



Руководство

программного обеспечения Domination Management Server

(Центральный сервер управления)

Версия 1.4.0

1. Лицензионное соглашение	2
2. Общие сведения.....	5
2.1. Полное наименование программного обеспечения	5
2.2. Краткое наименование программного обеспечения.....	5
2.3. Термины и сокращения	5
3. Системные требования.....	5
3.1. Минимальные системные требования к ПК	5
3.2. Требование к видеосерверу Domination	5
4. Функциональные характеристики программного обеспечения.....	5
5. Настройка программного обеспечения	6
5.1. Настройка Active Directory для работы с ЦСУ	6
5.2. Создание атрибутов для Active Directory.....	6
5.3. Добавление правил в firewall	13
5.4. Настройка конфигурационного файла appsettings.json	13
5.5. Настройка автоматического входа в Domination Client через Active Directory.....	16
6. Установка программного обеспечения на Windows.....	17
7. Установка программного обеспечения на Linux	19
8. Расположение файлов	21
9. Вход в панель администратора	21
10. Вкладка «Информация»	22
11. Вкладка «Серверы».....	23
11.1. Вкладка «Видеосерверы».....	23
11.2. Вкладка «Серверы аналитики»	24
12. Пользователи.....	25
13. Роли.....	28
14. Политика безопасности	30
14.1. Политика безопасности видеосерверов.....	30
14.2. Политика безопасности серверов аналитики	31
15. Аудит	31
15.1. Аудит видеосерверов.....	31
15.2. Аудит серверов аналитики	32
16. Резервирование	32
17. Логирование действий пользователей	34
17.1. Описание раздела «Логирование»	34
17.2. Фильтрация журнала.....	35
18. Подтверждение событий	35
18.1. Сценарии реагирования	36
18.1.1. Настройка ролей	36
18.1.2. Настройка триггеров	37
18.2. Настройка списка действий	37
18.3. Логирование	38
19. Другое	39



Продукт непрерывно подвергается модернизации с целью улучшения его потребительских свойств. Данное руководство может несколько не соответствовать текущей версии продукта. За последними обновлениями следует обращаться к поставщику или к производителю.

1. Лицензионное соглашение

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

Правообладателем программного продукта **Domination Management Server** (далее «Программа») является **ООО «ВИПАКС+»**, ИНН 5902140005, ОГРН 1025900518181, место нахождения: 115162, г. Москва, вн.тер.г. муниципальный округ Якиманка, ул. Мытная, д.40, к.4, кв. 135.

Правообладатель сохраняет за собой исключительное право на Программу и ее использование в любой форме и любым способом.

Лицензиаром программного продукта **Domination Management Server** является правообладатель, либо юридическое лицо или физическое лицо, которые распространяют программное обеспечение на основе соглашения и лицензии с правообладателем.

Настоящее Лицензионное соглашение действует в течение всего срока эксплуатации Лицензиатом Программы и/или нахождения у него экземпляров Программы. Активируя Программу путем использования материального носителя, на котором установлен экземпляр Программы (далее по тексту – оборудование), Лицензиат признает правила настоящего Лицензионного соглашения.

Действие настоящего Лицензионного соглашения распространяется на все будущие обновления и новые версии Программы. Правообладатель имеет право в любое время вносить изменения в Программу по собственному усмотрению без согласования с Лицензиатом. Устанавливая обновление или новую версию программы, Лицензиат соглашается и принимает условия настоящего Лицензионного соглашения для соответствующих обновлений и новых версий Программы, если такие обновления или новые версии Программы не сопровождаются другим лицензионными соглашением.

Правообладатель оставляет за собой право по собственному усмотрению изменять, дополнять или удалять части условий настоящего соглашения в любое время. Лицензиат несет ответственность за периодическую проверку условий настоящего Лицензионного соглашения на предмет изменений. Каждое использование Программы будет означать, что Лицензиат согласился принять и соблюдать условия настоящего Лицензионного соглашения с внесенными в него поправками и применимыми на данный момент. Правообладатель оставляет за собой право отказать в доступе к Программе любому, кто, по его мнению, нарушил какое-либо из условий настоящего Лицензионного соглашения или по какой-либо причине по своему собственному усмотрению.

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

ИСКЛЮЧИТЕЛЬНЫЕ ПРАВА

Программа защищена действующим законодательством Российской Федерации и международными соглашениями. Все исключительные права на Программу принадлежат правообладателю. При распространении программы обязательно указывается правообладатель, его контактная информация и сайт.

ПРАВА УСТАНОВКИ И ИСПОЛЬЗОВАНИЯ

Лицензиат имеет право устанавливать и использовать Программу на оборудовании:

- при приобретении Программы в комплекте с оборудованием (лицензионные отчисления являются единоразовыми, уплачиваются лицензиару при приобретении материального носителя, либо включено лицензиаром в цену материального носителя);
- при скачивании с сайта Правообладателя, либо с сайта уполномоченного Правообладателем лица (порядок уплаты лицензионных отчислений указывается на сайте).

После активации Программы при начале использования материального носителя (оборудования), на котором установлен экземпляр Программы, Лицензиат получает право использовать Программу без лицензионных отчислений неограниченное время согласно условиям настоящего Лицензионного соглашения.

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 Программу в виде, отличном от того, в котором она была получена Лицензиатом, распространять части программы, ее компоненты отдельно от остальных компонентов Программы;
- 2) изменять, модифицировать, дешифровать, осуществлять любые иные действия с объектным кодом Программы, в том числе с целью получения информации о реализации алгоритмов, используемых в Программе;
- 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) декомпилировать, деассемблировать Программу, дорабатывать Программу, менять что-либо в ней и дополнять ее новыми функциями, исследовать Программу в любых целях и любыми способами, приспособливать Программу своими силами либо силами третьих лиц для обеспечения работоспособности Программы с аппаратными (программным) обеспечением Лицензиата, а равным образом не осуществлять воспроизведение экземпляров Программы;
- 5) осуществлять доступ к информационной базе Программы и построение систем на основе Программы с помощью средств и технологических решений, не предусмотренных в сопроводительной документации;
- 6) создавать на основании Программы или с ее использованием производные произведения;
- 7) совершать действия, результатом которых является устранение или снижение эффективности технических средств защиты исключительных, 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 устранимыми или измененными без разрешения Правообладателя средствами защиты;
- 8) передавать в аренду Программу, продавать, передавать в аренду или иным образом распространять любую копию, модификацию или комбинацию части, компоненты Программы.

Программа может включаться в состав сборников третьих лиц, помещаться на сайтах, отличных от сайта Правообладателя только с письменного согласия Правообладателя.

ОГРАНИЧЕНИЕ ГАРАНТИЙНЫХ ОБЯЗАТЕЛЬСТВ

Программа предоставляется Лицензиату «как есть» (as is) в соответствии с общепринятым в международной коммерческой практике принципом. Это означает, что за проблемы, возникающие в процессе установки, обновления, поддержки и эксплуатации Программы (в т. ч. проблемы совместимости с другими программными продуктами (пакетами, драйверами и др.), несоответствия результатов использования Программы ожиданиям Лицензиата и т.п.) Правообладатель ответственности не несет, равным образом Правообладатель не обязан предоставлять Лицензиату исправления, дополнения, новые версии Программы и (или) обеспечивать функционирование Программы с аппаратным (программным) обеспечением Лицензиата. Лицензиат принимает и соглашается с тем, что он несет полную ответственность за возможные негативные последствия, вызванные несовместимостью или конфликтами Программы с другими программными продуктами. 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 письменно заявленных и предполагаемых по умолчанию гарантийных обязательств, включая ограничения в применении гарантийных обязательств после определенного срока и годности Программы к продаже. Правообладатель не несет ответственности за отсутствие доступа к Программе, технические сбои и перерывы в работе Программы, вызванные неполадками используемых технических средств, иные аналогичные сбои, а также вызванные неполадками оборудования, компьютерного оборудования, которое Лицензиат использовал для работы с Программой, вызванные действиями третьих лиц, перебоями связи, электричества, иных ресурсов, необходимых для функционирования Программы. Ни при каких обстоятельствах Правообладатель не несет обязательств перед Лицензиатом 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 претензии, иски на любые другие имущественные требования Лицензиата.

ПРОЧИЕ УСЛОВИЯ

Настоящее Лицензионное соглашение соответствует действующим законодательством Российской Федерации и международными соглашениями. Все спорные вопросы решаются по взаимной договоренности сторон, а если соглашение не было достигнуто, то в судебном порядке в порядке, предусмотренном действующим законодательством Российской Федерации.

КОНТАКТНАЯ ИНФОРМАЦИЯ:

Правообладатель: **ООО «ВИПАКС+»**

ИНН 5902140005 ОГРН 1025900518181,

Место нахождения: 115162, г. Москва, вн.тер.г. муниципальный округ Якиманка, ул. Мытная, д.40, к.4, кв. 135
тел. 8-800-700-20-95

info@vipaks.com

<https://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 11, Windows Server 2012-2022, Astra Linux 1.7.2 и выше, Debian 12, 13.

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 2.15 и выше.

При использовании сервера аналитики: версия 1.12 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) резервирование 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. Настройка программного обеспечения

5.1. 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.

