеосерверы


Чтобы посмотреть в какие роли добавлен пользователь и есть права на каком сервере/канале,

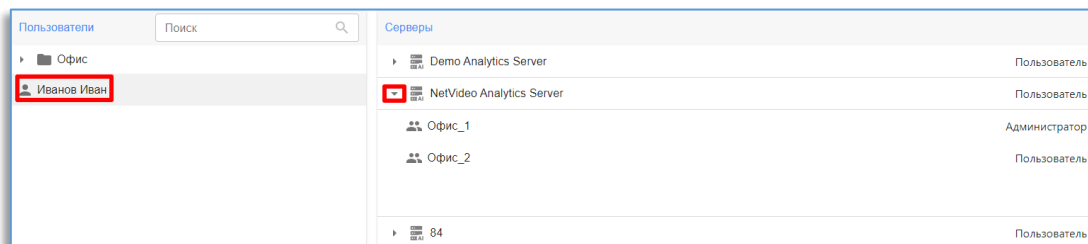
выберите пользователя/видеосервер и наведите на нужный сервер/канал и нажмите  .



19.2. Серверы аналитики

Чтобы посмотреть в какие роли добавлен пользователь и есть права на каком сервере аналитики,

выберите пользователя, разверните  сервер аналитики.



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