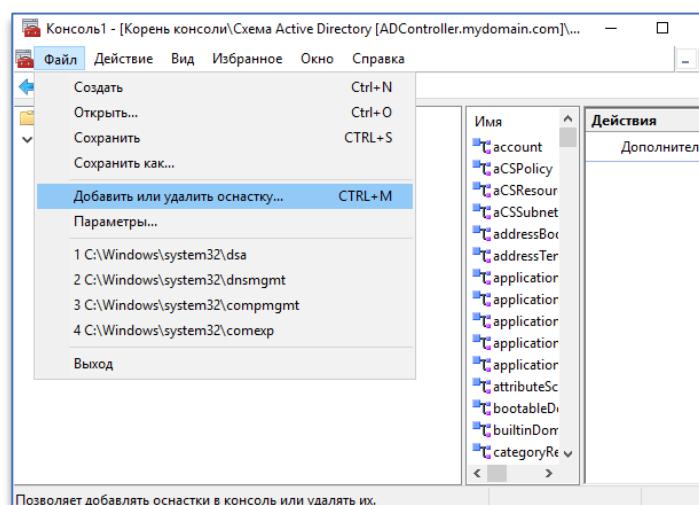
5.2. Создание атрибутов для Active Directory

Выполнить в cmd.exe команды:

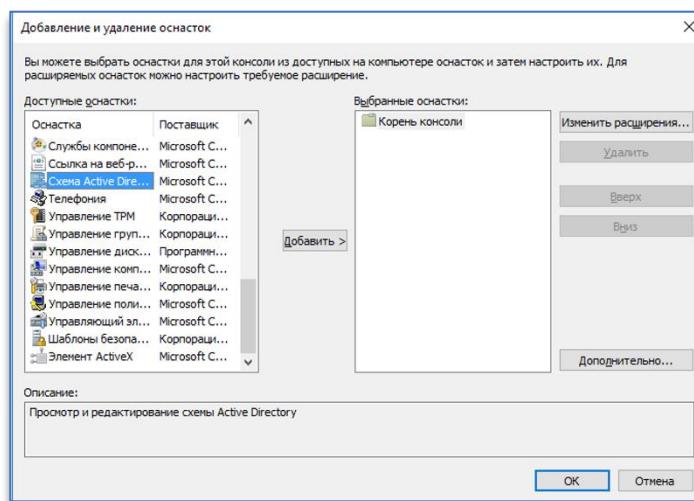
regsvr32 schmmgmt.dll

mmc

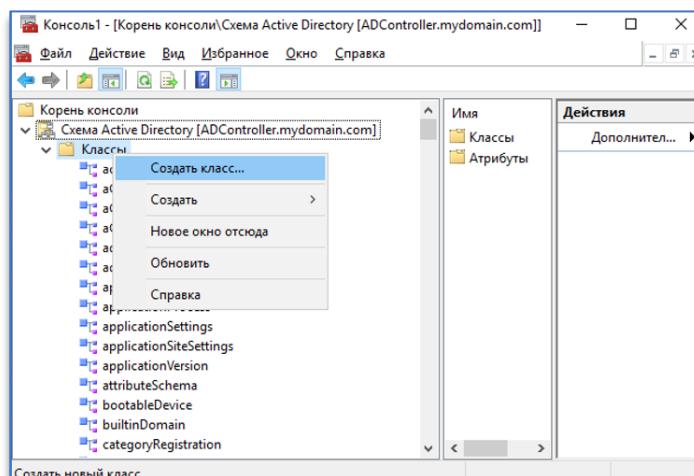
В открывшемся окне «Консоль1 – Корень консоли» выбрать «Файл» – «Добавить или удалить оснастку».



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



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

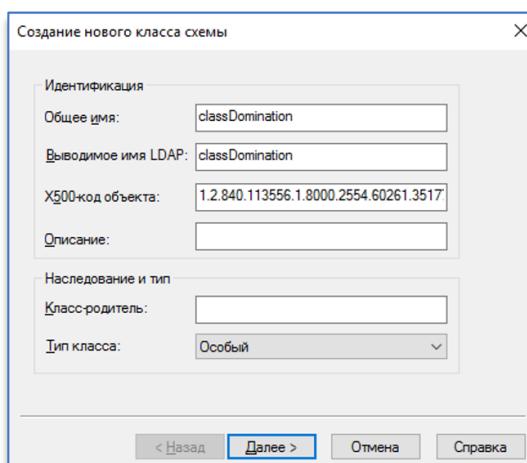


В окне «Создание нового класса схемы» необходимо ввести следующие данные:

Общее имя: *classDomination*

X500-код объекта: *1.2.840.113556.1.8000.2554.60261.35177.16306.19442.40185.2384456.12562999.1.1*

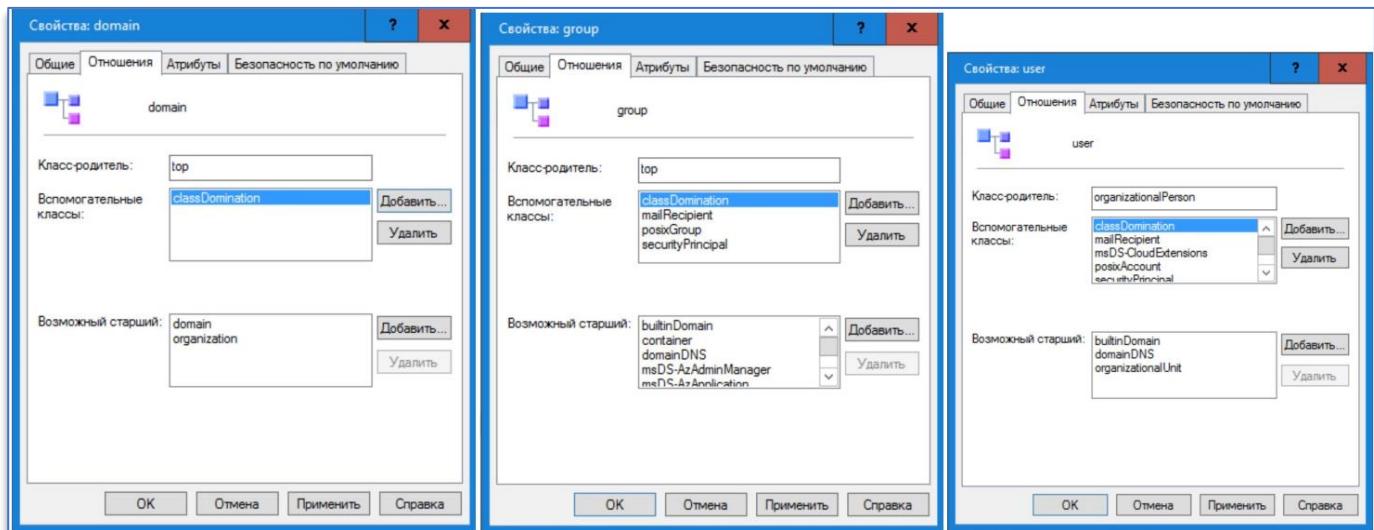
Тип класса: Особый



Нажать «Далее», затем «Готово».

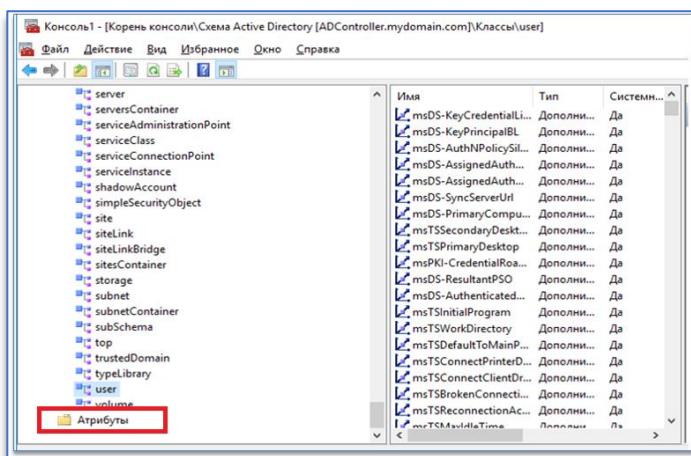
В списке «Классы» у классов «domain», «user» и «group»:

- 1) через ПКМ выбрать «Свойства»;
- 2) на вкладке «Отношения» напротив списка «Вспомогательные классы» нажать «Добавить...»;
- 3) выбрать созданный ранее класс «classDomination»;
- 4) нажать «OK».



- Атрибут «DomAuthServer».

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



В окне «Создание нового атрибута» ввести следующие данные:

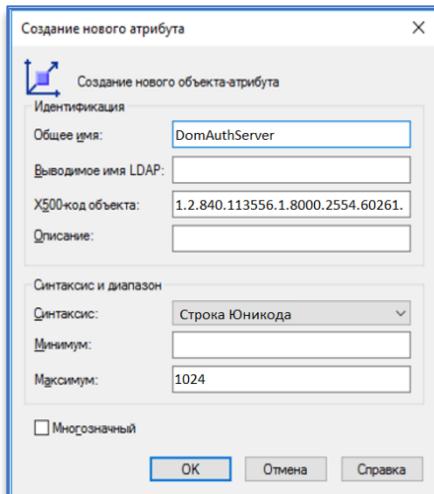
Общее имя: DomAuthServer

X500-код объекта: 1.2.840.113556.1.8000.2554.60261.35177.16306.19442.40185.2384456.12562999.2.1

Синтаксис: Стока Юникода

Максимум: 1024

Многозначчный: 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: Стока Юникода

Максимум: *4096*

Многозначный: Да

! Обязательно нужно поставить отметку в чекбоксе «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: Стока Юникода

Максимум: *4096*

Многозначный: Да

! Обязательно нужно поставить отметку в чекбоксе «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: Стока 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: Стока Юникода

Максимум: 4096

Многозначный: Нет

Для сохранения данных нажать на кнопку «OK».

- 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: Стока Юникода

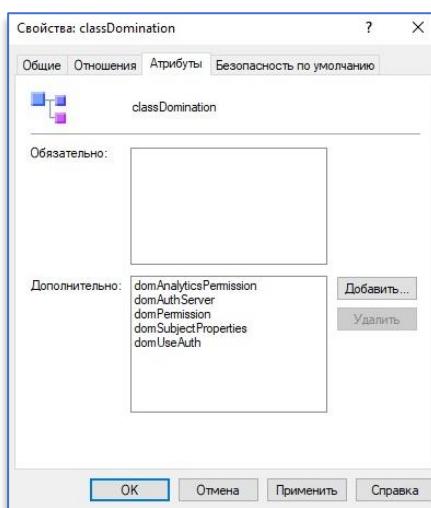
Максимум: 1024

Многозначный: Нет

Для сохранения данных нажать на кнопку «OK».

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 «OK» и перезагрузить сервер для применения изменений.

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

The screenshot shows the Windows Server Active Directory management console. The left navigation pane shows 'Пользователи и компьютеры Active Direct...' and 'Сохраненные запросы'. The main pane is titled 'Пользователи' and shows the 'Users' folder expanded. It lists numerous user accounts and groups, each with a 'Имя' (Name), 'Тип' (Type), and 'Описание' (Description). Some examples include 'Ivan Ivanov' (User, Global), 'domination' (User, Global), 'Protected Users' (Group, Global), and various security groups like 'Administrators' and 'Guests'.

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

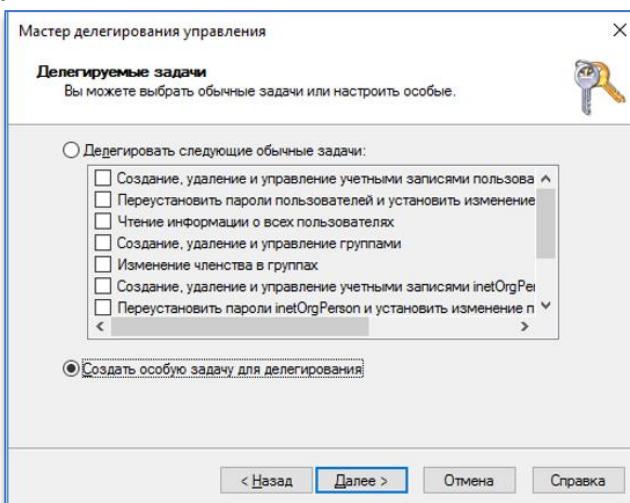
Через ПКМ выбрать «**Делегирование управления**», в открывшемся окне нажать «**Добавить...**».

The screenshot shows the 'Delegate management' wizard. The current step is 'Пользователи или группы' (Select users or groups). It displays a list of selected users and groups in the 'Выбранные пользователи и группы:' (Selected users and groups:) list box. Below the list are 'Добавить...' (Add...) and 'Удалить' (Delete) buttons. At the bottom are navigation buttons: '< Назад' (Back), 'Далее >', 'Отмена' (Cancel), and 'Справка' (Help).

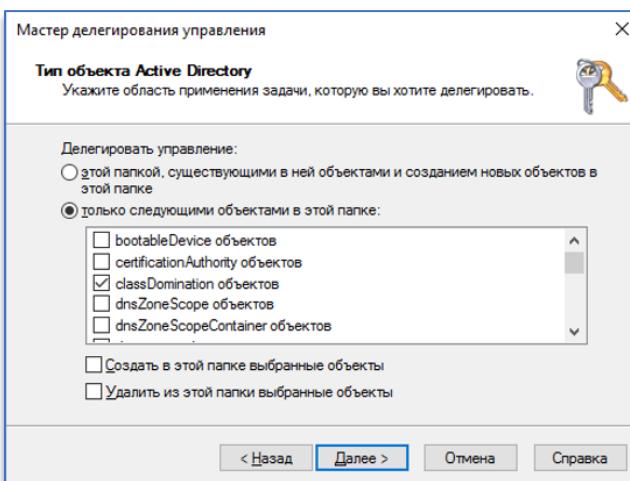
Вписать в поле имя «**Сервисного пользователя**» ЦСУ (если пользователь не создан, то создать пользователя домена; его название может быть произвольным, например: «`dominationServiceAccount`»). В примере это пользователь «`ubuntuuser`». Далее нажать «**OK**».

The screenshot shows the 'Выбор: "Пользователи", "Компьютеры" или "Группы"' (Select: "Users", "Computers" or "Groups") dialog. It has fields for 'Выберите тип объекта:' (Select object type:), 'В следующем месте:' (In the following place:), and 'Ведите имена выбираемых объектов (примеры):' (Enter names of selected objects (examples:)). The 'Selected objects' list box contains 'ubuntuuser (ubuntuuser@mydomain.com)'. At the bottom are 'Дополнительно...' (Advanced...), 'OK', and 'Отмена' (Cancel) buttons.

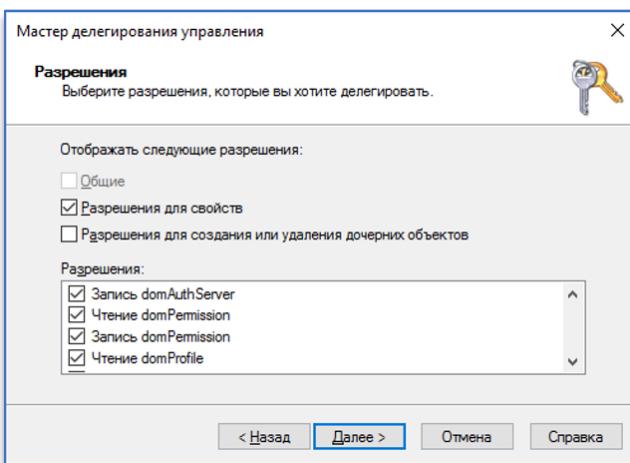
В окне «Мастер делегирования управления» в пункте «Делегируемые задачи» выбрать «Создать особую задачу для делегирования», нажать «Далее».



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



В следующем окне нужно отметить в чекбоксе пункт «Разрешения для свойств», также установить отметки в чекбоксах 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.

5.3. 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`

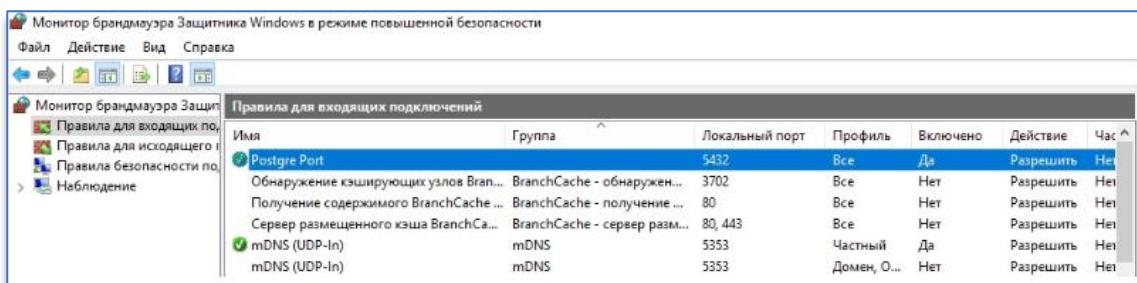
`netsh advfirewall firewall add rule name="ЦСУ Port" dir=in action=allow protocol=TCP localport=8001`

Где:

rule name – имя правила,

localport – разрешенный порт.

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



5.4. 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.

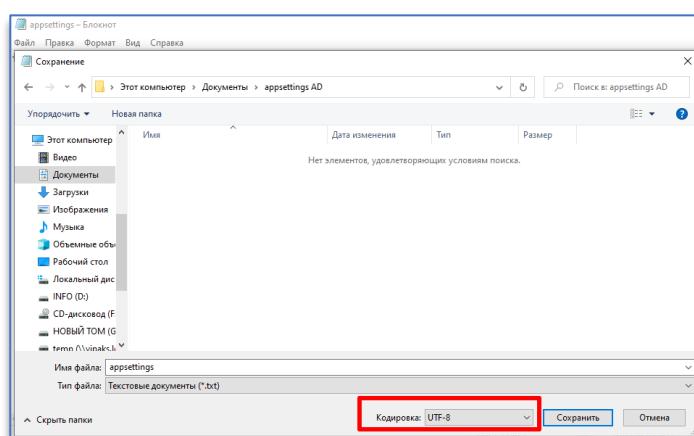
```
"ElasticConfiguration": {
  "Uri": "http://localhost:9200"
}
```

Секция настройки сервиса Swagger.

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



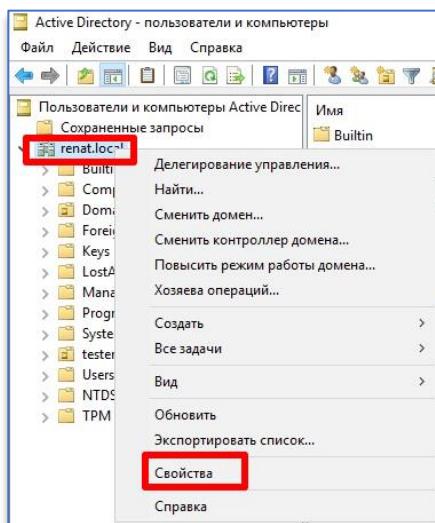
Файл конфигурации **appsettings.json** необходимо сохранять в кодировке UTF-8.



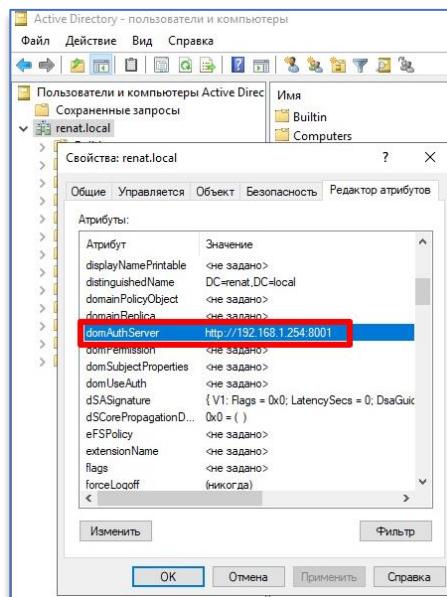
5.5. Настройка автоматического входа в Domination Client через Active Directory

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

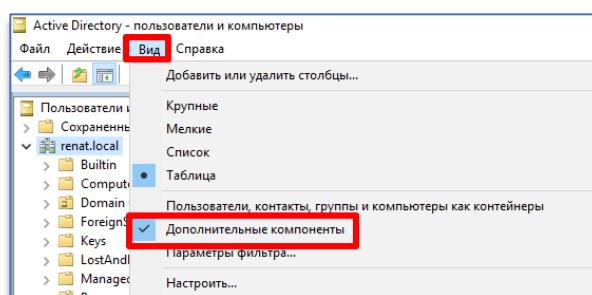
1. Зайти в «Active Directory – пользователи и компьютеры». Через ПКМ по названию домена выбрать «Свойства».



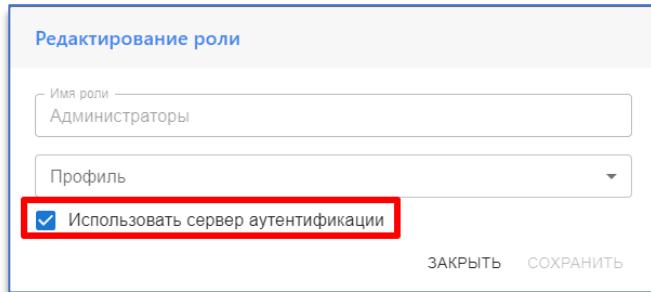
2. Во вкладке «Редактор атрибутов» найти атрибут «domAuthServer» и прописать IP-адрес ЦСУ.



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 отметку в чекбоксе напротив «Использовать сервер аутентификации».



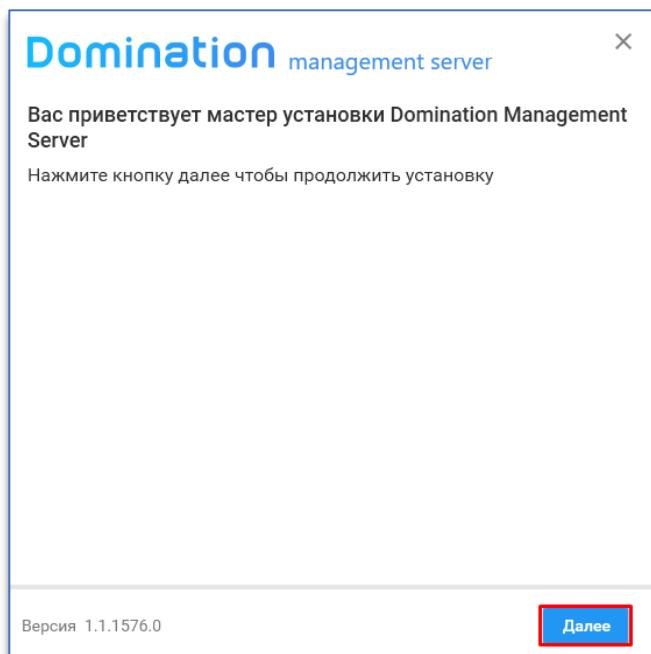
Добавление пользователя и роли в ЦСУ производится через Active Directory.

6. Установка программного обеспечения на Windows

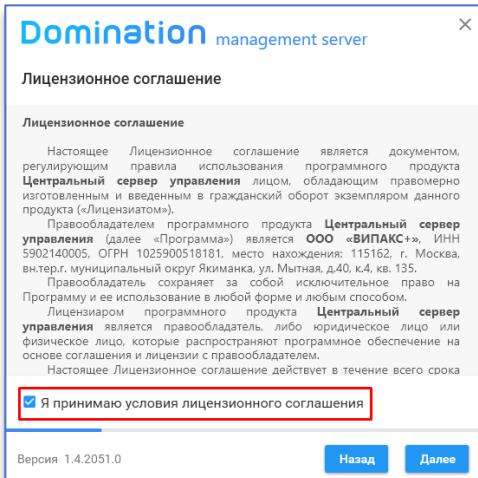
Для установки ЦСУ необходимо:

1. Скачать дистрибутив по ссылке:
<https://vipaks.com/support/download/domination-management-server/>
2. Распаковать полученный архив.
3. Запустить файл установки **Domination Management Server**.

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

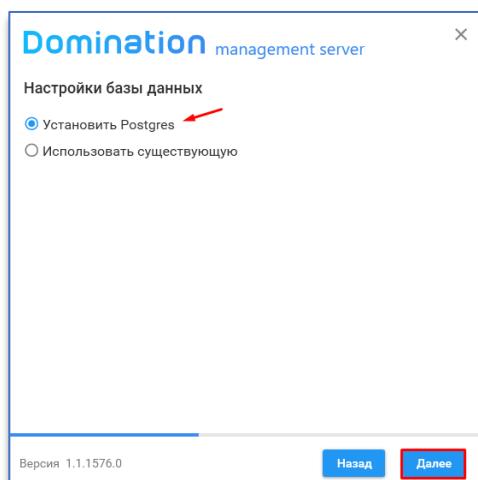


После этого потребуется ознакомиться и принять условия лицензионного соглашения, потом нажать «Далее».

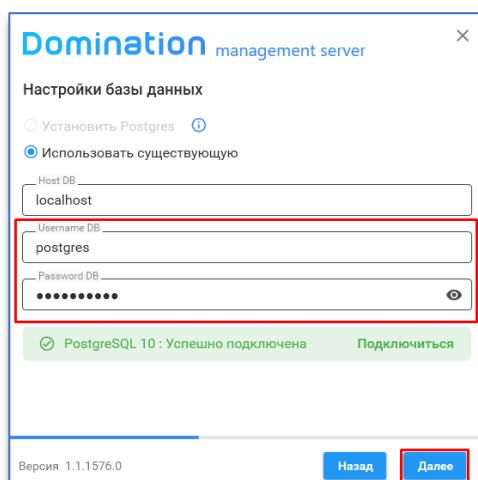


Дальнейшие действия по установке будут зависеть от того, установлена или нет база данных PostgreSQL на компьютере.

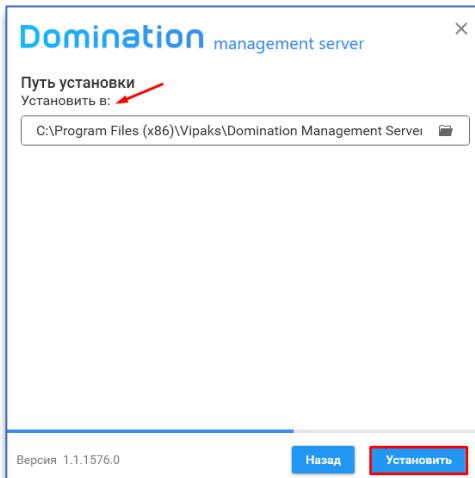
В случае если база данных Postgresl не установлена на компьютере, необходимо выбрать пункт «**Установить Postgres**» и нажать «Далее».



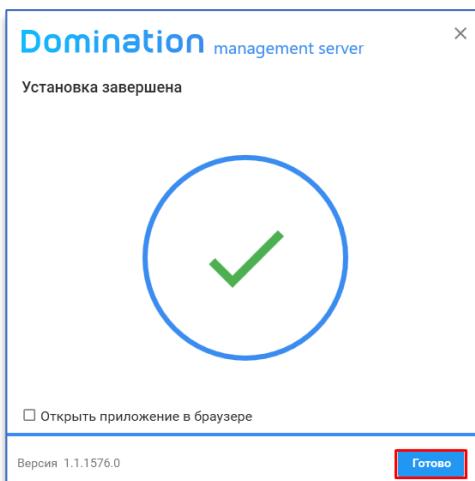
В случае если база данных Postgresl уже установлена на компьютере, необходимо выбрать пункт «**Использовать существующую**», ввести учётные данные и нажать «Далее».



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



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



При необходимости можно установить отметку в чекбоксе «Открыть приложение в браузере». В этом случае панель администратора ЦСУ откроется в web-браузере.

7. Установка программного обеспечения 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/>.....».

The screenshot shows a terminal window titled 'sudo mc - Терминал Fly'. The window has a menu bar 'Файл Правка Настройка Справка' and a toolbar with icons for file operations. The main area is a terminal window with the command 'GNU nano 3.2' and the file path '/etc/apt/sources.list'. The content of the file is as follows:

```

# Astra Linux repository description https://wiki.astralinux.ru/x/0oLiC
#deb cdrom:[OS Astra Linux 1.7.2 1.7_x86-64 DVD 1/ 1.7_x86-64 contrib main non-free
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-main/ 1.7_x86-64 main con$deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-update/ 1.7_x86-64 main c$deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-base/ 1.7_x86-64 main con$deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-extended/ 1.7_x86-64 main c$
```

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 &&`

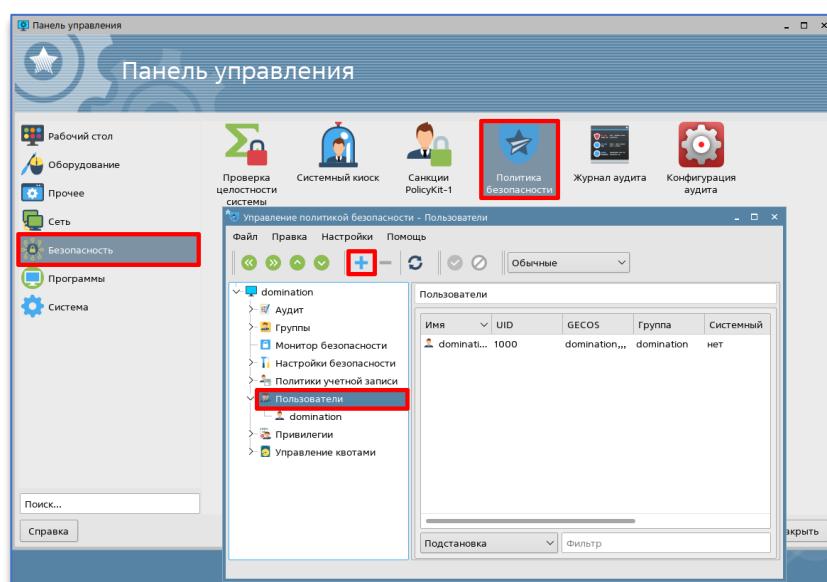
`sudo setfacl -d -m u:postgres:r /etc/parsec/capdb &&`

`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 .



 При установке на ОС Astra Linux 1.7.6/1.8 и выше необходимо настроить новому пользователю максимальный уровень целостности для работы в базе данных. Для этого требуется:

- для пользователя «enterprise» прописать команду:
`sudo pdpl-user -i 63 enterprise`
- для пользователя «postgres» прописать команду:
`sudo pdpl-user -i 63 postgres`

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

8. 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».

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.

Центральный сервер управления

Информация Серверы Пользователи Роли Политика безопасности Аудит Резервирование

Информация о лицензии (демо режим) !

Максимальное число каналов	16
Используемое кол-во каналов	0
Максимальное число зарезервированных каналов	1
Мониторинг действий пользователей	Нет

Подключенные пользователи

Необходимо вставить аппаратный USB-ключ защиты в USB-порт компьютера, на котором установлен ЦСУ.

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.

Центральный сервер управления

Информация Серверы Пользователи Роли

Информация о лицензии

Максимальное число каналов	200
Используемое кол-во каналов	0
Максимальное число зарезервированных каналов	200

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

Подключенные пользователи Поиск

Иванов Иван
0.204

11. Вкладка «Серверы»

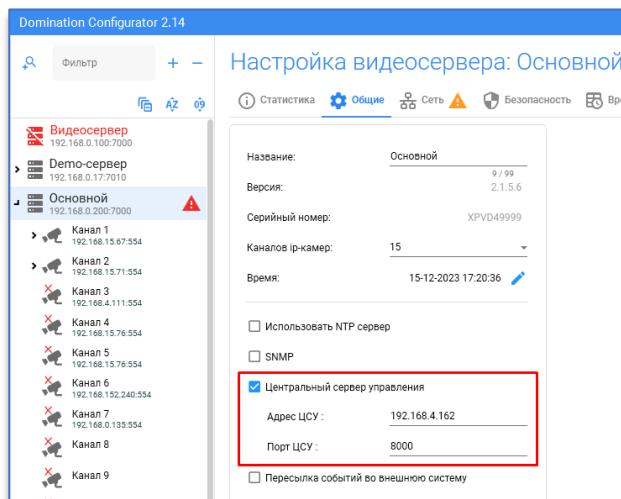
На вкладке «Серверы» можно управлять видеосерверами и серверами аналитики.

11.1. Вкладка «Видеосерверы»

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

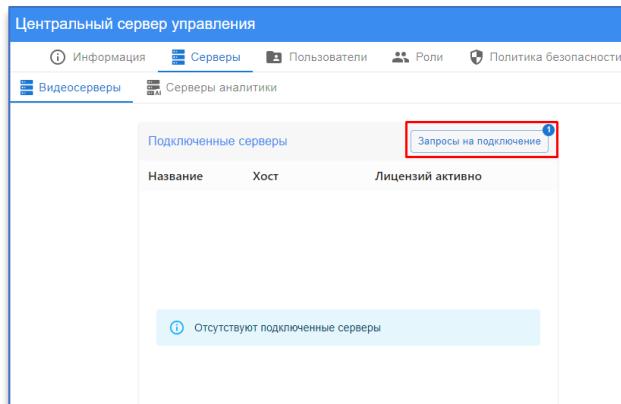
Для добавления видеосервера в ЦСУ нужно сначала перейти в Конфигуратор видеосервера и выполнить его настройку:

- 1) добавить или выбрать видеосервер, работа с которым планируется через ЦСУ;
- 2) на вкладке «Общие» установить отметку в чекбоксе 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.

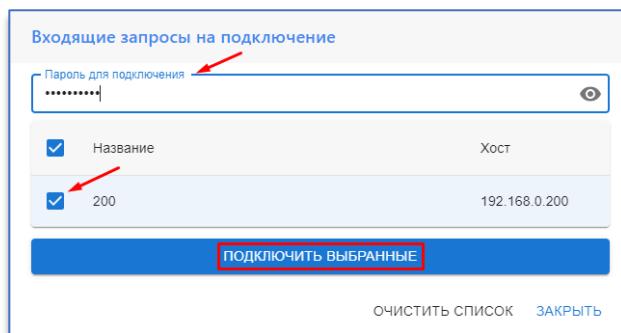


После этого в ЦСУ придёт запрос на подключение выбранного видеосервера.

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

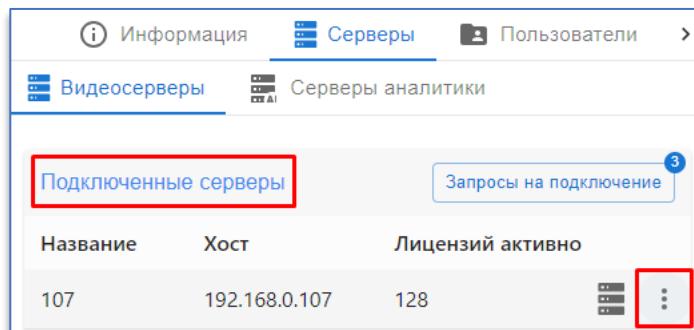


Далее нужно выбрать в списке видеосервер, ввести пароль для подключения и нажать на кнопку «Подключить выбранные».



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

После подключения видеосервер отобразится в разделе «Подключенные серверы».



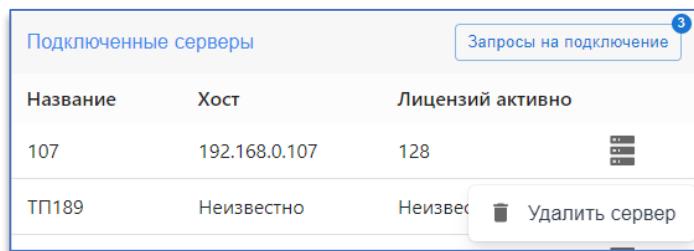
Информация Серверы Пользователи >

Видеосерверы Серверы аналитики

Подключенные серверы Запросы на подключение 3

Название	Хост	Лицензий активно
107	192.168.0.107	128

Чтобы удалить сервер нужно навести курсор мыши на нужный видеосервер и нажать на кнопку . В открывшемся меню выбрать «Удалить сервер».



Подключенные серверы Запросы на подключение 3

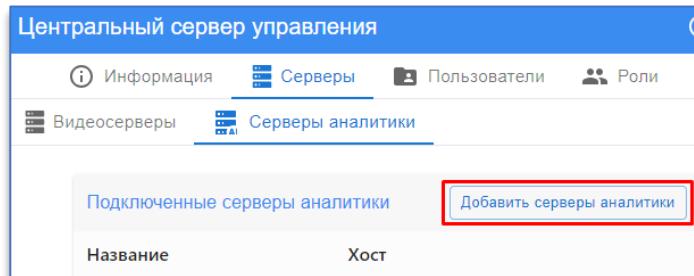
Название	Хост	Лицензий активно
107	192.168.0.107	128
TP189	Неизвестно	Неизвестно

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».



Центральный сервер управления

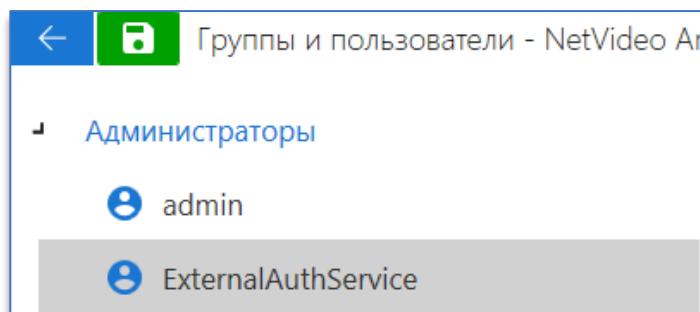
Информация Серверы Пользователи Роли

Видеосерверы Серверы аналитики

Подключенные серверы аналитики Добавить серверы аналитики 3

Название	Хост
----------	------

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



Группы и пользователи - NetVideo Admin

Администраторы

admin

ExternalAuthService

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 нажать 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, необходимо нажать 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.

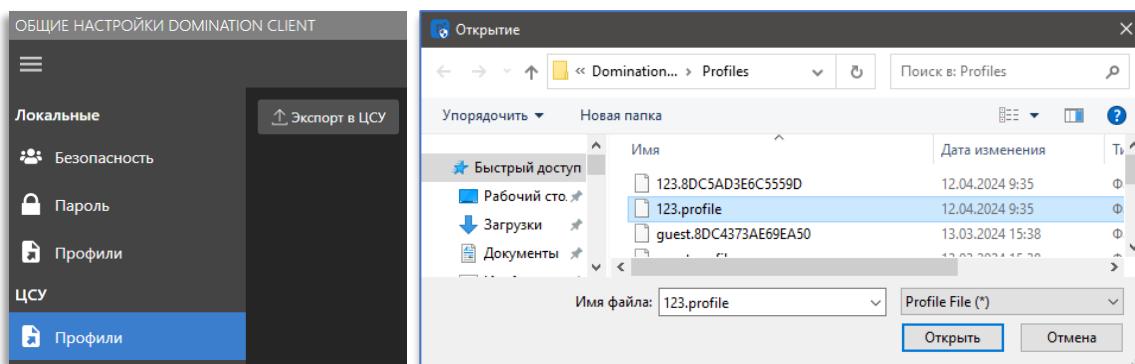
В поле «Профиль» можно указать заранее настроенный профиль, который будет использоваться при открытии клиента Domination (Domination Client).

Чтобы экспорттировать настроенный профиль в ЦСУ, необходимо:

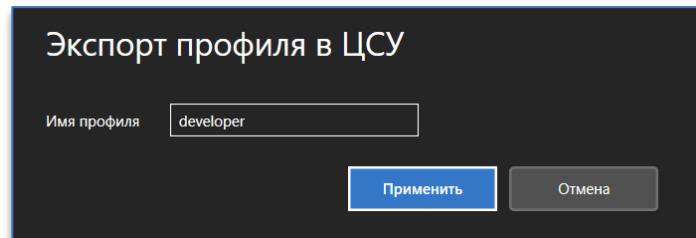
1. Зайти в «Общие настройки» Domination Client, выбрать «Профили», выделить нужный профиль пользователя и нажать на кнопку «Экспорт».

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

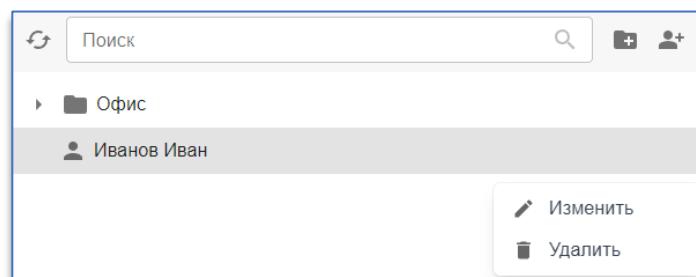
4. После успешного подключения к ЦСУ нажать на кнопку «Экспорт в ЦСУ», выбрать нужный профиль и нажать «Открыть».



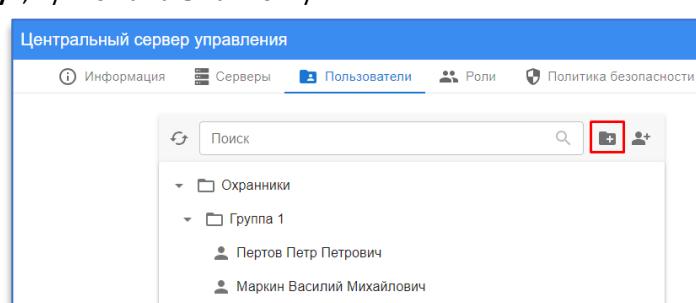
5. При необходимости можно изменить имя профиля и нажать «Применить».



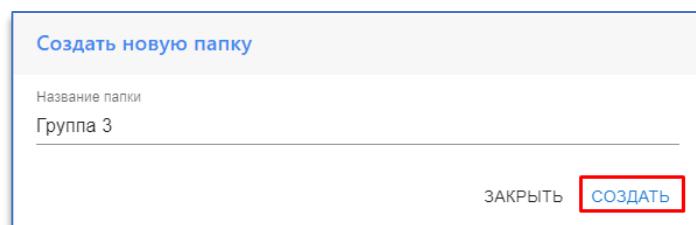
Чтобы «Изменить» или «Удалить» пользователя, нужно навести курсор на нужного пользователя и нажать .



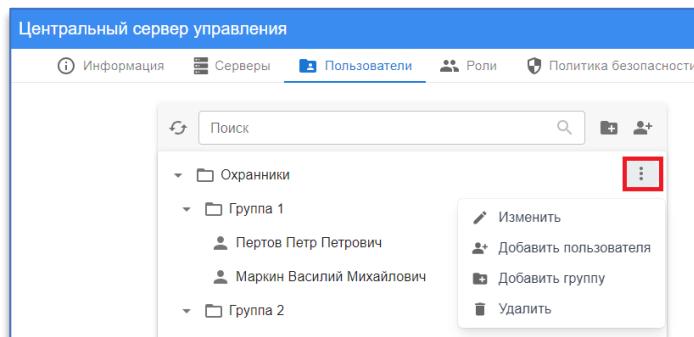
Чтобы создать «Группу», нужно нажать на кнопку .



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



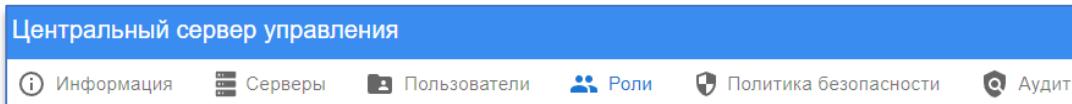
Чтобы «Изменить» название группы, «Добавить пользователя» в группу, «Добавить группу» и «Удалить» группу, нужно навести курсор мыши на нужную группу и нажать  , откроется меню, из которого необходимо выбрать нужное действие.



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

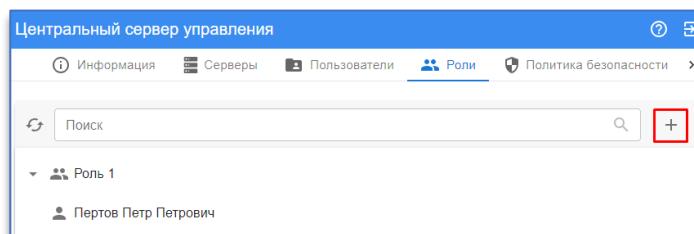
Роли позволяют группировать пользователей по общей принадлежности к одной категории для более удобной и единовременной настройки политики безопасности выбранных групп.



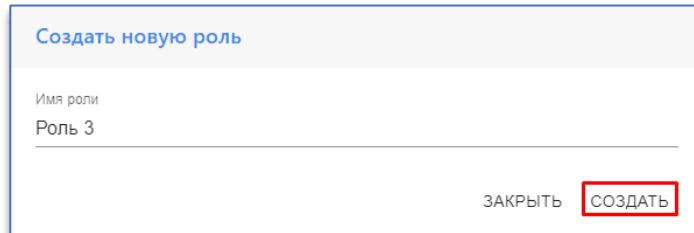
На вкладке «Роли» можно управлять ролями пользователей:

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

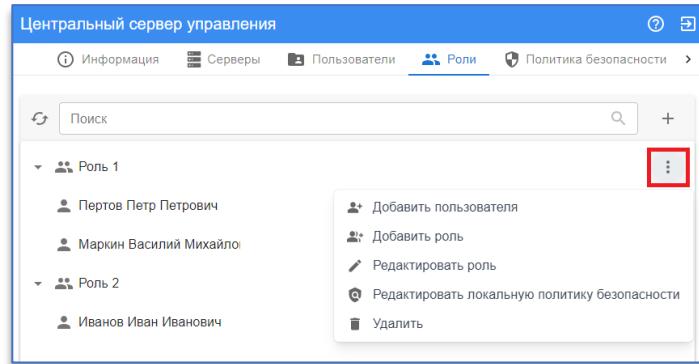
Чтобы добавить новую роль, нужно нажать на кнопку .



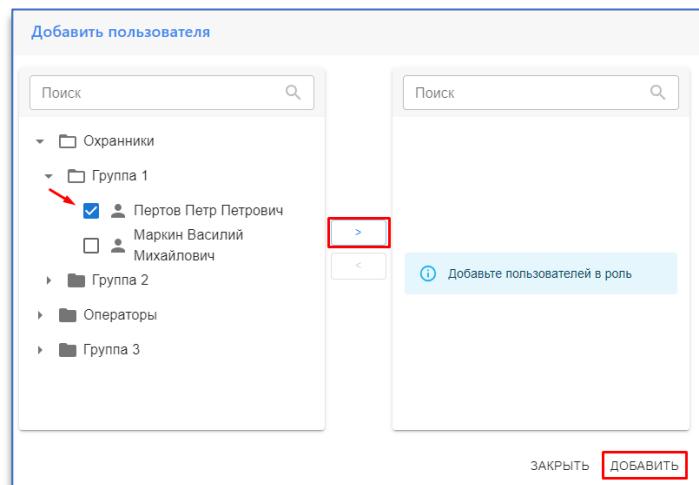
Откроется окно создания новой роли. Необходимо указать имя роли и нажать на кнопку «Создать».



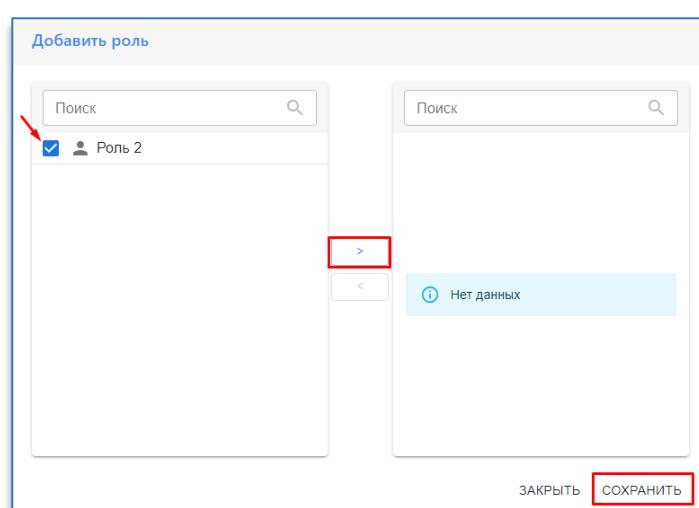
Чтобы «Добавить пользователя», «Добавить роль», «Редактировать роль», «Редактировать локальную политику безопасности» и «Удалить» роль, требуется навести курсором мыши на нужную роль и нажать  , откроется меню, из которого необходимо выбрать нужное действие.



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».



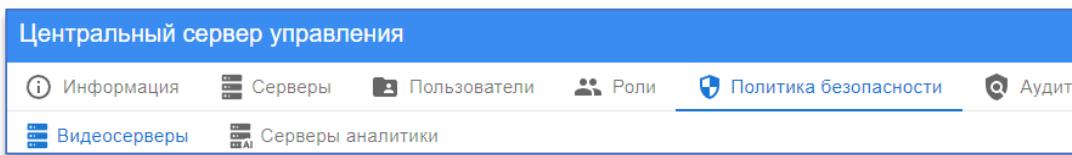
Редактирование локальной политики безопасности относится к правам роли пользователя в клиенте Domination («Domination Client»).

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 отметку в чекбоксе в необходимом пункте.

Роли	Полик	Поиск	Объект	Подключение	Настройка	Архив	Управление	Звук подключение	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"/>					
			Канал 2	<input checked="" type="checkbox"/>					
			Канал 3	<input checked="" type="checkbox"/>					
			Канал 4	<input checked="" type="checkbox"/>					
			Канал 5	<input checked="" type="checkbox"/>					

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.

Доступ до реакций — 1 +

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

Ограничение трафика, Мбит/сек. 100

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.

Серверы	Ур. доступа
NetVideo Analytics Server	Operator

15. Аудит

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

15.1. Аудит видеосерверов

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.

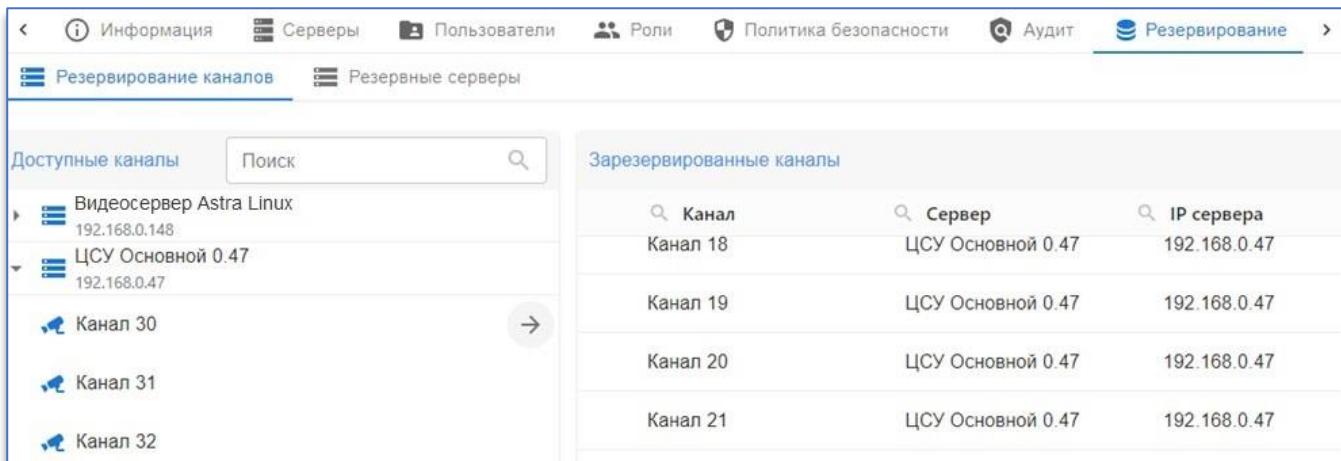
16. Резервирование

На вкладке «Резервирование» можно настроить резервирование каналов видеосерверов.

В случае если сервер отключится или станет недоступен, ЦСУ перенаправит запись каналов на другой видеосервер, указанный в настройках как резервный. Как только основной сервер будет восстановлен, ЦСУ переключит запись каналов с резервного сервера на основной.

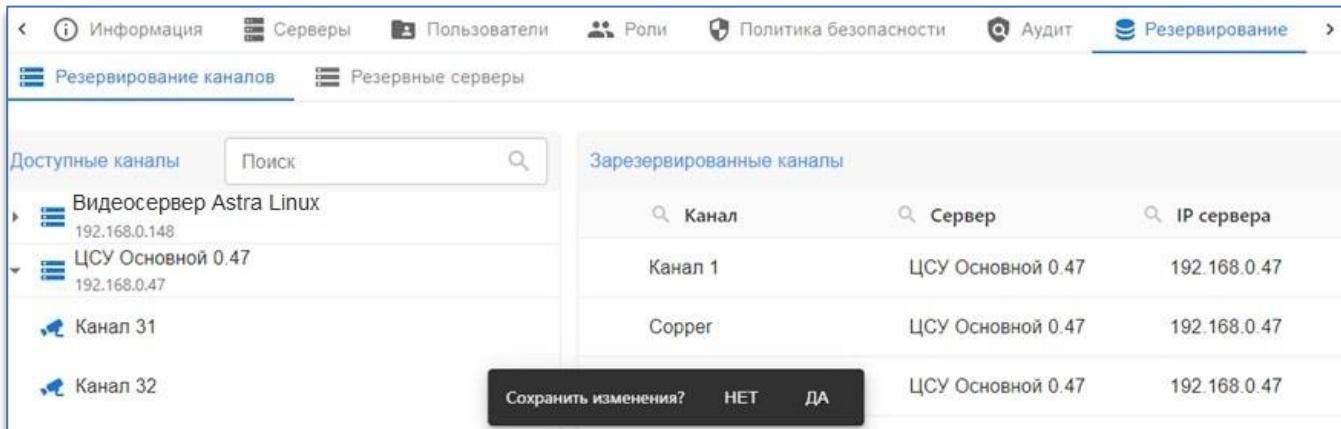
Для того чтобы настроить резервное копирование, необходимо:

- 1) в подразделе «Резервирование каналов» в столбце «Доступные каналы» выбрать видеосервер и канал (или несколько каналов), по которым необходимо будет вести резервное копирование, и нажать на кнопку . Каналы переместятся в столбец «Зарезервированные каналы»:



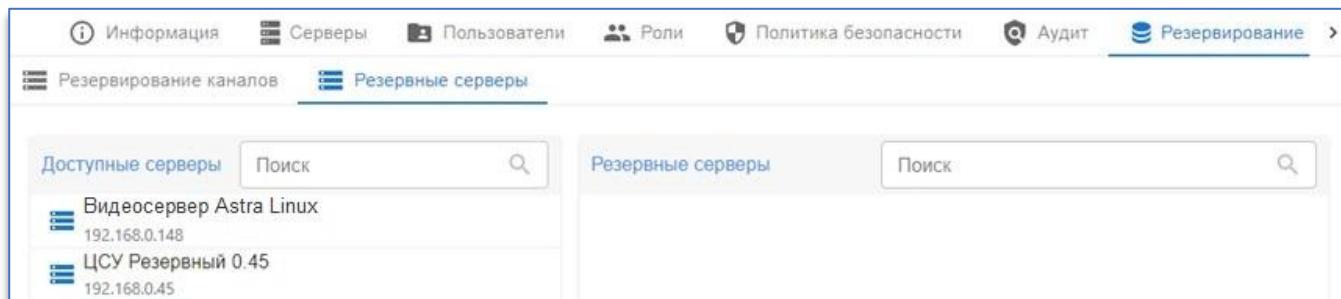
Скриншот страницы «Резервирование каналов». В левой колонке «Доступные каналы» перечислены «Видеосервер Astra Linux 192.168.0.148» и «ЦСУ Основной 0.47 192.168.0.47». В правой колонке «Зарезервированные каналы» перечислены «Канал 18» («Сервер ЦСУ Основной 0.47»), «Канал 19» («Сервер ЦСУ Основной 0.47»), «Канал 20» («Сервер ЦСУ Основной 0.47») и «Канал 21» («Сервер ЦСУ Основной 0.47»). Кнопка  расположена между колонками.

- 2) сохранить изменения, нажав на кнопку «Да» во всплывающем окне:



Скриншот страницы «Резервирование каналов» с всплывающим диалогом «Сохранить изменения?». В диалоге присутствуют кнопки «НЕТ» и «ДА». В правой колонке «Зарезервированные каналы» перечислены «Канал 1» («Сервер ЦСУ Основной 0.47»), «Copper» («Сервер ЦСУ Основной 0.47») и «ЦСУ Основной 0.47 192.168.0.47».

- 3) в подразделе «Резервные серверы» из столбца «Доступные серверы» выбрать видеосервер, на который будет вестись резервное копирование, и нажать на кнопку . Видеосервер переместится в столбец «Резервные серверы»:



Скриншот страницы «Резервирование серверов». В левой колонке «Доступные серверы» перечислены «Видеосервер Astra Linux 192.168.0.148» и «ЦСУ Резервный 0.45 192.168.0.45». В правой колонке «Резервные серверы» перечислен «ЦСУ Резервный 0.45 192.168.0.45». Кнопка  расположена между колонками.

4) сохранить изменения, нажав на кнопку «Да» во всплывающем окне.

Чтобы пользователь мог смотреть записи на резервном видеосервере, ему нужно выдать права на просмотр каналов резервного видеосервера (см. раздел «[Политика безопасности](#)»).

17. Логирование действий пользователей

17.1. 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.

Время	Пользователь	IP пользователя	Сервер	Событие
15.12.23 / 15:26:01	User	DEVELOPERDOM28	200	Пользователь сохранил снимок с канала "H265" (15.12.23 / 15:26:01)
15.12.23 / 15:26:05	User	192.168.4.162	200	Просмотр каналов в реальном времени
15.12.23 / 15:26:13	User	192.168.4.162	200	Просмотр каналов в режиме архива

 The search and filter fields at the top are set to 'Время начала: 15.12.2023 00:00' and 'Конечное время: 15.12.2023 15:27'."/>

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.

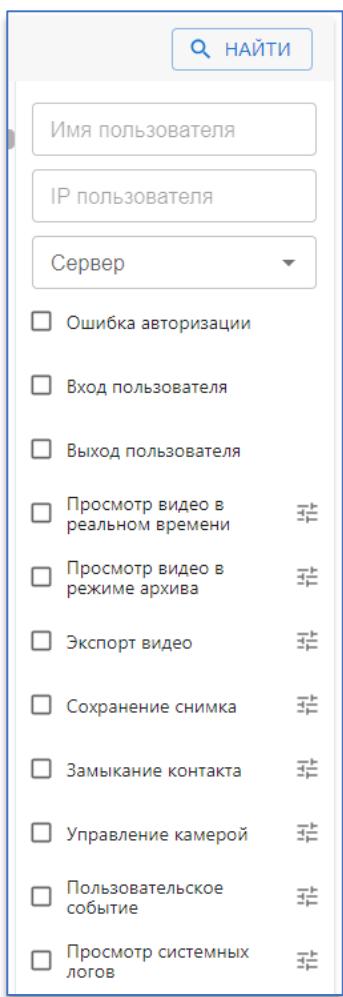
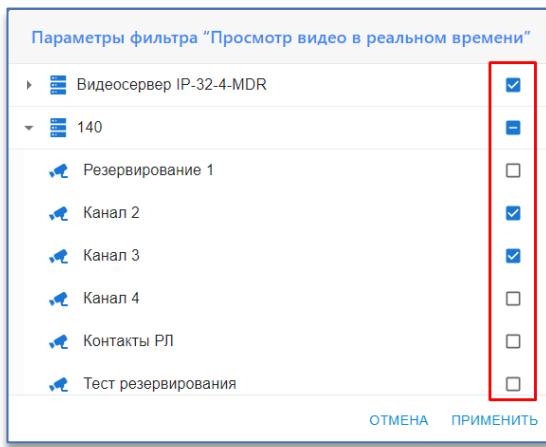
17.2. Фильтрация журнала

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.

18. 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.

Функцию «Подтверждение событий» можно настроить для следующих модулей видеоаналитики:

- «Вторжение в зону»,
- «Детектор громкого звука»,
- «Детектор дыма»,

- «Детектор жестов»,
- «Детектор касок»,
- «Детектор огня»,
- «Детектор периметра и пересечение линии»,
- «Детектор праздношатания»,
- «Детектор применения СИЗ»,
- «Детектор саботажа»,
- «Детектор скрытого лица»,
- «Детектор спецодежды»,
- «Детектор человека»,
- «Классификатор объектов»,
- «Контроль активности оборудования»,
- «Контроль наличия маски»,
- «Контроль объёмов»,
- «Контроль опасной зоны»,
- «Контроль скорости и направления»,
- «Контроль технологической планировки»,
- «Мультикамерный подсчёт объектов» (для одного канала),
- «Оставленные предметы»,
- «Подсчёт посетителей».

18.1. 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 .

18.1.1. Настройка ролей

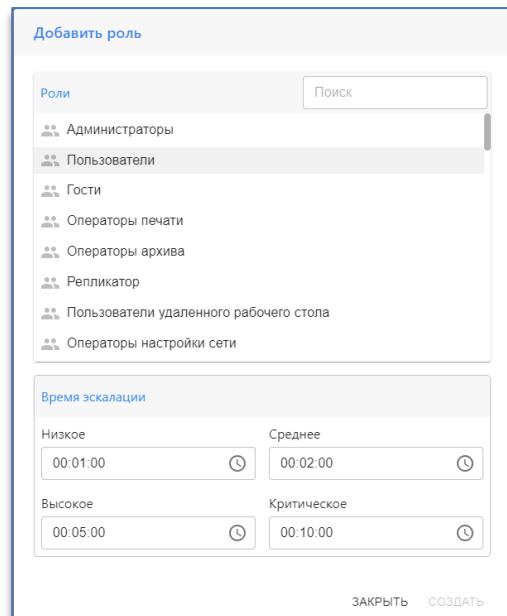
Роли необходимы для того, чтобы обозначить, какой группе операторов будет поступать событие на обработку.

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 вверху списка.



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

18.1.2. 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 присыпать 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.

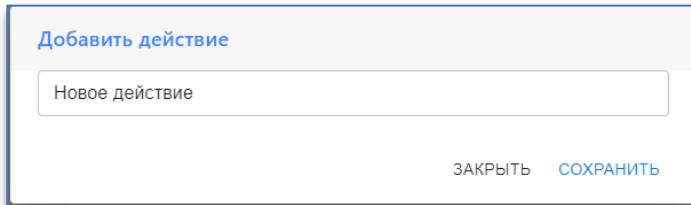
«Список действий» – позволяет выбрать список действий, который поступит оператору при срабатывании события.

Для завершения и сохранения настройки необходимо нажать кнопку .

18.2. 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  . Далее выбрать созданный список действий, нажав по его названию левой кнопкой мыши. После чего справа станет доступна кнопка  , с её помощью можно добавлять действия в список.



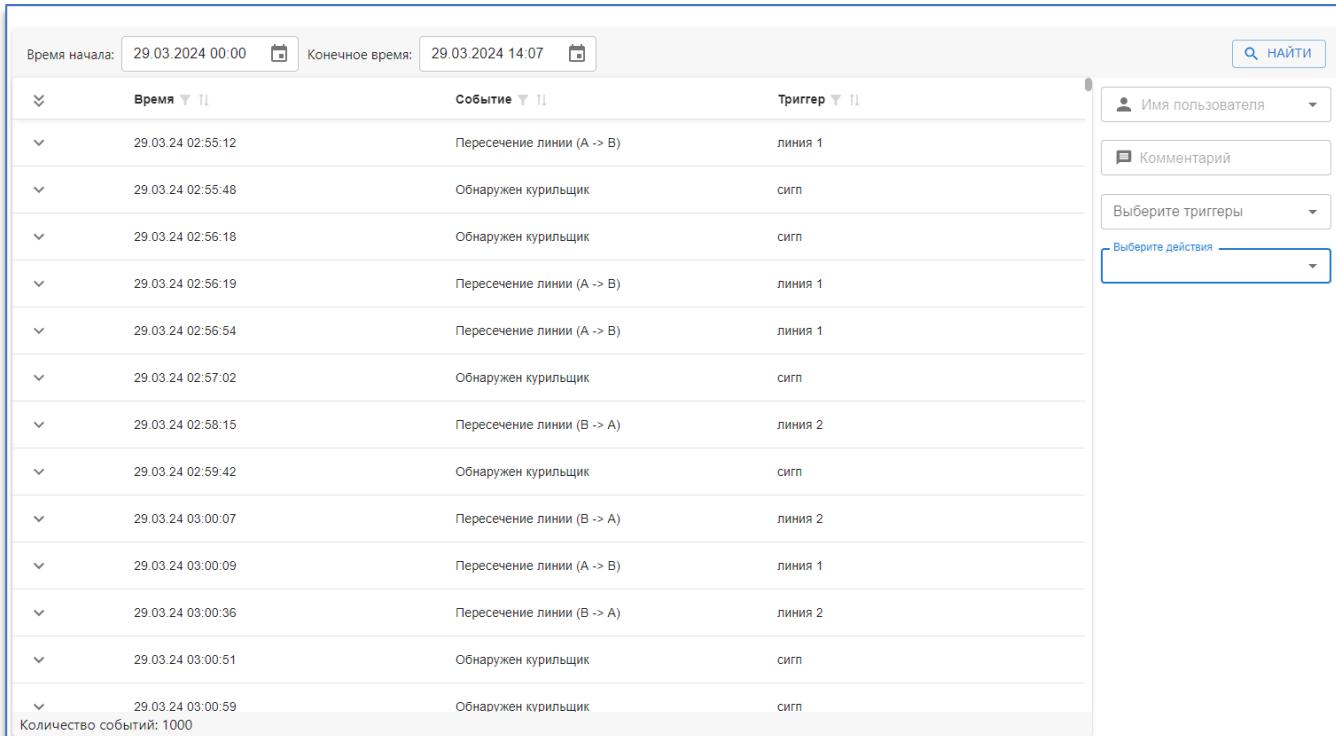
Редактировать или удалять созданные списки можно с помощью кнопки  , которая становится активной при наведении курсора мыши на строку с названием списка.

18.3. 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 событие;
- комментарий;
- триггер;
- действие оператора.



Время начала: 29.03.2024 00:00 Конечное время: 29.03.2024 14:07

Найти

Время Событие Триггер

29.03.24 02:55:12 Пересечение линии (A -> B) линия 1

29.03.24 02:55:48 Обнаружен курильщик сигп

29.03.24 02:56:18 Обнаружен курильщик сигп

29.03.24 02:56:19 Пересечение линии (A -> B) линия 1

29.03.24 02:56:54 Пересечение линии (A -> B) линия 1

29.03.24 02:57:02 Обнаружен курильщик сигп

29.03.24 02:58:15 Пересечение линии (B -> A) линия 2

29.03.24 02:59:42 Обнаружен курильщик сигп

29.03.24 03:00:07 Пересечение линии (B -> A) линия 2

29.03.24 03:00:09 Пересечение линии (A -> B) линия 1

29.03.24 03:00:36 Пересечение линии (B -> A) линия 2

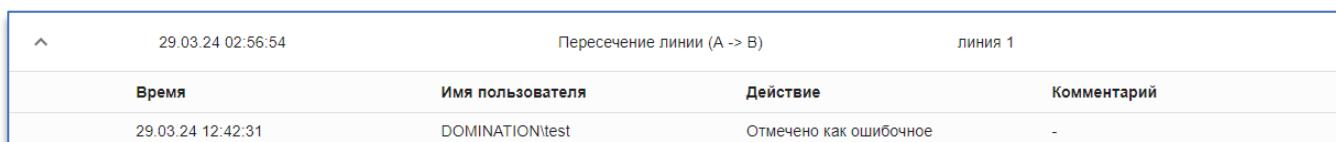
29.03.24 03:00:51 Обнаружен курильщик сигп

29.03.24 03:00:59 Обнаружен курильщик сигп

Количество событий: 1000

Более детальный отчет можно увидеть, нажав на кнопку .

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



Время Событие Действие Комментарий

29.03.24 02:56:54 Пересечение линии (A -> B) линия 1

29.03.24 12:42:31 DOMINATION\test Отмечено как ошибочное -

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.

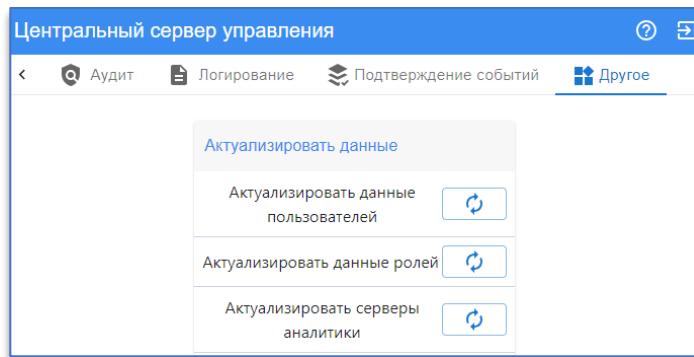
Также отфильтровать события можно с помощью кнопки фильтра , доступной в строке заголовков. После ее нажатия откроется строка, в которую можно ввести необходимое значение или его часть и события автоматически будут отфильтрованы по введённым данным, регистр букв при вводе не учитывается. Для скрытия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

19. 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:

