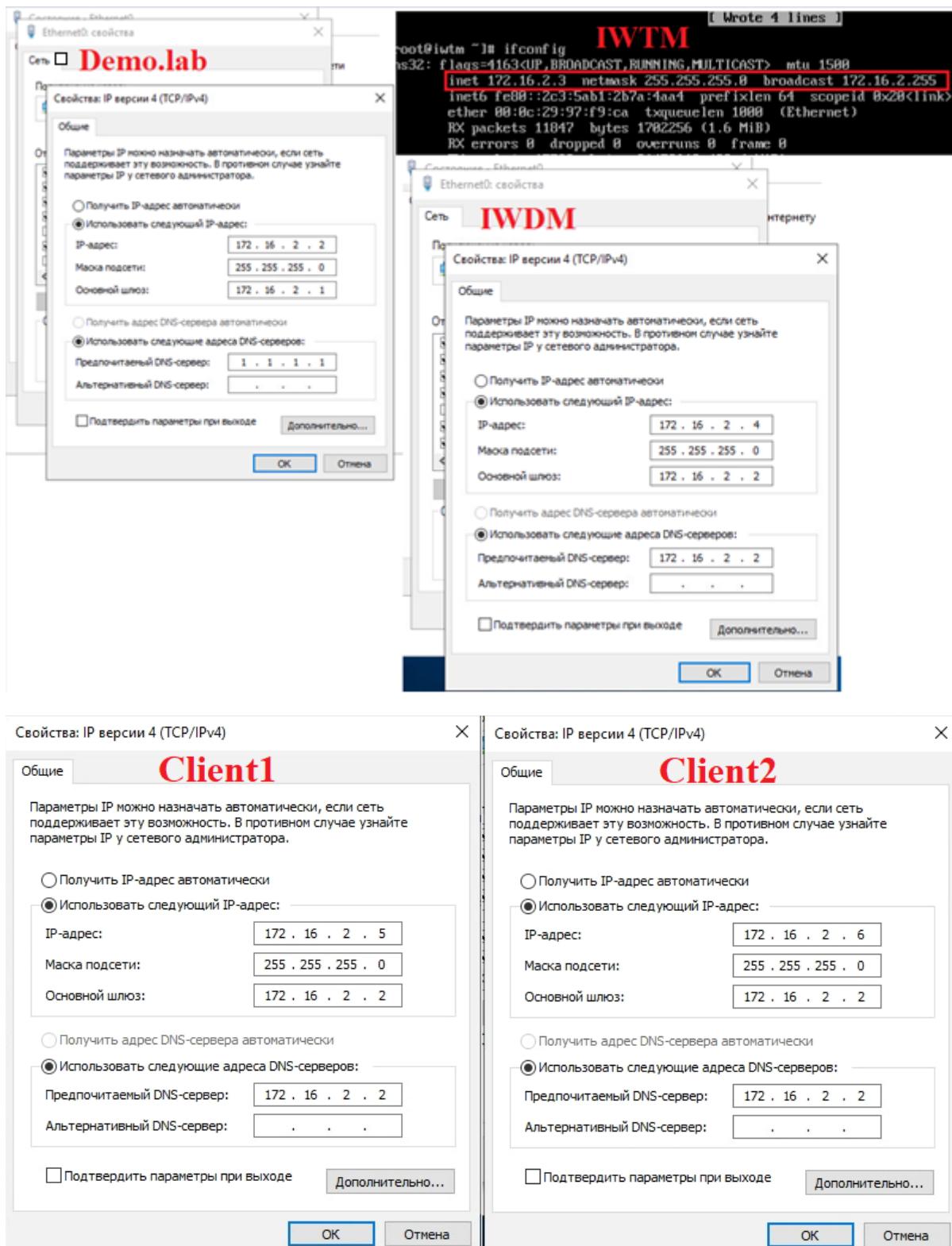


## IP-адреса Demo.lab, IWTM, IWDM, Client1, Client2



## Задание 1: Настройка контроллера домена

Для удобства работы рекомендуется создать подразделение “Champ” в

корневом каталоге оснастки “Пользователи и компьютеры” AD сервера.

Внутри созданного подразделения “Champ” необходимо создать и настроить

следующих доменных пользователей с соответствующими правами:

Логин: user-agent1, пароль: xxXX1234, права пользователя домена

Логин: user-agent2, пароль: xxXX1234, права пользователя домена

Логин: iw-admin, пароль: xxXX1234, права администратора домена

Логин: iwtm-officer, пароль: xxXX1234, права пользователя домена

Логин: ldap-sync, пароль: xxXX1234, права пользователя домена

Создаем пользователей и добавляем администратору права –

Администратора, Администратора Домена (Domain Admin)

The screenshot shows the 'Active Directory - пользователи и компьютеры' snap-in. On the left, the navigation pane displays the 'demo.lab' domain structure, including 'demo.lab', 'Builtin', 'Champ', 'Computers', 'demo', 'Demolabs', 'Domain Controllers', 'ForeignSecurityPrincipals', 'Managed Service Accounts', and 'Users'. The 'Champ' folder is expanded. On the right, a table lists users under 'Champ': CLIENT1, CLIENT2, IWDM, iw-admin, iwtm-officer, ldap-sync, user-agent1, and user-agent2. The 'iw-admin' user is selected, indicated by a blue selection bar.

The screenshot shows the 'Active Directory - пользователи и компьютеры' snap-in. The 'Champ' organizational unit is selected in the navigation pane. The 'iw-admin' user is selected in the main list. A properties dialog box is open for 'Свойства: iw-admin'. The 'Член групп:' tab is selected, showing the user's group memberships: 'Administrators' (demo.lab/Builtin), 'Domain Admins' (demo.lab/Users), and 'Domain Users' (demo.lab/Users). Buttons for 'Добавить...' (Add...) and 'Удалить' (Delete) are at the bottom of the dialog.

## Задание 2: Настройка DLP сервера

DLP-сервер контроля сетевого трафика уже предустановлен, но не настроен.

Необходимо синхронизировать каталог пользователей и компьютеров

LDAP с домена с помощью ранее созданного пользователя ldap-sync.

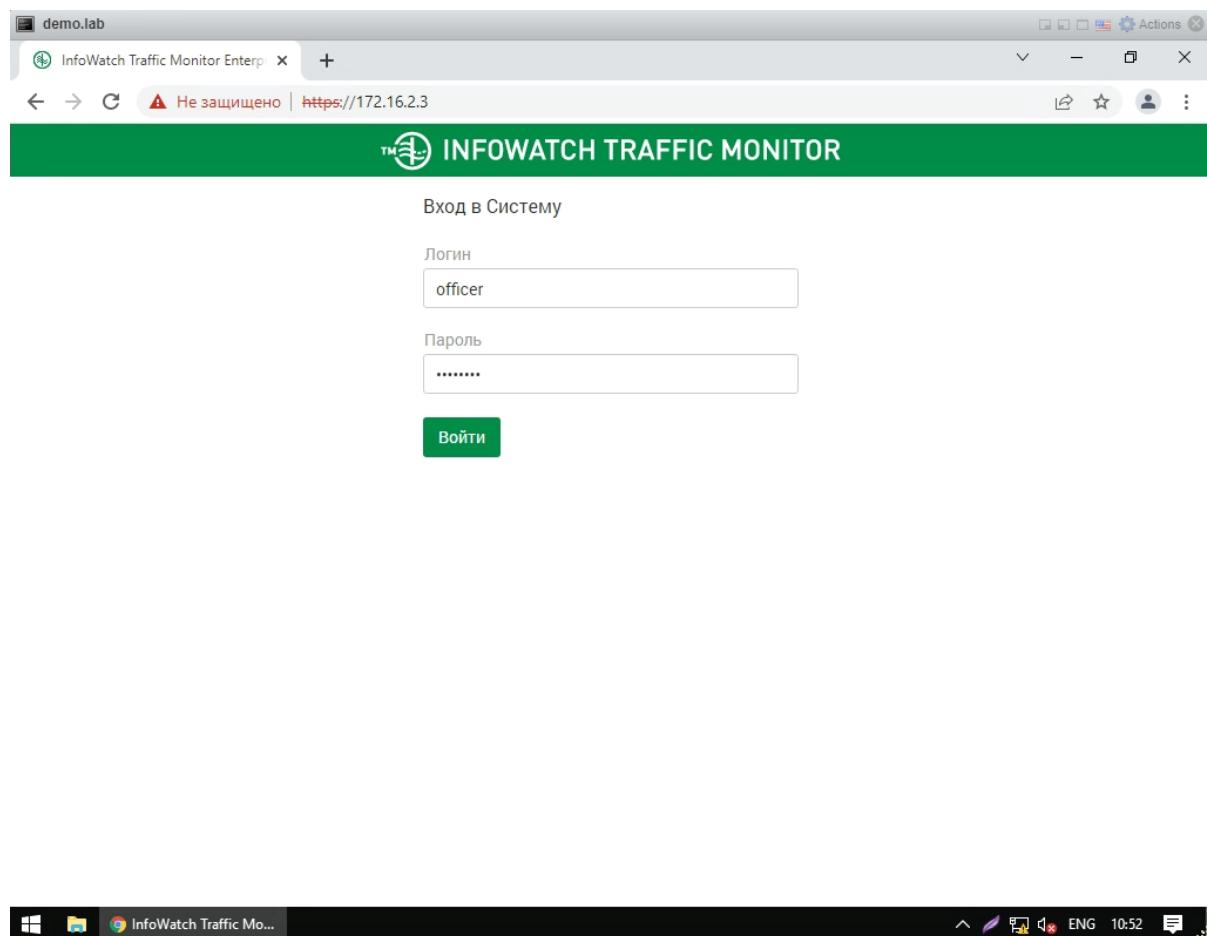
Для входа в веб-консоль необходимо настроить использование ранее

созданного пользователя домена iwtm-officer с полными правами офицера безопасности и на администрирование системы, полный доступ на все области видимости.

Запишите IP-адреса, токен, логины и пароли от учетных записей, а также

все прочие нестандартные данные (измененные вами) вашей системы в текстовом

файле «отчет.txt» на рабочем столе компьютера.



InfoWatch Traffic Monitor Enterprise x +

InfoWatch Traffic Monitor Enterprise 172.16.2.3 https://172.16.2.3/settings/ldap

Сводка События Отчеты Технологии ▾ Объекты защиты Персоны Еще ▾ Помощь Поиск соб...

### LDAP-серверы

+ | edit | X | ▾

Demo.lab

Demo.lab	
Тип сервера	Active Directory
Синхронизация	Автоматическая
Период синхронизации	Ежеминутно
Повторение	каждые 15 минут

### Настройки соединения

LDAP-сервер	172.16.2.2
Использовать протокол Kerberos	Не использовать
Глобальный LDAP-порт	3268
LDAP-порт	389
Использовать глобальный каталог	Использовать
Анонимный доступ	Не использовать
LDAP-запрос	dc=demo, dc=lab
Логин	ldap-sync

### Статус

Последняя синхронизация	Сегодня в 10:50 (4 минуты назад)
Статус синхронизации	Успешно
Следующая синхронизация	Сегодня в 11:05 (через 11 минут)

Проверить соединение

### Управление доступом

Пользователи Роли Области видимости

### Пользователи

+ | X | ▾

	Логин	Название	Email	Роли	Области видим.	Описание
<input type="checkbox"/>	iw-admin	iw-admin	231@mail.ru	Администратор, VIP	Полный доступ	
<input type="checkbox"/>	iwtm-officer	iwtm-officer	23@mail.ru	Администратор, VIP	Полный доступ	
<input type="checkbox"/>	administrator	Администратор		Администратор		Предустановлен
<input type="checkbox"/>	officer	Офицер безопасности		Администратор, Полный доступ		Предустановлен

### **Задание 3: Установка и настройка сервера агентского мониторинга**

Необходимо ввести сервер в домен, после перезагрузки войти в систему от ранее созданного пользователя `iw-admin` (важно). После входа в систему необходимо переместить введенный в домен компьютер в ранее созданное подразделение “Champ” на домене.

Установить базу данных PostgreSQL с паролем суперпользователя `ххХХ1234`.

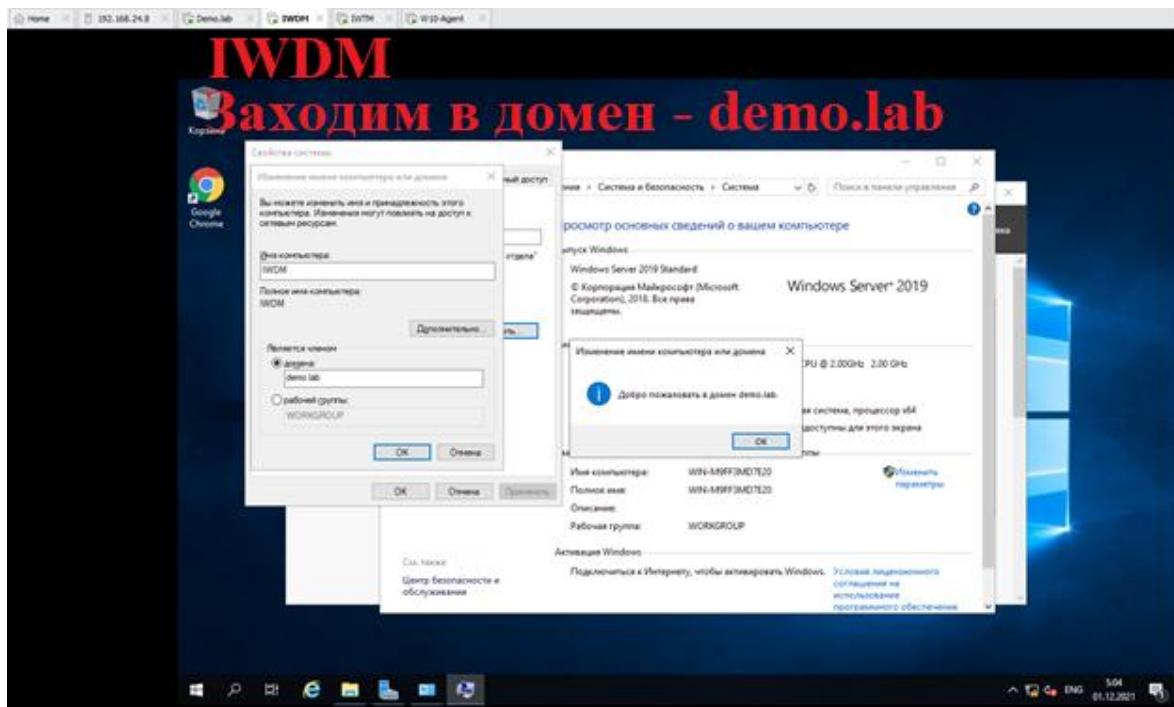
Установить сервер агентского мониторинга с параметрами по умолчанию, подключившись к ранее созданной БД.

При установке сервера агентского мониторинга необходимо установить соединение с DLP-сервером по IP-адресу и токену, но можно сделать это и после установки. При установке настроить локального пользователя консоли управления: `officer` с паролем `ххХХ1234`

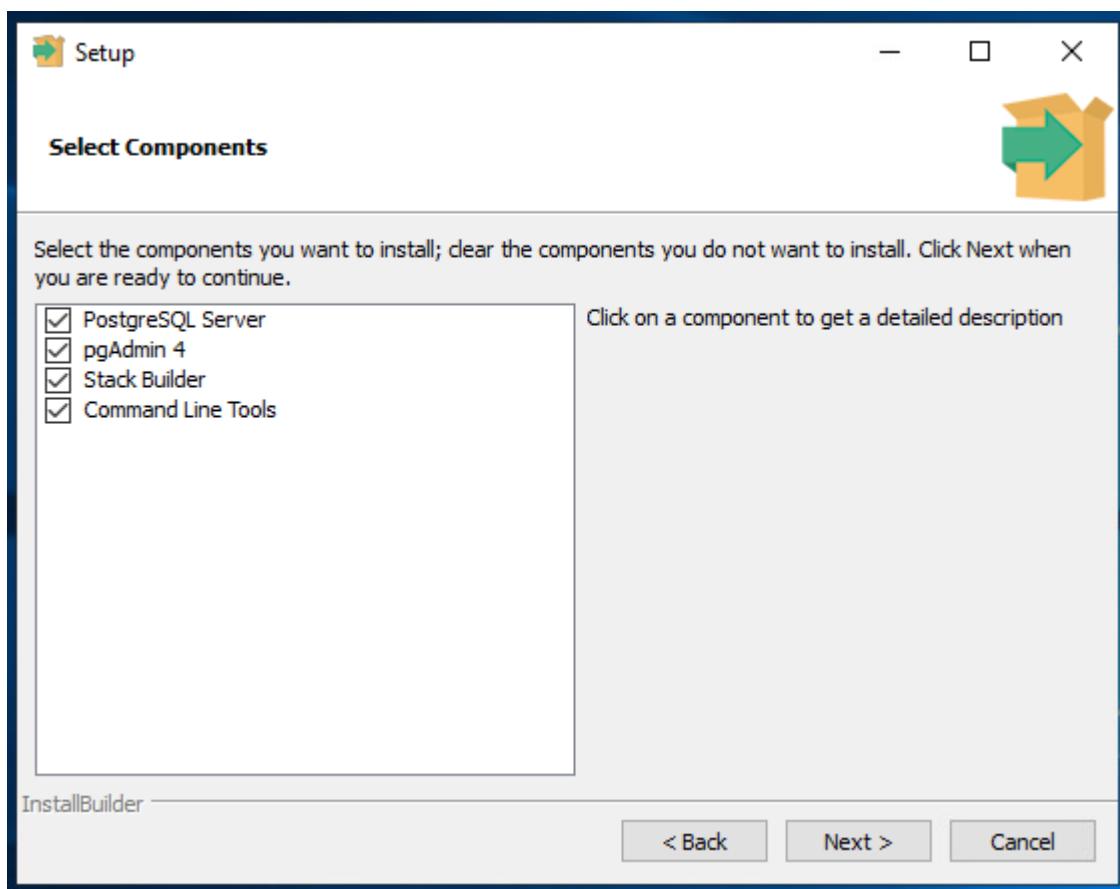
Синхронизировать каталог пользователей и компьютеров с Active Directory.

После синхронизации настроить беспарольный вход в консоль управления от ранее созданного доменного пользователя `iw-admin`, установить полный доступ к системе, установить все области видимости.

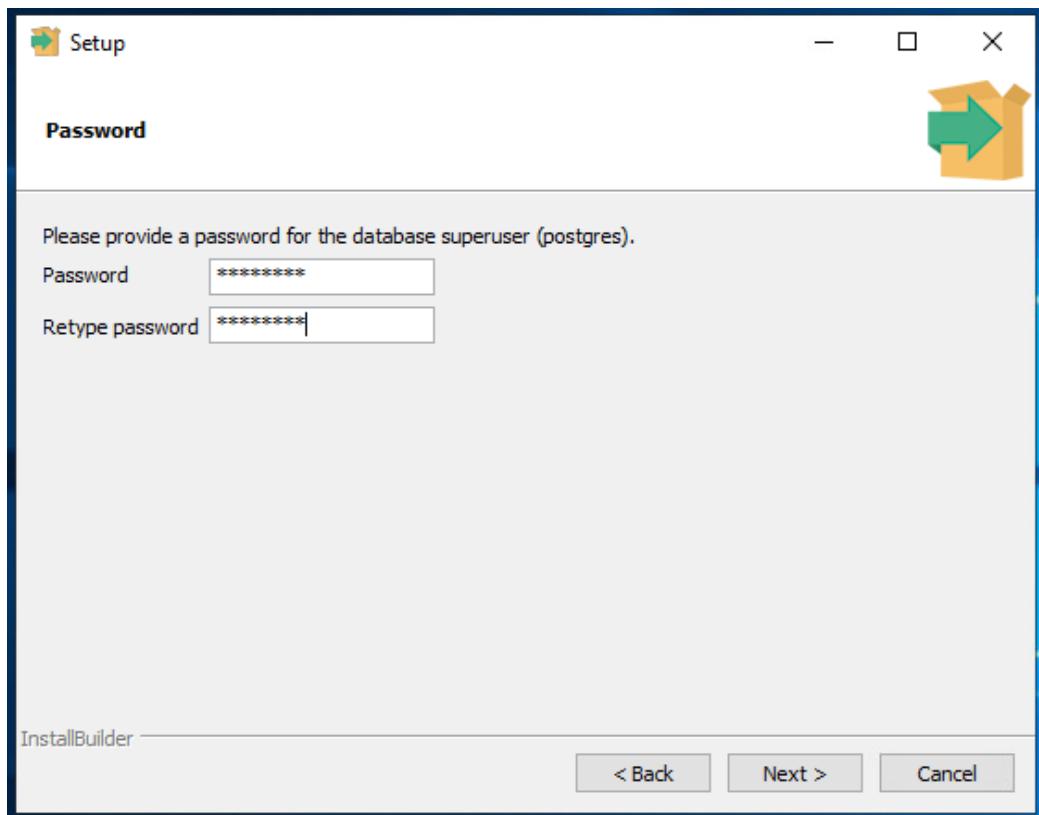
Проверить работоспособность входа в консоль управления без ввода пароля. Если сервер не введен в домен или работает от другого пользователя, данная опция работать не будет.



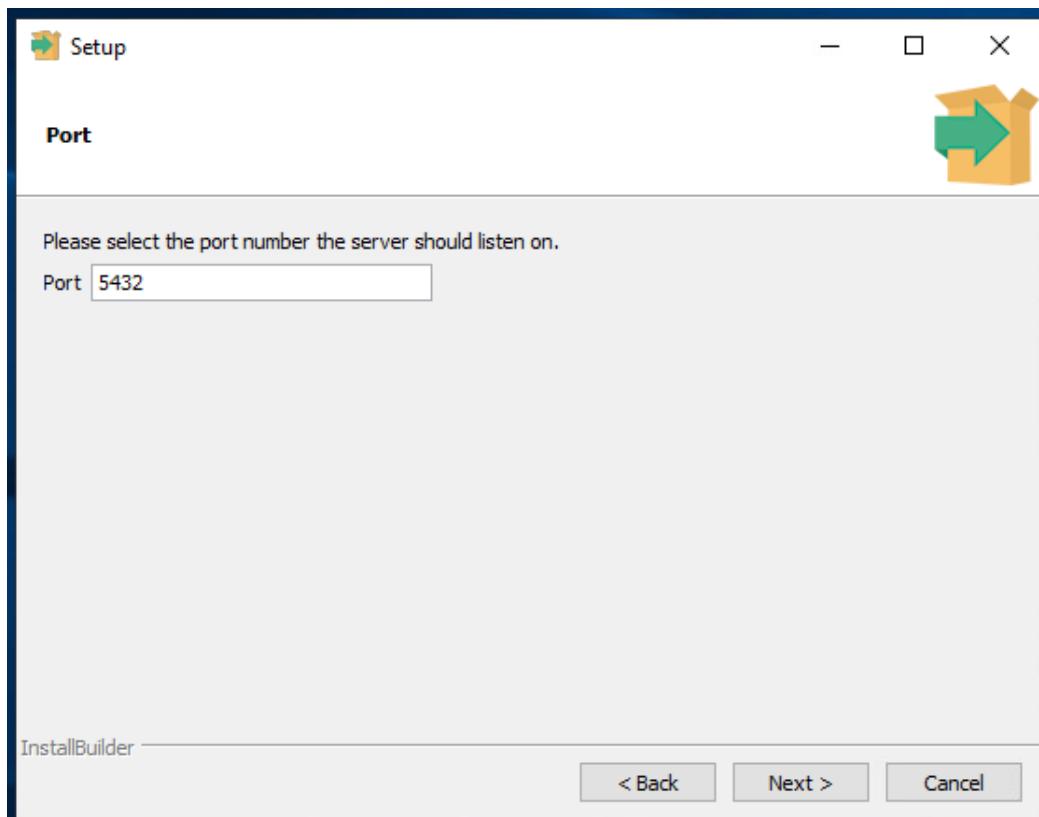
После перезагрузки заходим под iw-admin



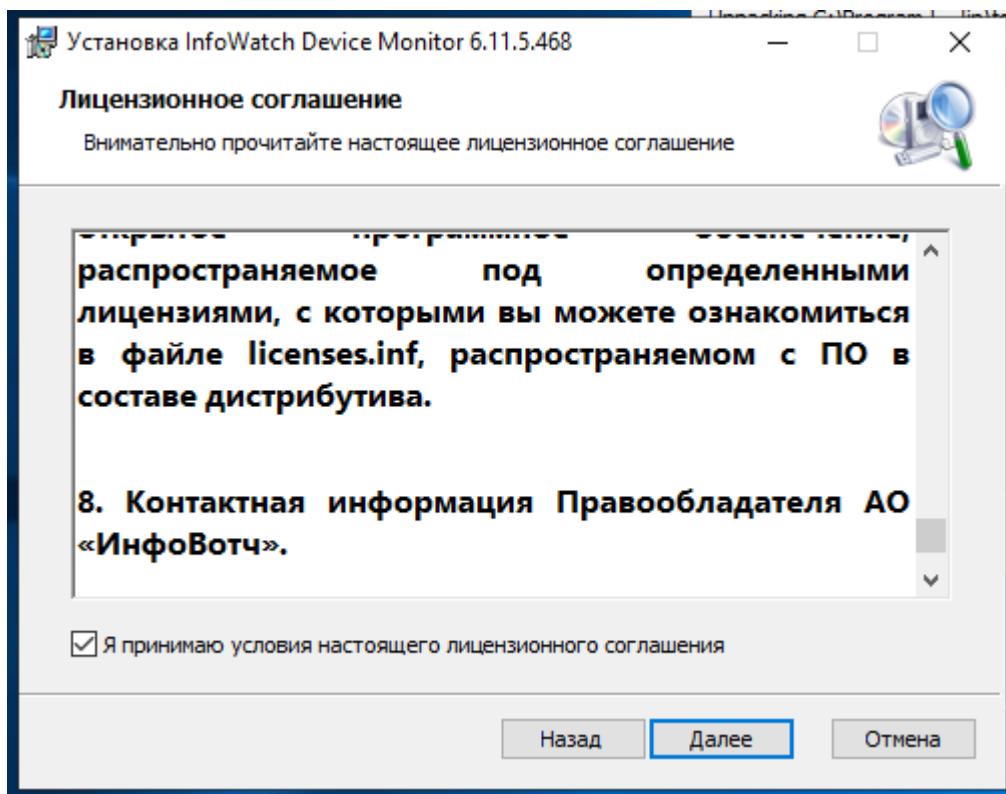
Вводим стандартный пароль



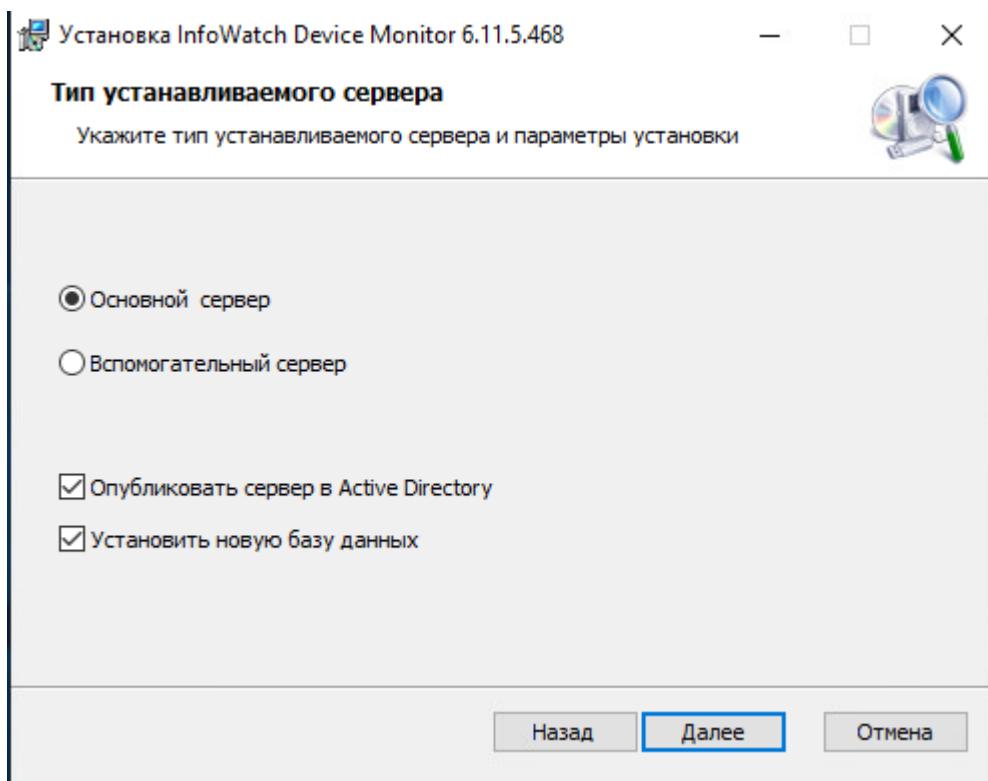
Порт оставляем по умолчанию

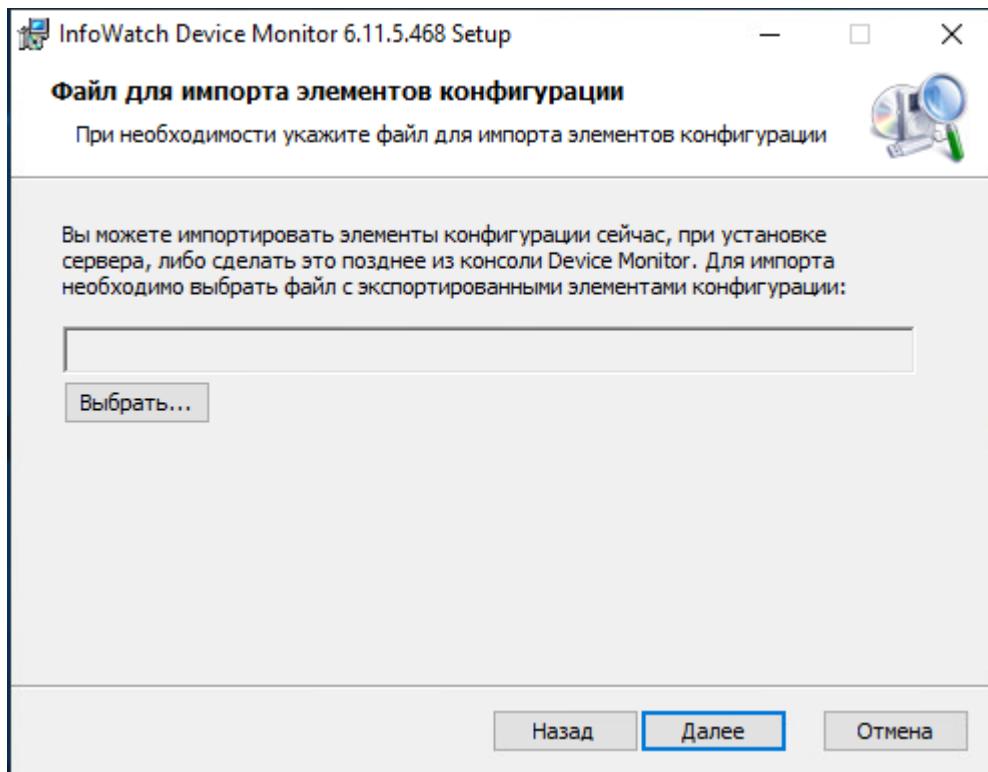


Затем, переходим к установке InfoWatch Device Monitor

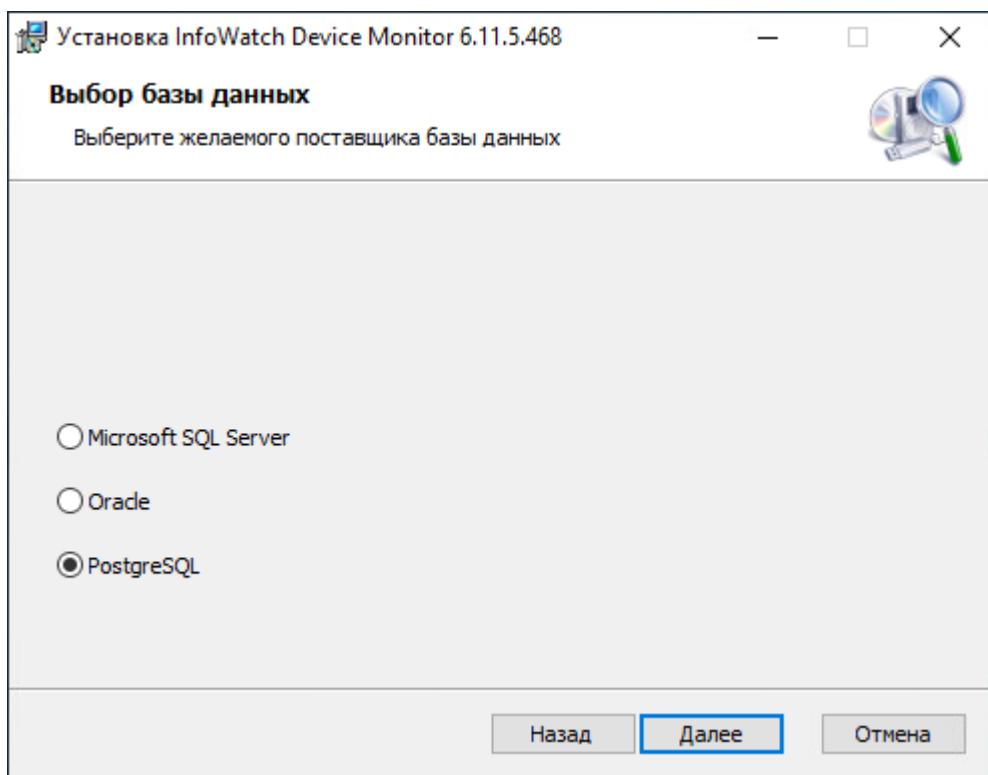


Оставляем галочку на основном сервере

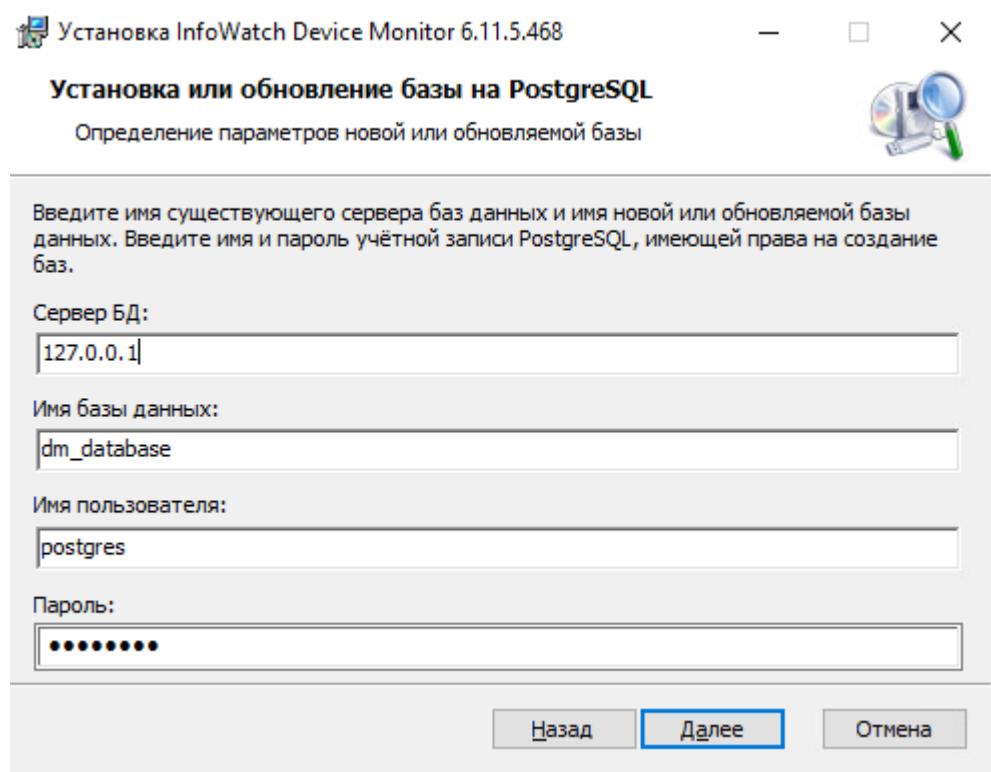




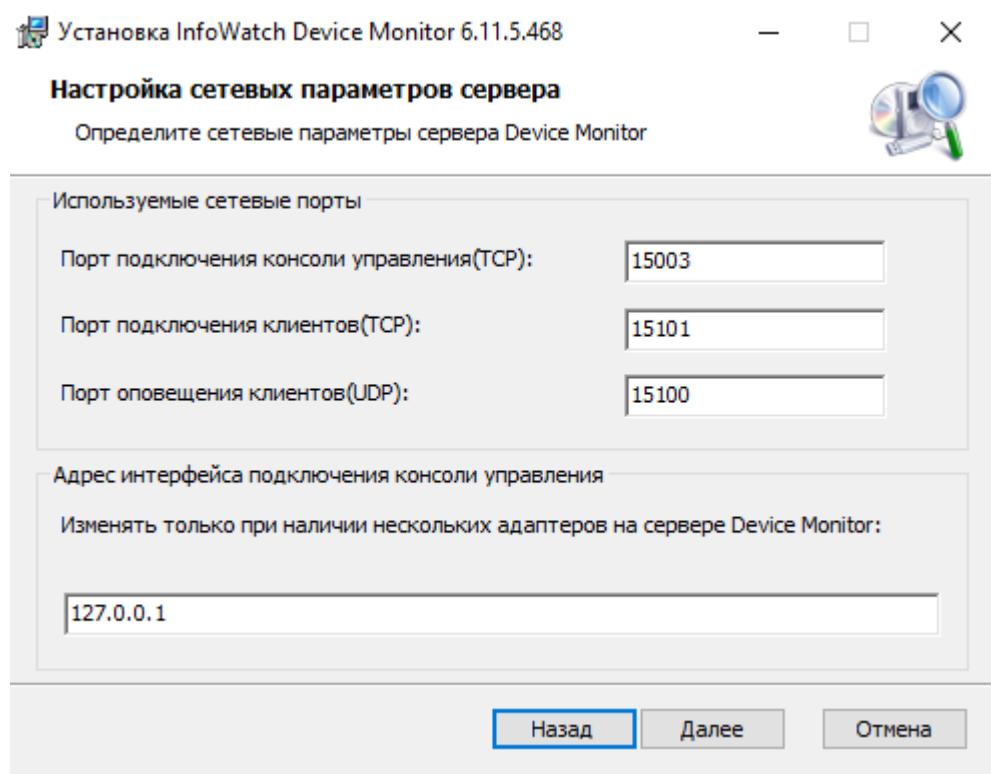
Выбираем базу данных, в нашем случае будет - PostgresSQL



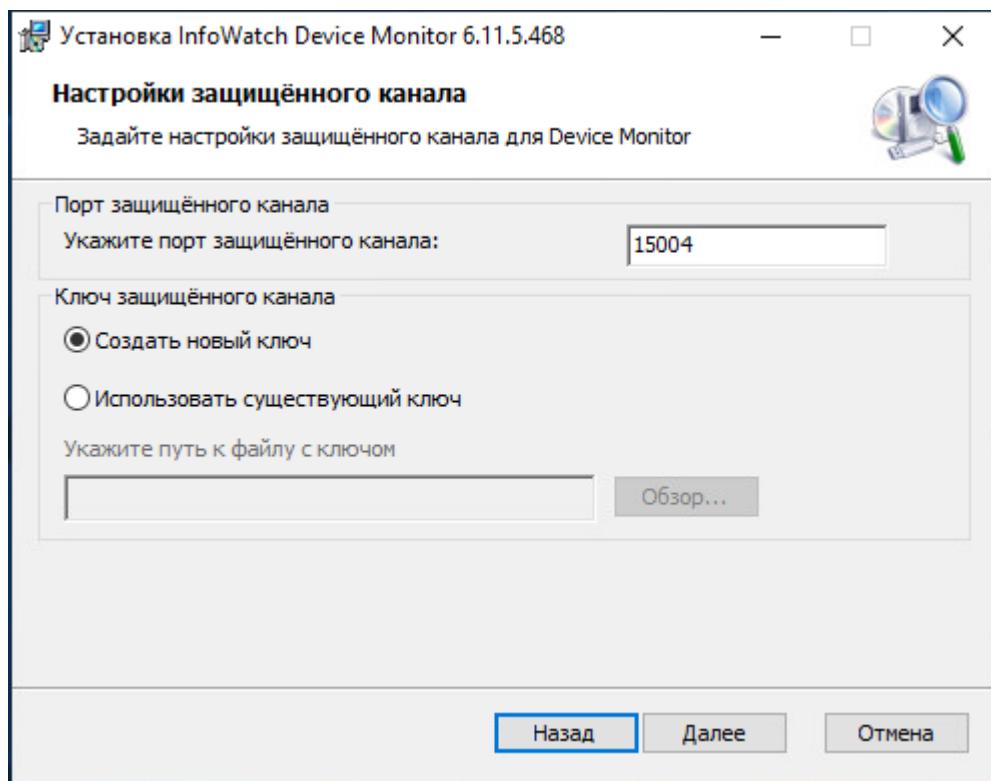
Задаем сервер БД – 127.0.0.1; Имя БД – dm\_database, имя пользователя – postgres и стандартный пароль



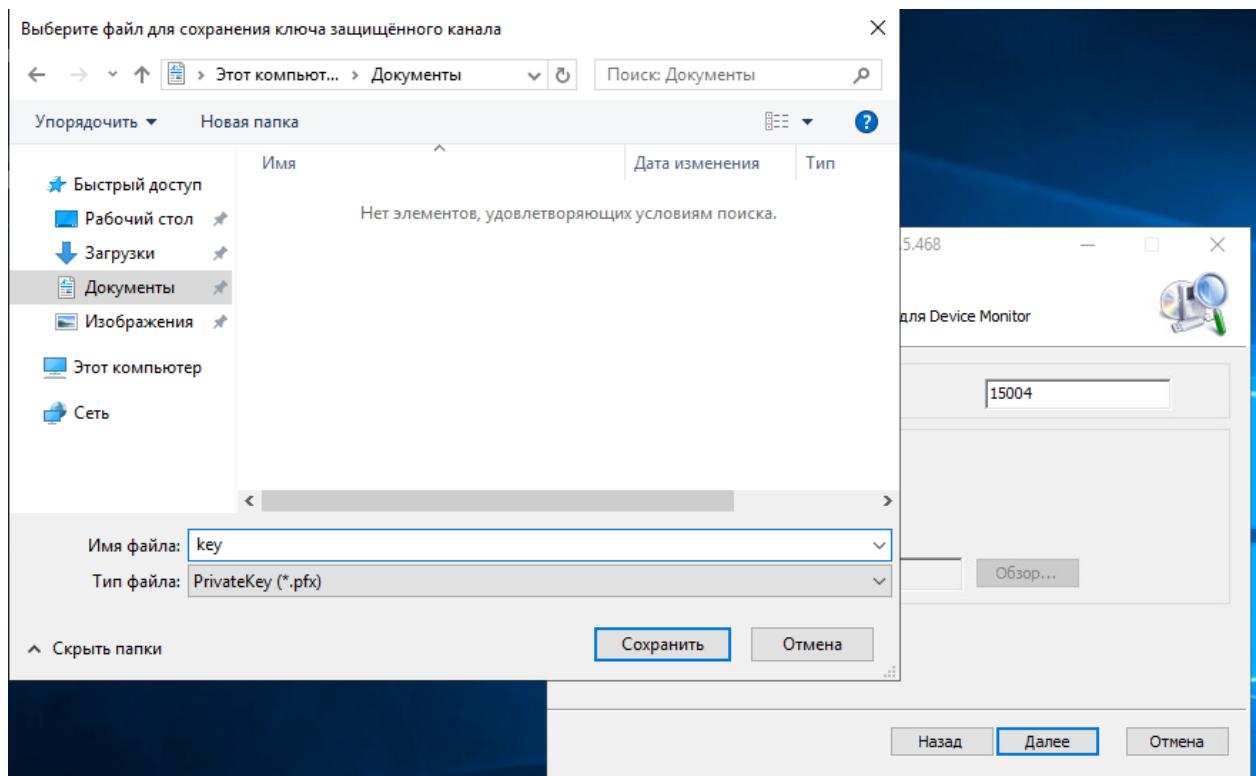
Настраиваем сетевые параметры



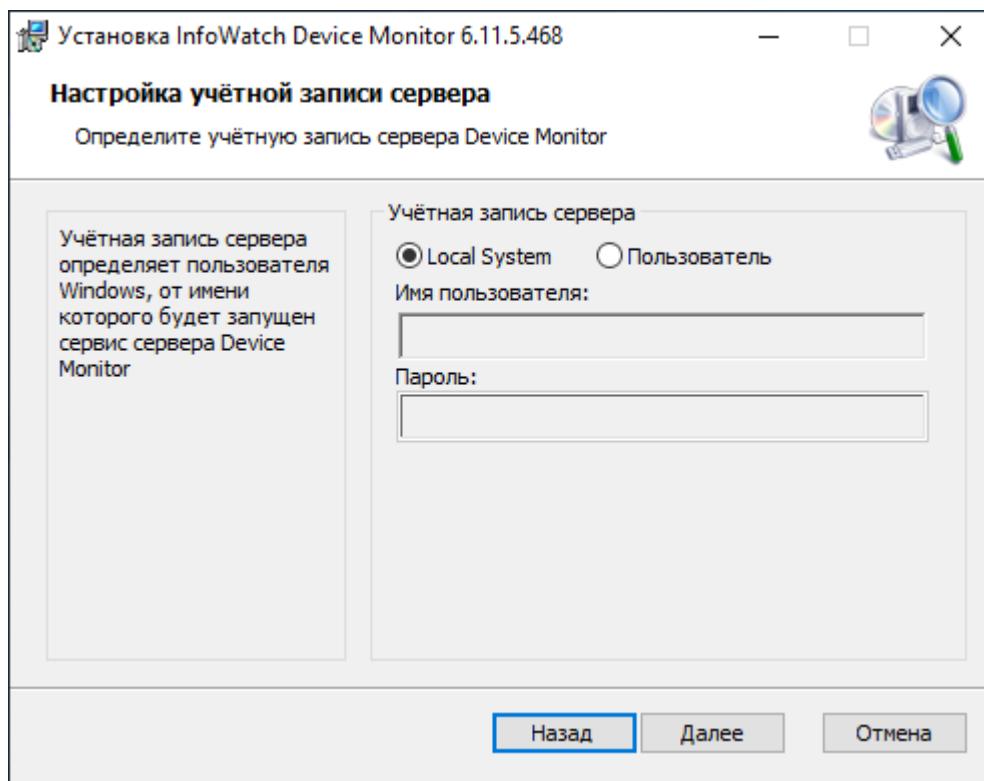
## Настраиваем защищённый канал и создаём новый ключ



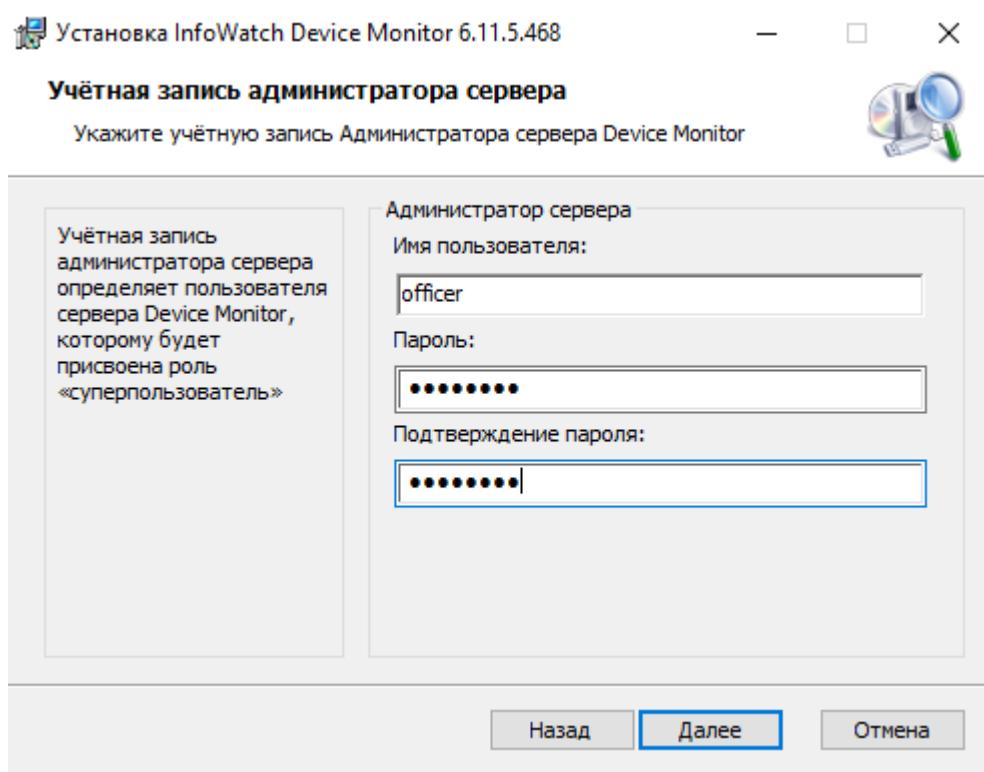
## Сохраняем ключ



Оставляем локальную учётную запись



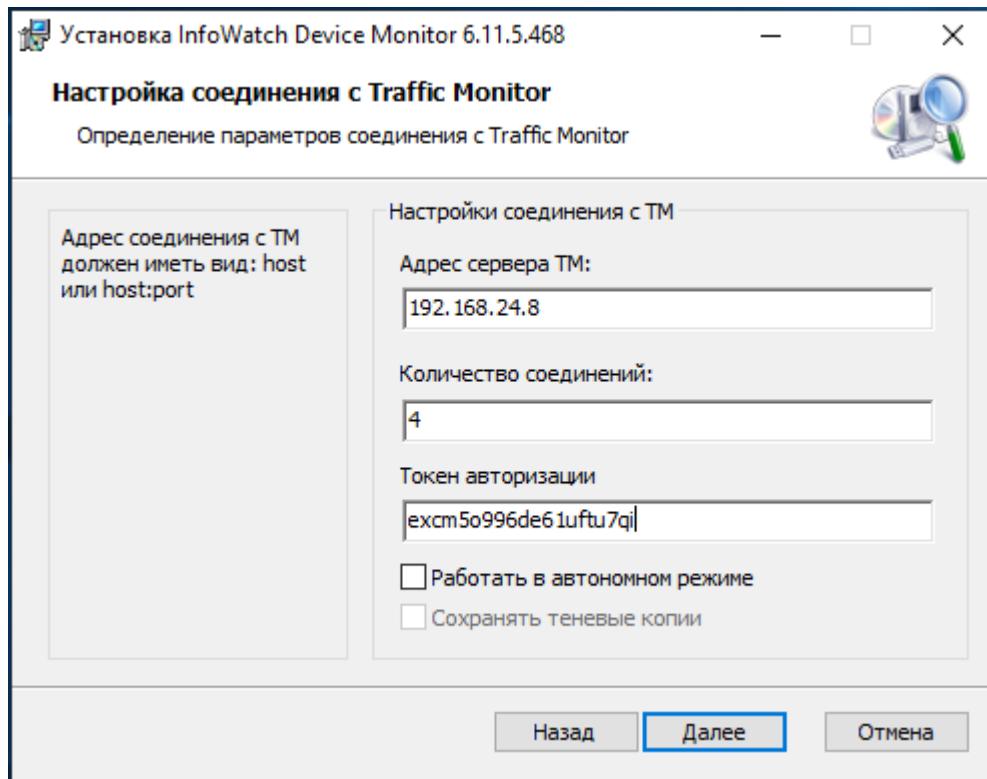
Вводим логин и пароль администратора



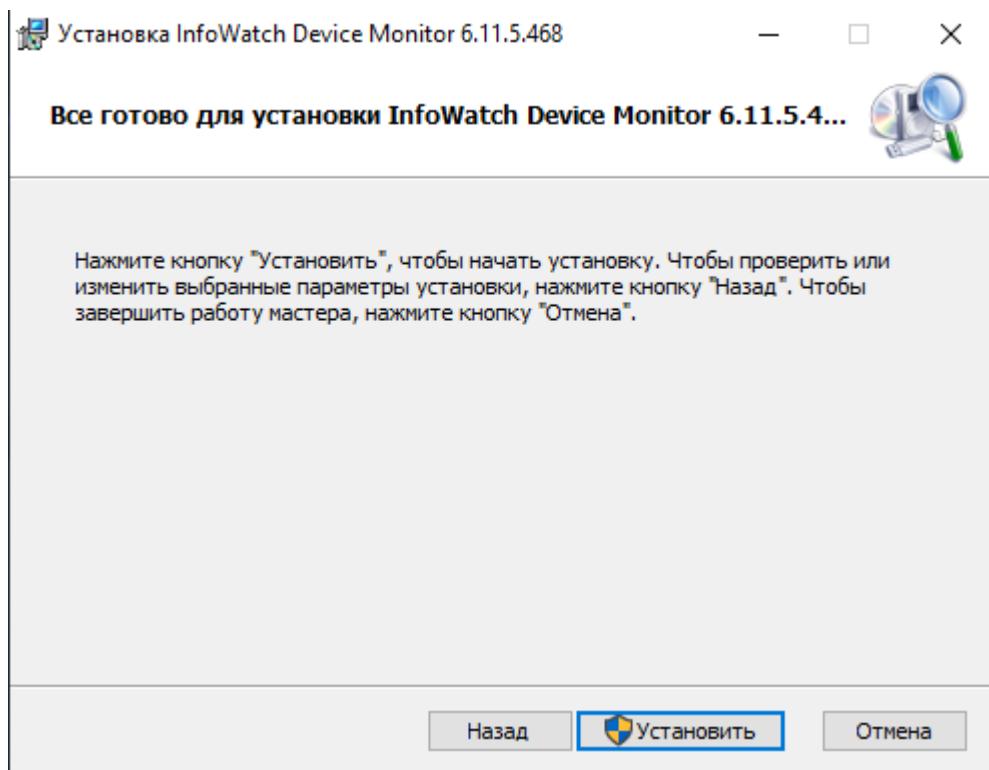
## Смотрим токен

The screenshot shows the InfoWatch Traffic Monitor Enterprise web interface. In the top navigation bar, there are tabs like 'Сводка', 'События', 'Отчеты', 'Технологии', 'Объекты защиты', 'Персоны', 'Политики', 'Списки', 'Управление', 'Краулер', 'Поиск событий', and 'Офицер безопасности'. The main content area is titled 'Плагины' and shows a list of installed plugins: 'InfoWatch Device Monitor' (InfoWatch Device Monitor, Производитель: IW, Версия 6.11.5). Below this, there's a table with columns 'Статус', 'Имя', 'Содержание', and 'Описание'. One row is selected, showing 'Активный' status, 'Token-3' name, 'excm5o996de61uftu7qi' content, and an empty description.

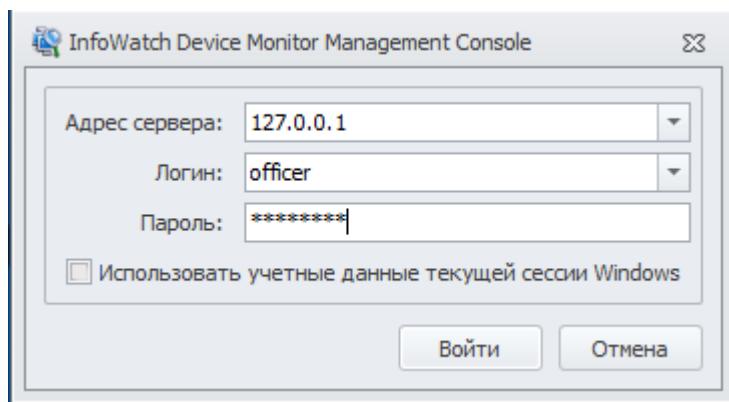
Указываем Ip-адрес IWTM и токен (который только что посмотрели в трафик мониторе)



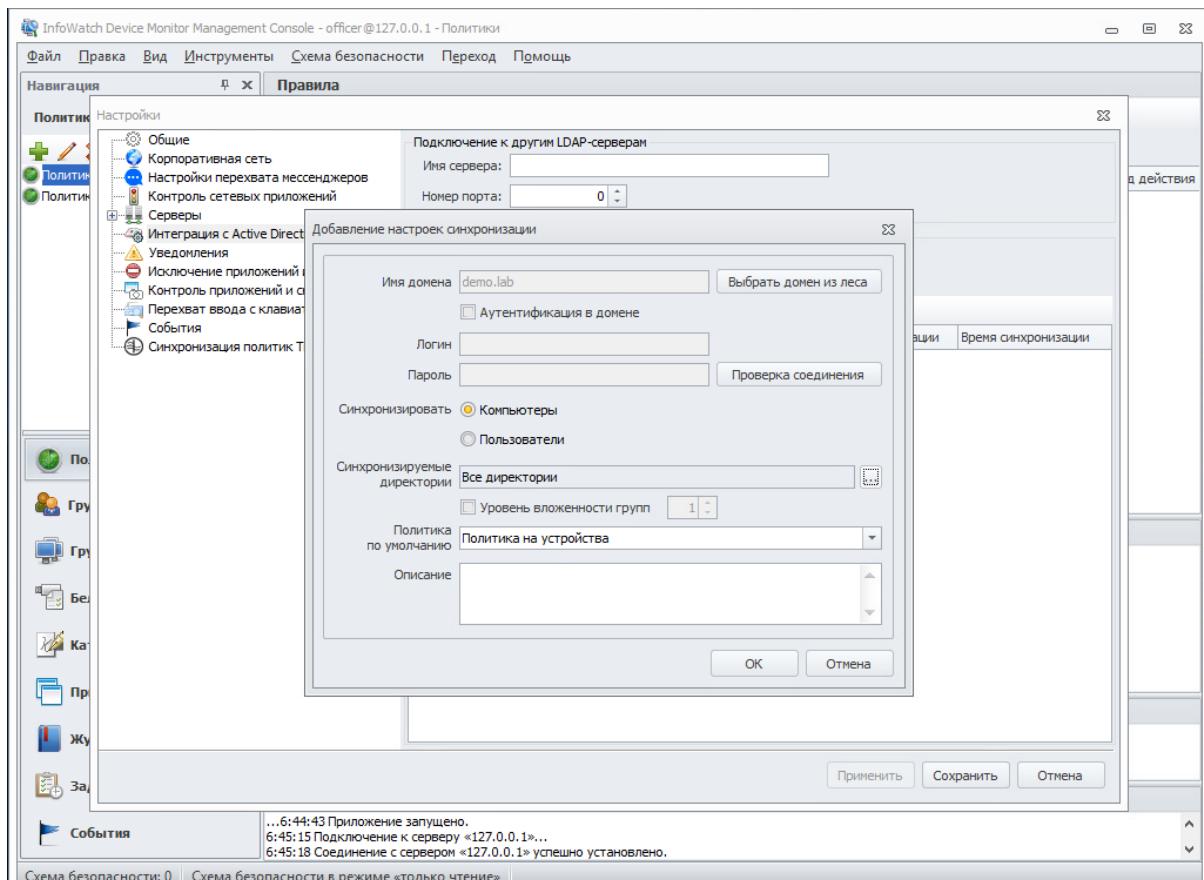
## Устанавливаем



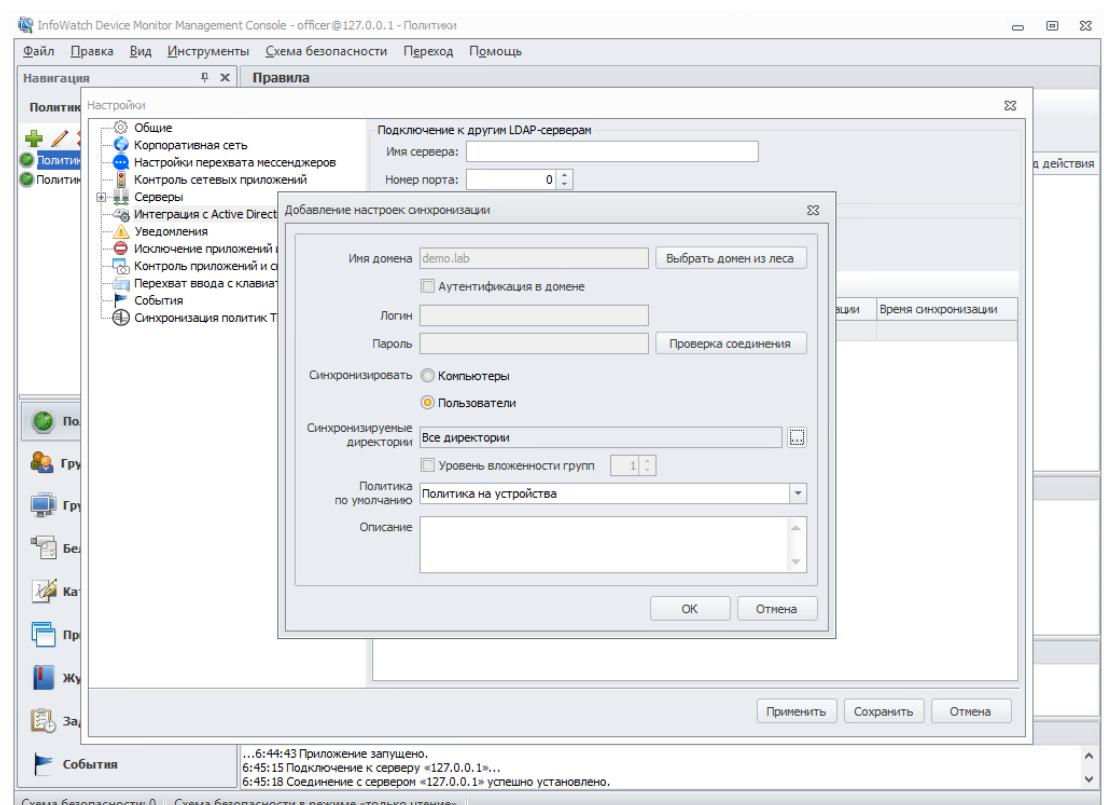
## Подключаемся к InfoWatch Device Monitor Management Console



## Синхронизуем компьютеры

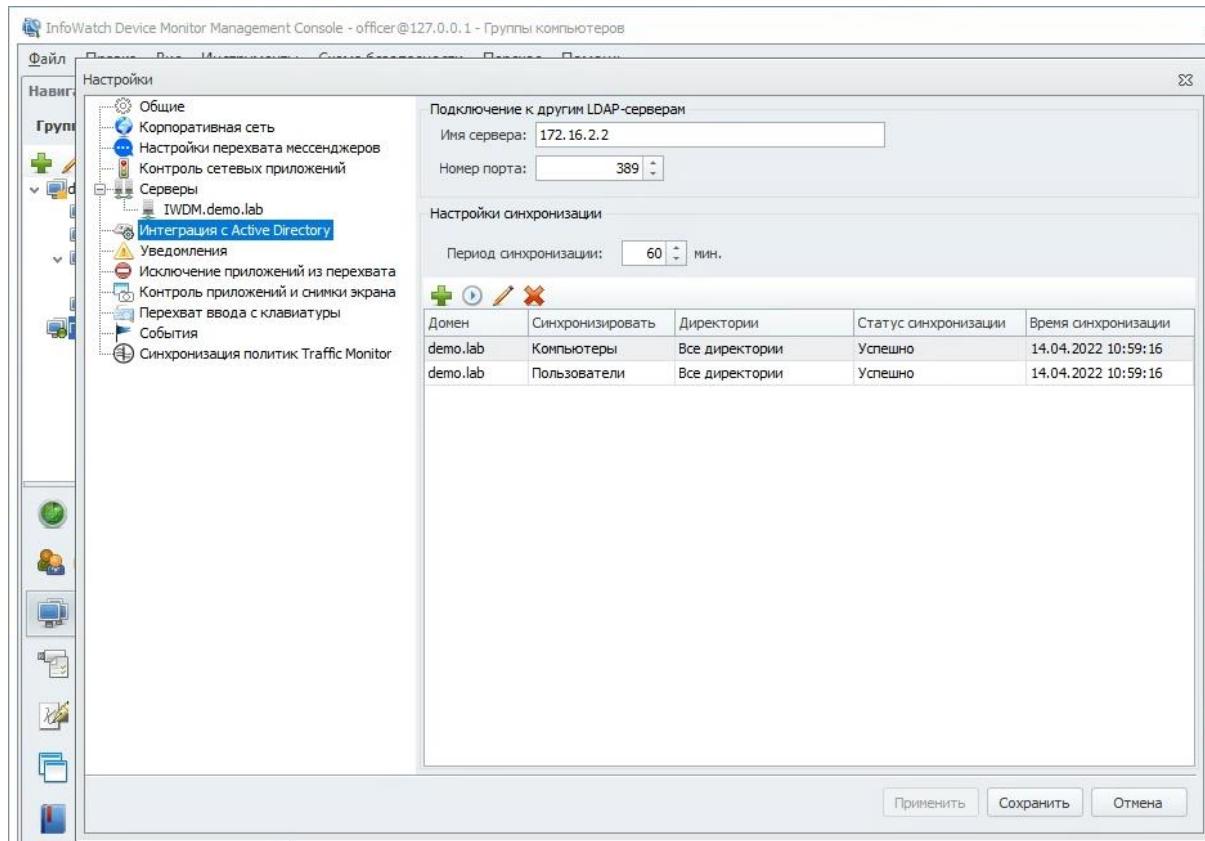


## Синхронизуем пользователей



Указываем Ip-адрес сервера demo.lab и порт

Синхронизация у компьютеров и пользователей



Изменение пользователя

Логин:	DEMO\jw-admin
Пароль:	*****
Повтор пароля:	*****
Полное имя:	iw-admin

**Видит сотрудников**

Группа сотрудников	Роль пользователя	
Группа сотрудников по умолчанию	Офицер безопасности группы	Добавить... Изменить... Удалить

**Видит компьютеры**

Группа компьютеров	Роль пользователя	
demo	Офицер безопасности группы	Добавить... Изменить... Удалить

**Общие роли**

Офицер безопасности	Выбрать
Администратор	Удалить

**Сохранить**    **Отмена**

Пользователи консоли

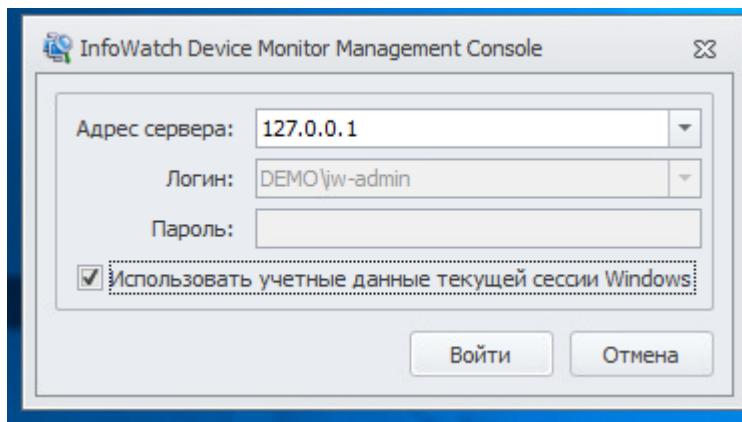
Пользователи консоли	Роли
----------------------	------

Показать записи: Все

Пользователи:

Статус	Логин	Группы	Полное имя	
●	DEMO\jw-admin	Группа сотрудников по ум...	iw-admin	Добавить из AD Создать... Изменить... Удалить Заблокировать
●	officer	Все группы		

## Настройка беспарольного входа



**Задание 4: Установка агента мониторинга на машине нарушителя**

Необходимо ввести клиентскую машину 1 в домен, после перезагрузки

войти в систему от ранее созданного пользователя user-agent1.

Необходимо ввести клиентскую машину 2 в домен, после перезагрузки

войти в систему от ранее созданного пользователя user-agent2.

После входа в систему необходимо переместить веденные в домен компьютеры в ранее созданное подразделение “Champ” на домене.

**Установить агент мониторинга:**

На машину 1 с помощью задачи первичного распространения с сервера

агентского мониторинга.

На машину 2 с помощью групповых политик домена.

Необходимо создавать отдельные объекты групповых политик на каждое

задание и делать снимки экрана для подтверждения создания и

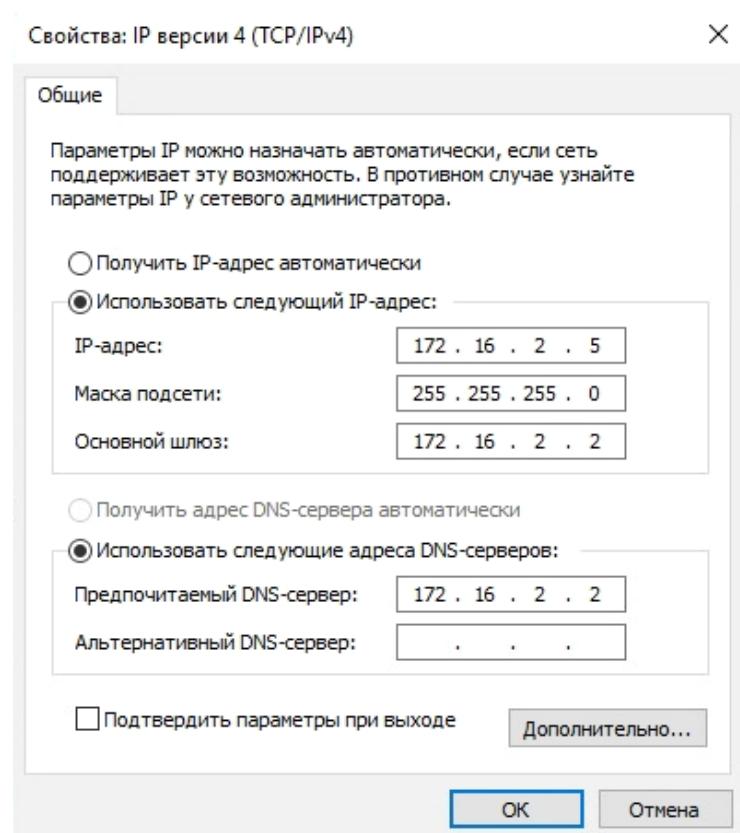
выполнения

политик.

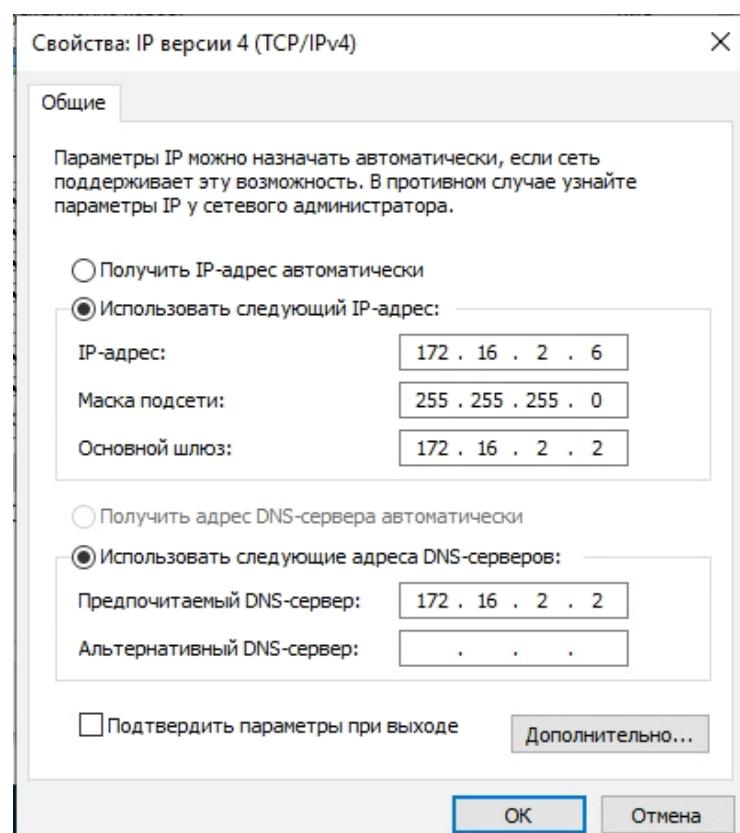
Ручная установка с помощью переноса на машину нарушителя пакета

установки является некорректным выполнением задания

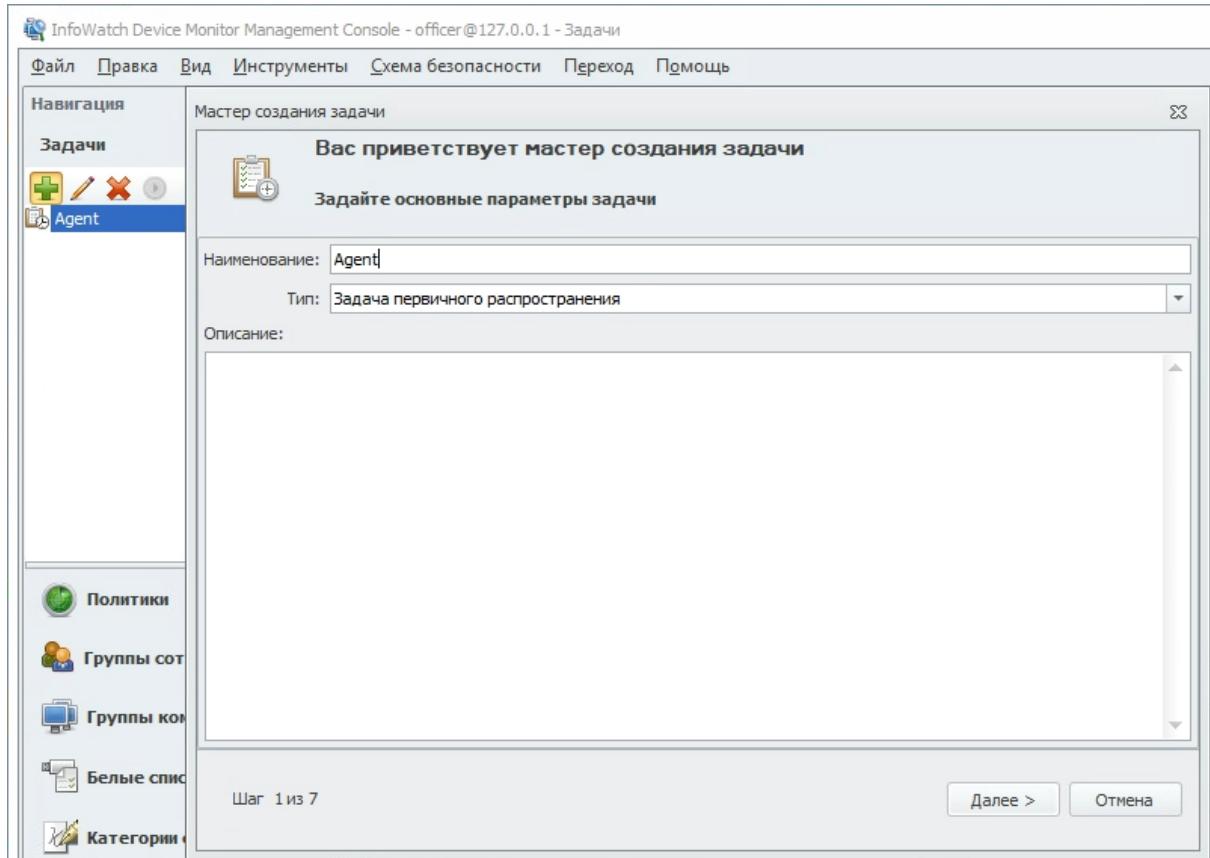
## Клиент1



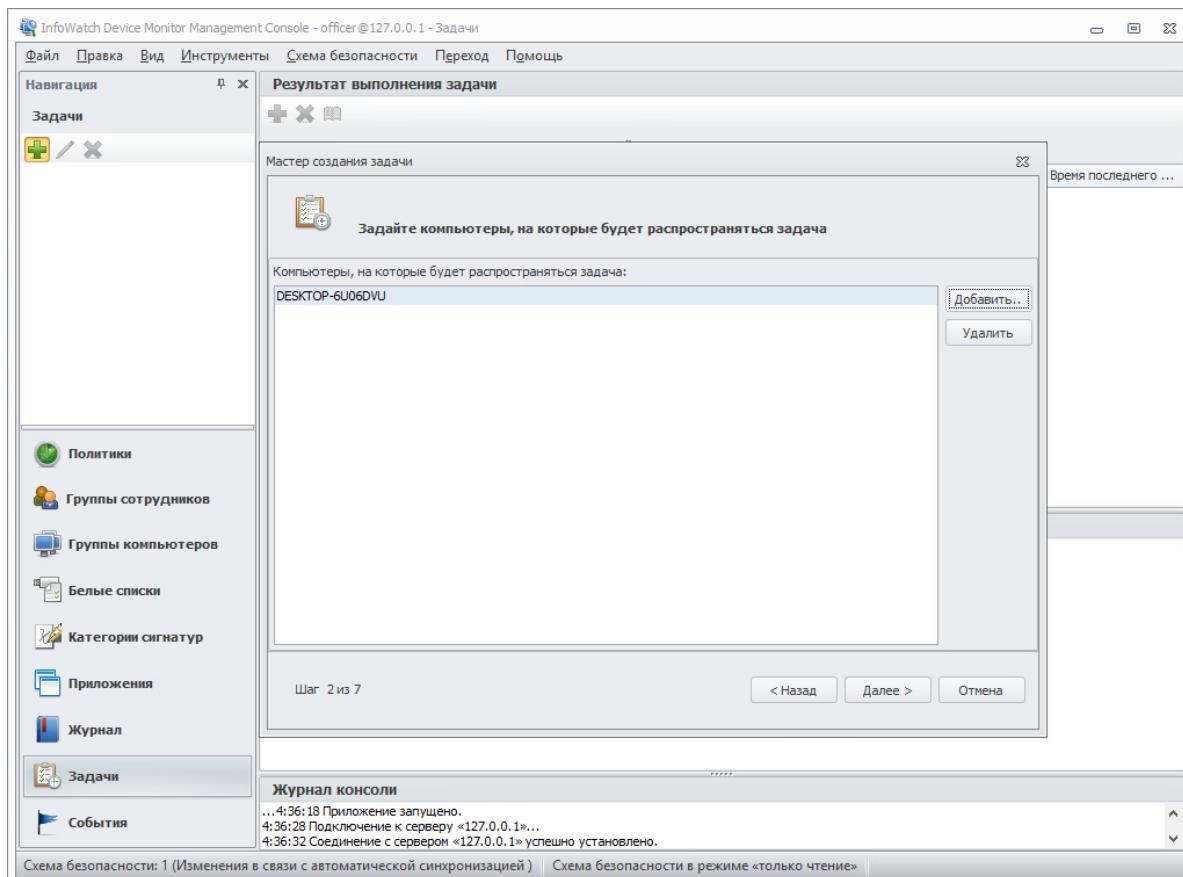
## Клиент2



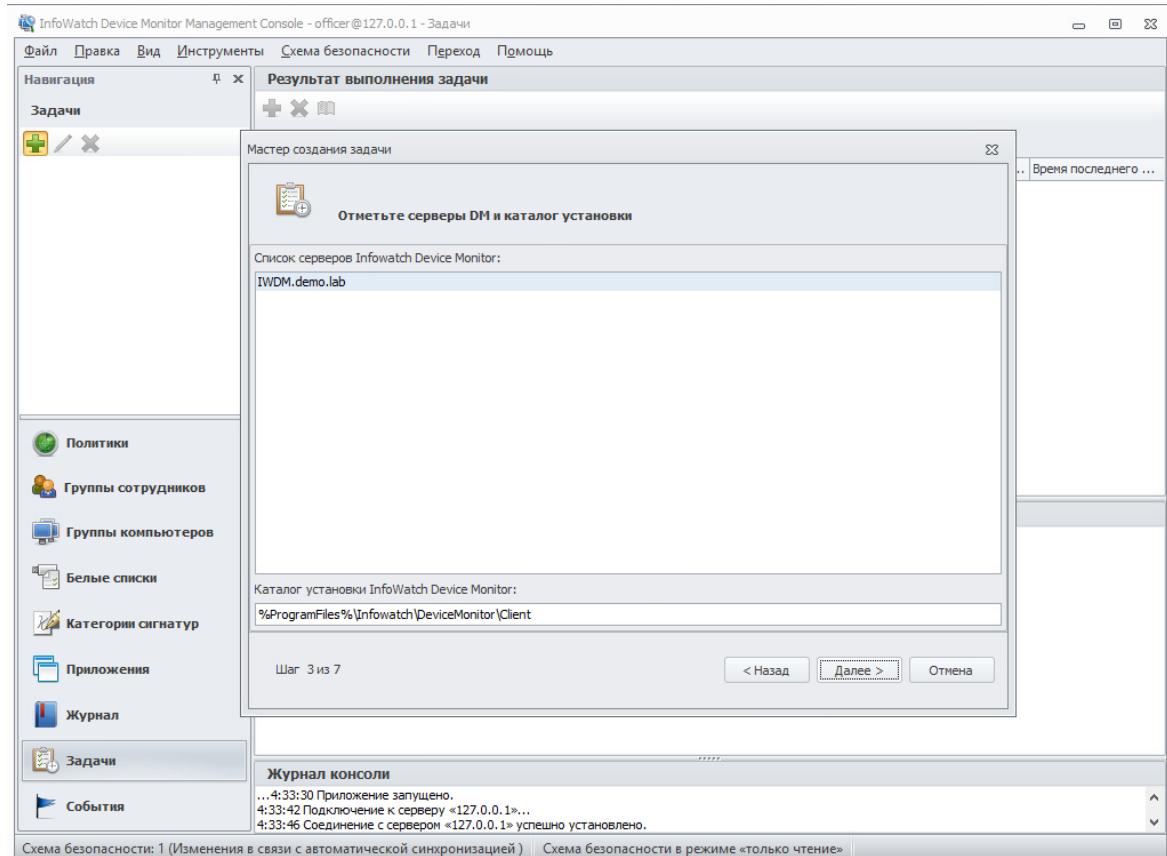
## Создаем новую задачу

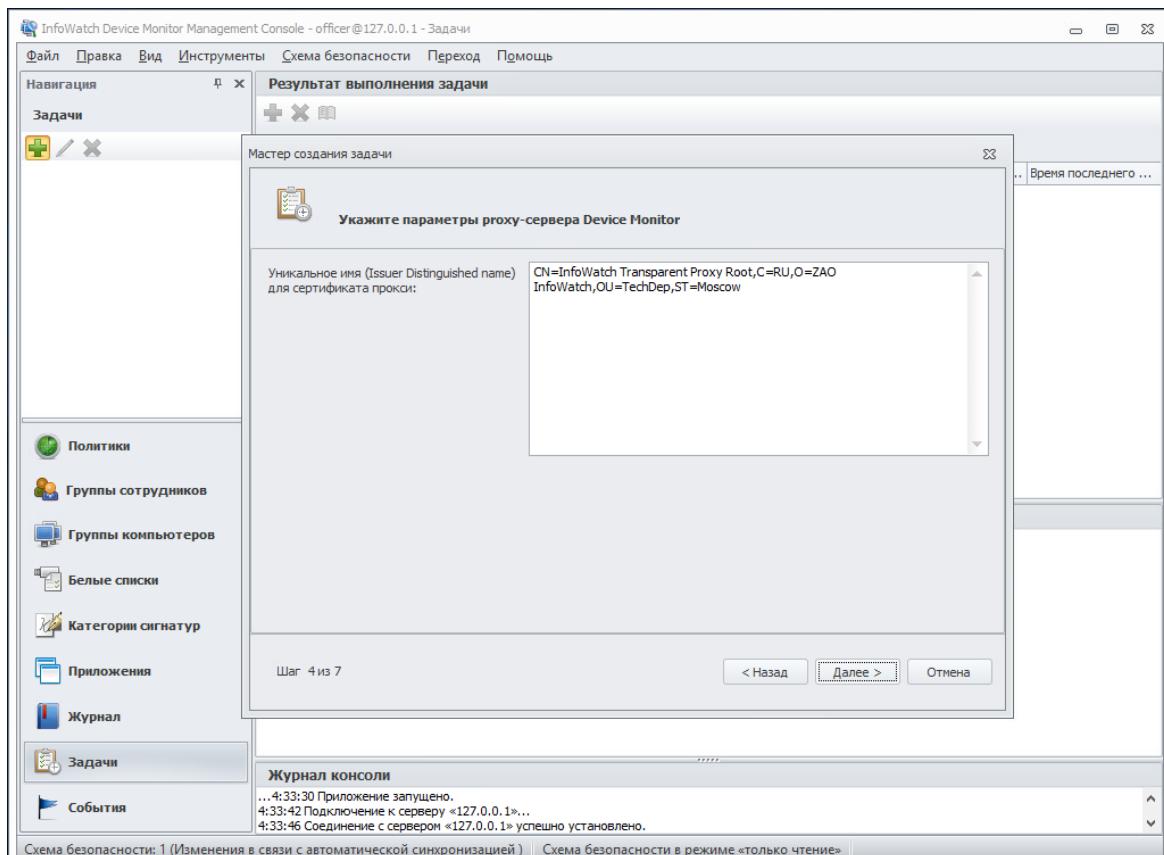


Выбираем компьютер агента

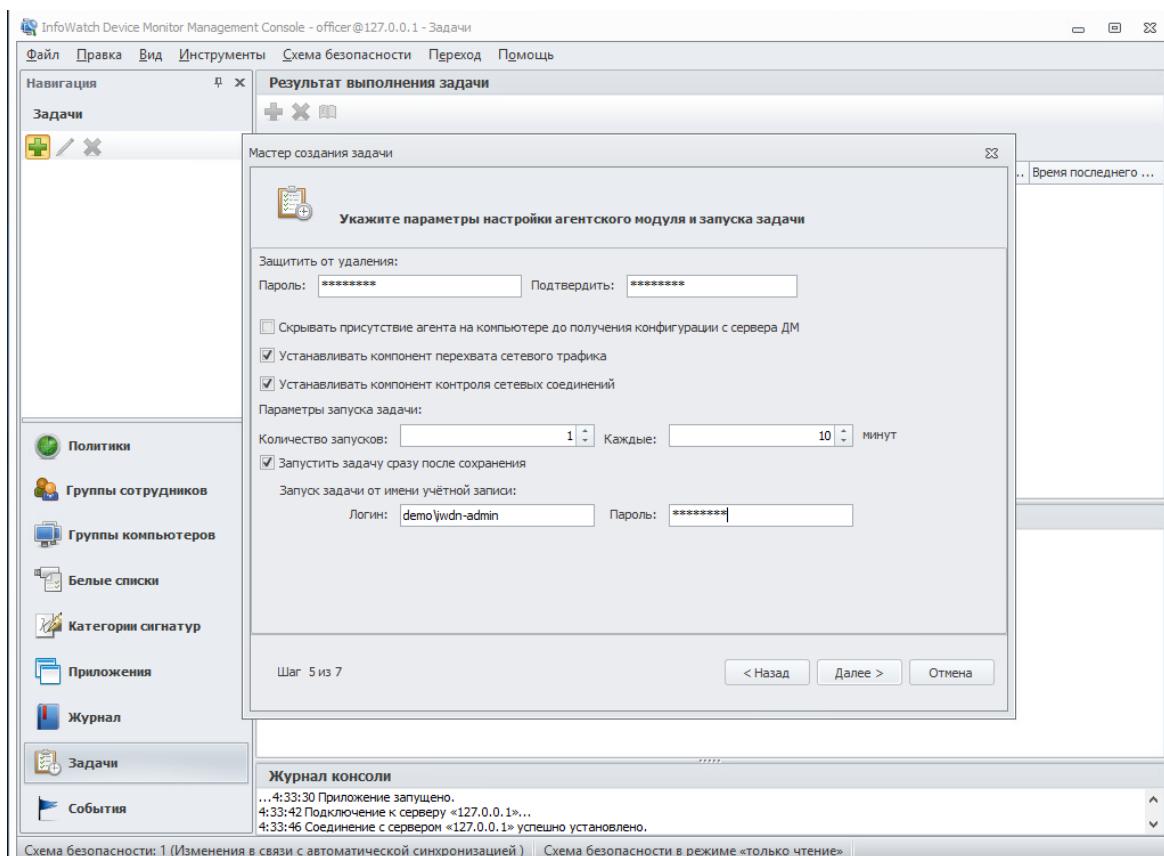


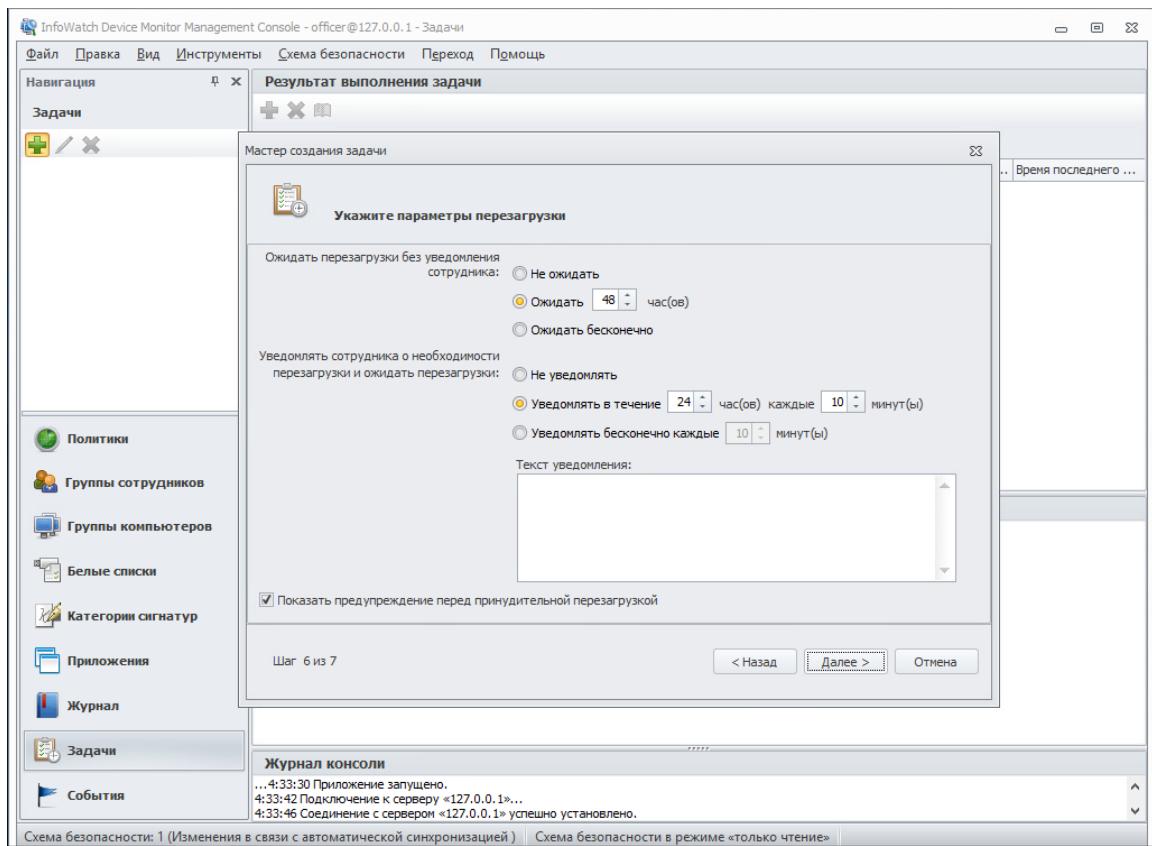
## Выбираем наш сервер IWDM



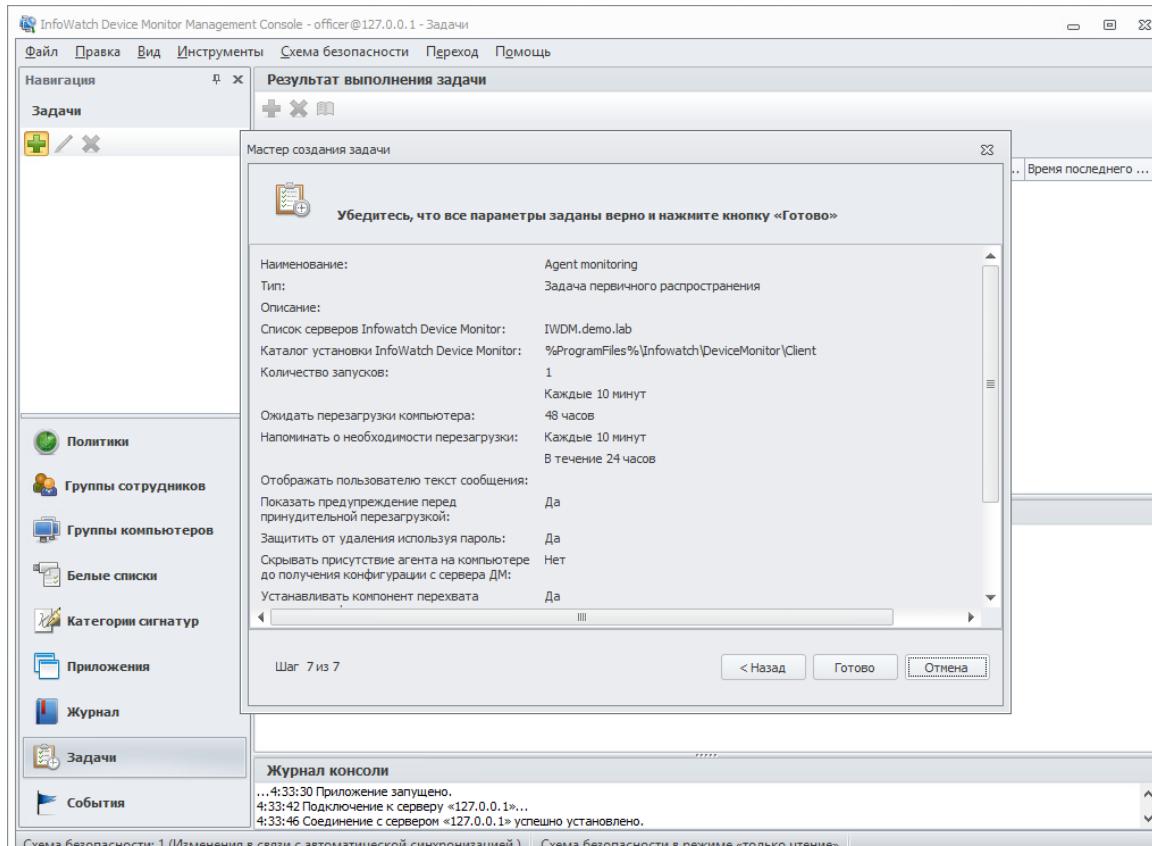


Вводим пароль, и учётную запись от которой будет запускаться задача





Готово



## Ожидаем подготовку

The screenshot shows the InfoWatch Device Monitor Management Console interface. The main window title is "InfoWatch Device Monitor Management Console - officer@127.0.0.1 - Задачи". The menu bar includes Файл, Дравка, Вид, Инструменты, Схема безопасности, Переход, Помощь. The left sidebar navigation includes Навигация, Задачи, Политики, Группы сотрудников, Группы компьютеров, Белые списки, Категории сигнатур, Приложения, Журнал, and Задачи. The central area displays a table titled "Результат выполнения задачи" (Task execution result) with columns: Имя, Статус выполн... (Status), Версия агента (Agent version), Операционная сис... (Operating system), Разрядность опер... (Processor bitness), Количество подкл... (Number of connections), and Время последнего ... (Last update time). One row is shown: DESKTOP-6U06DVU... with status "Подготовка" (Preparation) and timestamp 1 03.12.2021 7:35:08. Below this is a detailed view titled "Подробно" (Detailed) showing task configuration parameters like Наименование (Name: monitor), Тип (Type: Первичное распространение), and Статус (Status: Выполняется).

**Не забываем у компьютеров Клиент1 и Клиент2 включить сетевое обнаружение!**

## Ожидаем в процессе

The screenshot shows the InfoWatch Device Monitor Management Console interface. The main window title is "InfoWatch Device Monitor Management Console - officer@127.0.0.1 - Задачи". The menu bar includes Файл, Правка, Вид, Инструменты, Схема безопасности, Переход, Помощь. The left sidebar navigation menu includes Политики, Группы сотрудников, Группы компьютеров, Белые списки, Категории сигнатур, Приложения, Журнал, and Задачи (selected). The central area displays the "Результат выполнения задачи" (Task execution result) table with one row:

Имя	Статус выполнен...	Версия агента	Операционная сис...	Разрядность опер...	Количество подкл...	Время последнего ...
DESKTOP-6U06DVU...	В процессе		Windows 10	x64		1 03.12.2021 7:36:01

The "Подробно" (Detailed) section shows the task configuration:

Задача	
Наименование	monitor
Описание	
Тип	Первичное распространение
Статус	Выполняется
Период повторного запуска, мин	10
Количество попыток повторного запуска	1
Выводить сотруднику уведомления о работе Device Monitor Client	Да
Скрывать присутствие агента на компьютере до получения конфиг	Нет
Устанавливать компонент перехвата сетевого трафика	Да
Устанавливать компонент контроля сетевых соединений	Да

The "Журнал консоли" (Console log) shows the message "...7:33:35 Приложение запущено."

## Компьютер агента ожидает перезагрузки

InfoWatch Device Monitor Management Console - officer@127.0.0.1 - Задачи

Файл Дравка Вид Инструменты Схема безопасности Переход Помощь

Навигация Задачи

monitor

Результат выполнения задачи

Поместите сюда заголовок колонки для группировки по этой колонке

Имя	Статус выполнения задачи	Версия агента	Операционная с...	Разрядность оп...	Количество под...	Время последнего...
DESKTOP-6U06DVU...	Ожидание перезагрузки		Windows 10	x64		1 03.12.2021 7:39:01

Политики

Группы сотрудников

Группы компьютеров

Белые списки

Категории сигнатур

Приложения

Журнал

Задачи

Подробно

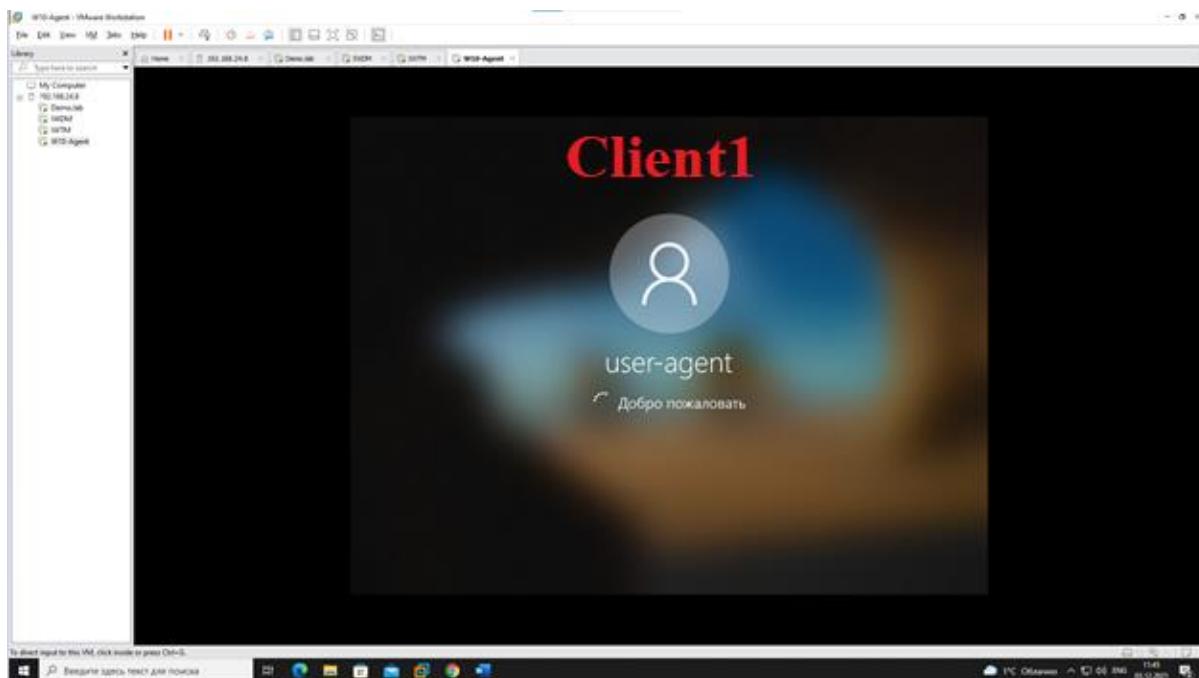
Задача

Наименование	monitor
Описание	
Тип	Первичное распространение
Статус	Выполняется
Период повторного запуска, мин	10
Количество попыток повторного запуска	1
Выvodить сотруднику уведомления о работе Device Monitor Client	Да
Скрывать присутствие агента на компьютере до получения конфиг	Нет
Устанавливать компонент перехвата сетевого трафика	Да
Устанавливать компонент контроля сетевых соединений	Да

Журнал консоли

...7:33:35 Приложение запущено.

Перезагружаем компьютер агента, и заходим под пользователя



Возвращаемся на компьютер IWDM и смотрим статус выполнения задачи — выполнено

The screenshot shows the InfoWatch Device Monitor Management Console interface. The main window title is "InfoWatch Device Monitor Management Console - officer @127.0.0.1 - Задачи". The menu bar includes: Файл, Правка, Вид, Инструменты, Схема безопасности, Переход, Помощь.

**Результат выполнения задачи**

Поместите сюда заголовок колонки для группировки по этой колонке

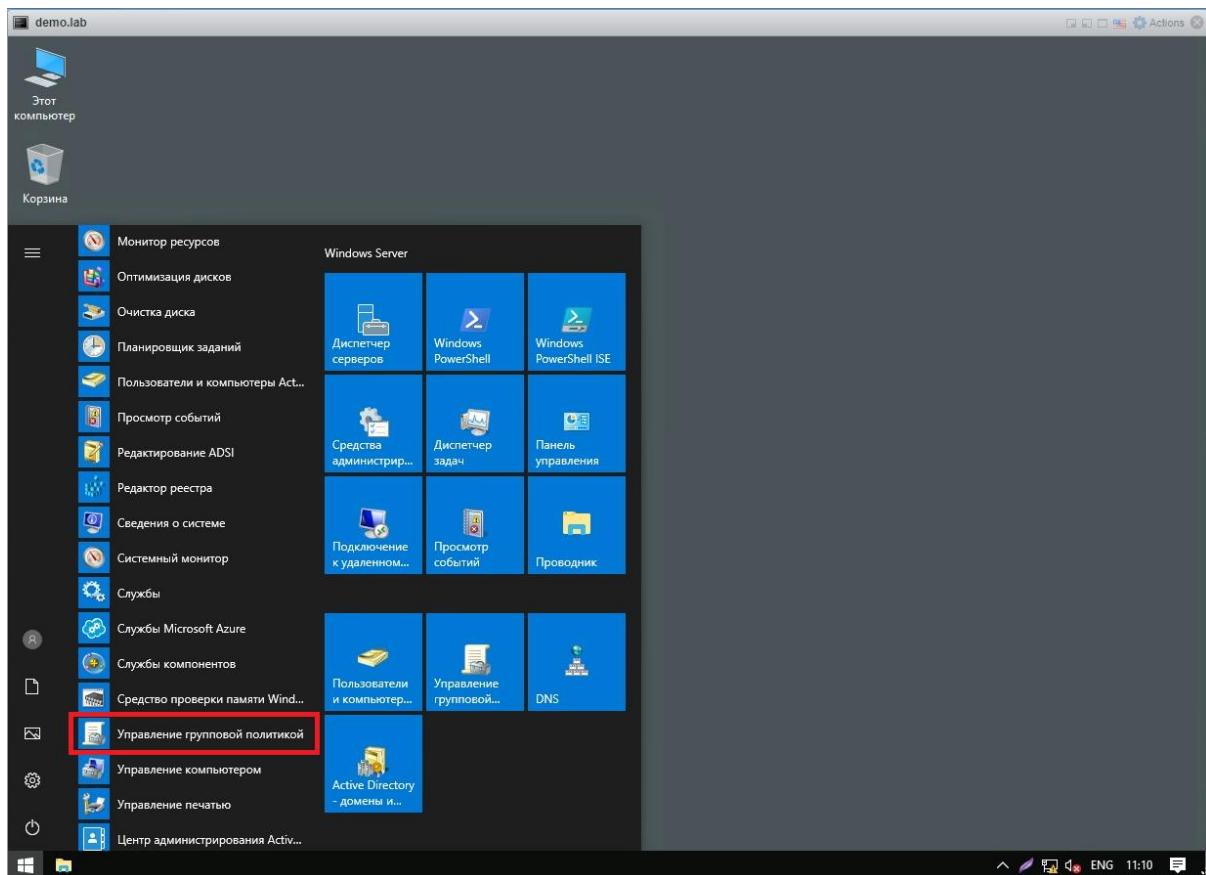
Имя	Статус выполнения задачи	Версия агента	Операционная с...	Разрядность оп...	Количество под...	Время последнего...
DESKTOP-6U06DVU...	Выполнено	6.11.5.468	Windows 10	x64	1	03.12.2021 7:47:05

**Подробно**

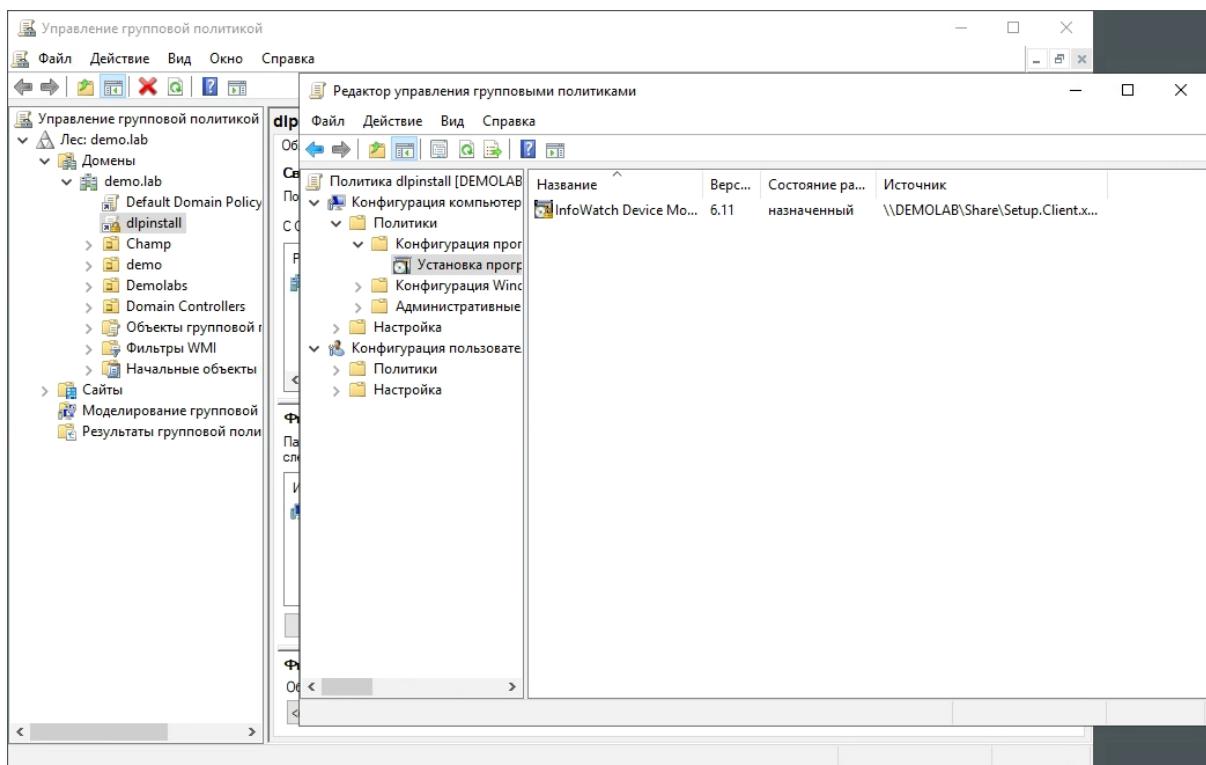
Задача	
Наименование	monitor
Описание	
Тип	Первичное распространение
Статус	Выполнена. Для каждого компьютера проверьте статус в поле "Статус..."
Период повторного запуска, мин	10
Количество попыток повторного запуска	1
Выводить сотруднику уведомления о работе Device Monitor Client	Да
Скрывать присутствие агента на компьютере до получения конфиг	Нет
Устанавливать компонент перехвата сетевого трафика	Да
Устанавливать компонент контроля сетевых соединений	Да

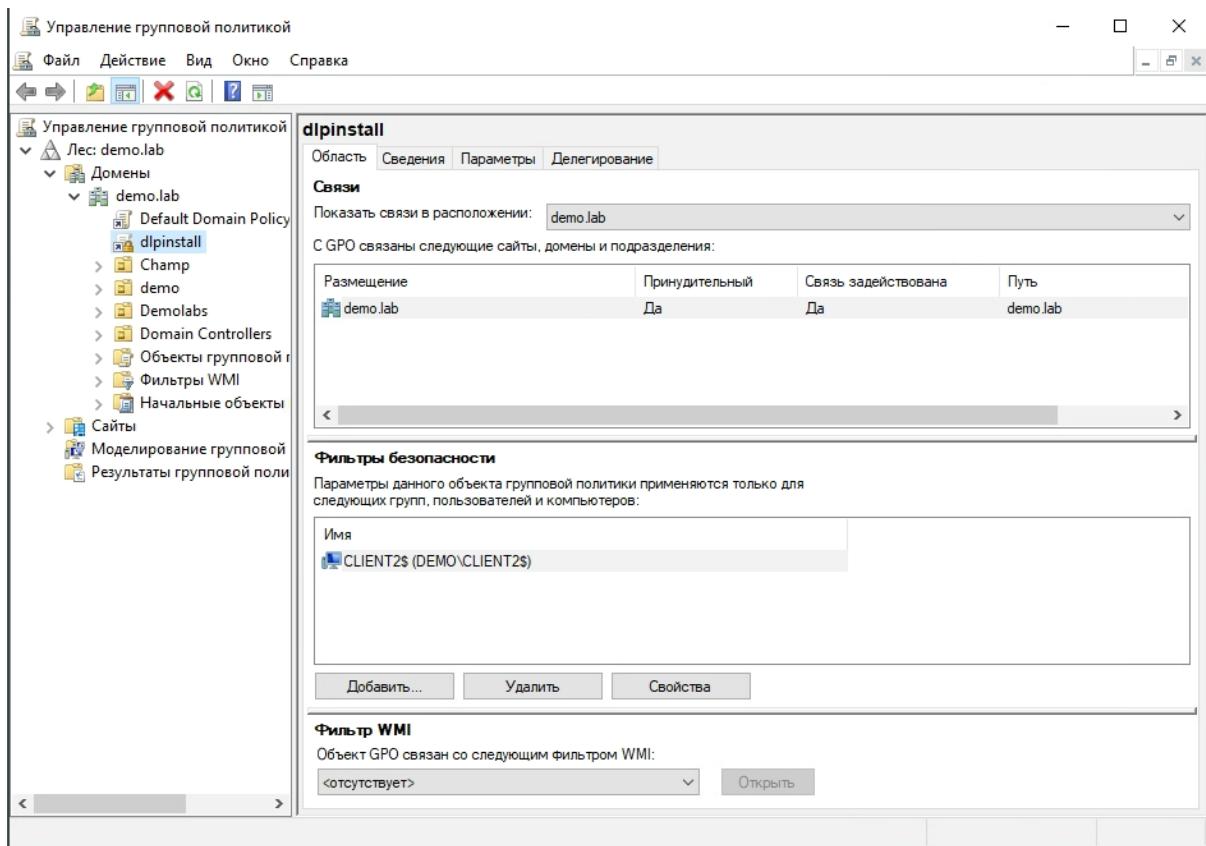
**Журнал консоли**

```
...7:33:35 Приложение запущено.  
7:34:16 Подключение к серверу «127.0.0.1»...  
7:34:20 Соединение с сервером «127.0.0.1» успешно установлено.
```



Файл установки выбираем 64 бита





The screenshot shows the 'Управление групповой политикой' (Group Policy Management) console. The left pane displays a tree structure of domains and objects under 'Лес: demo.lab'. The right pane is titled 'dlpininstall' and shows the 'Фильтр WMI' (WMI Filter) tab. It displays the message: 'Объект GPO связан со следующим фильтром WMI:' (The GPO object is associated with the following WMI filter:). A dropdown menu shows '<отсутствует>' (None) and a 'Открыть' (Open) button.

После этого перезапускаем компьютер – Клиент2

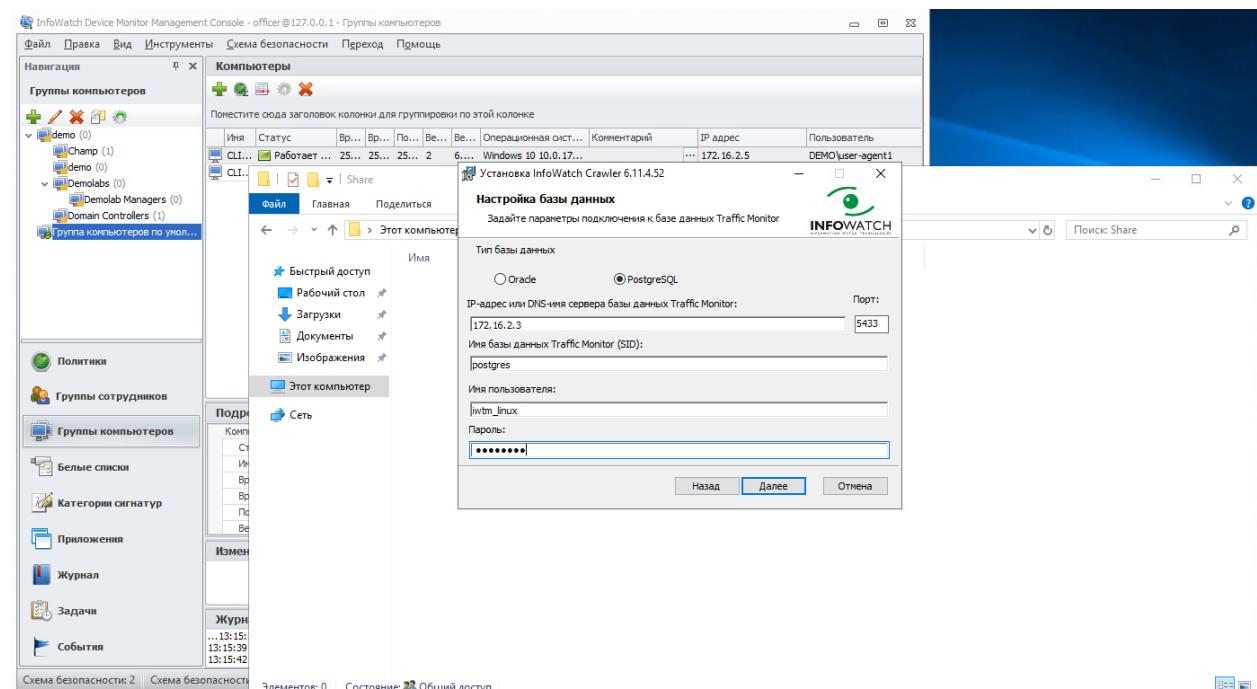
**Задание 5: Установка и настройка подсистемы сканирования сетевых ресурсов.**

Необходимо установить и настроить подсистему сканирования сетевых ресурсов на сервер с установленным сервером агентского мониторинга с настройками по умолчанию.

Необходимо создать общий каталог Share в корне диска сервера IWDM и установить права доступа на запись и чтение для всех пользователей домена.

Необходимо настроить подсистему сканирования сетевых ресурсов на автоматическое ежедневное сканирование только ранее созданного каталога. Для работы подсистемы может потребоваться редактирования конфигурационных файлов (для устранения предупреждения).

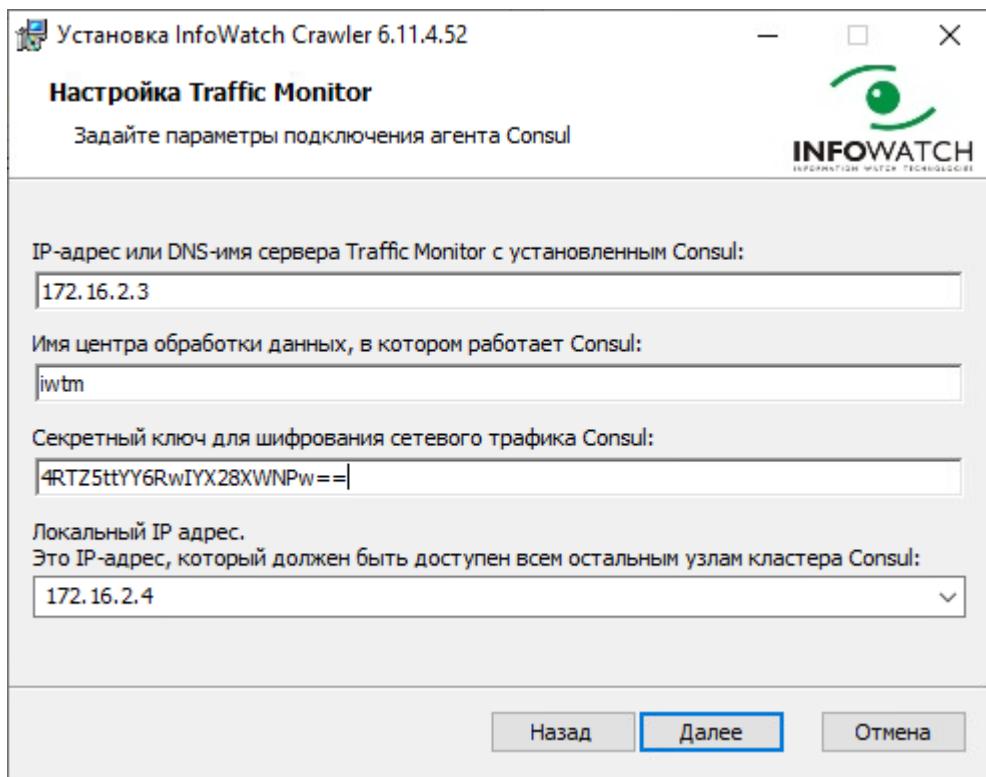
## Скринов создание общей папки – нет!



```
}[root@iwtm etc]# cd /opt/iw/tm5/etc/consul_
```

```
[root@iwtm consul]# ls
consul_db_check.json  consul_kv_watch_analysis.json  consul_kv_watch_messed.json
consul.json           consul_kv_watch_icap.json
[root@iwtm consul]# cat consul.json
```

```
[root@iwtm consul]# cat consul.json
{
    "bootstrap_expect": 1,
    "client_addr": "127.0.0.1",
    "data_dir": "/opt/iw/tm5/var/consul",
    "datacenter": "iwtm",
    "disable_update_check": true,
    "enable_syslog": true,
    "encrypt": "4RTZ5ttYY6RwIYX28XWNPw==",
    "leave_on_terminate": false,
    "log_level": "WARN",
    "rejoin_after_leave": true,
    "server": true,
    "skip_leave_on_interrupt": true
}[root@iwtm consul]#
```



Плагины

- InfoWatch Crawler

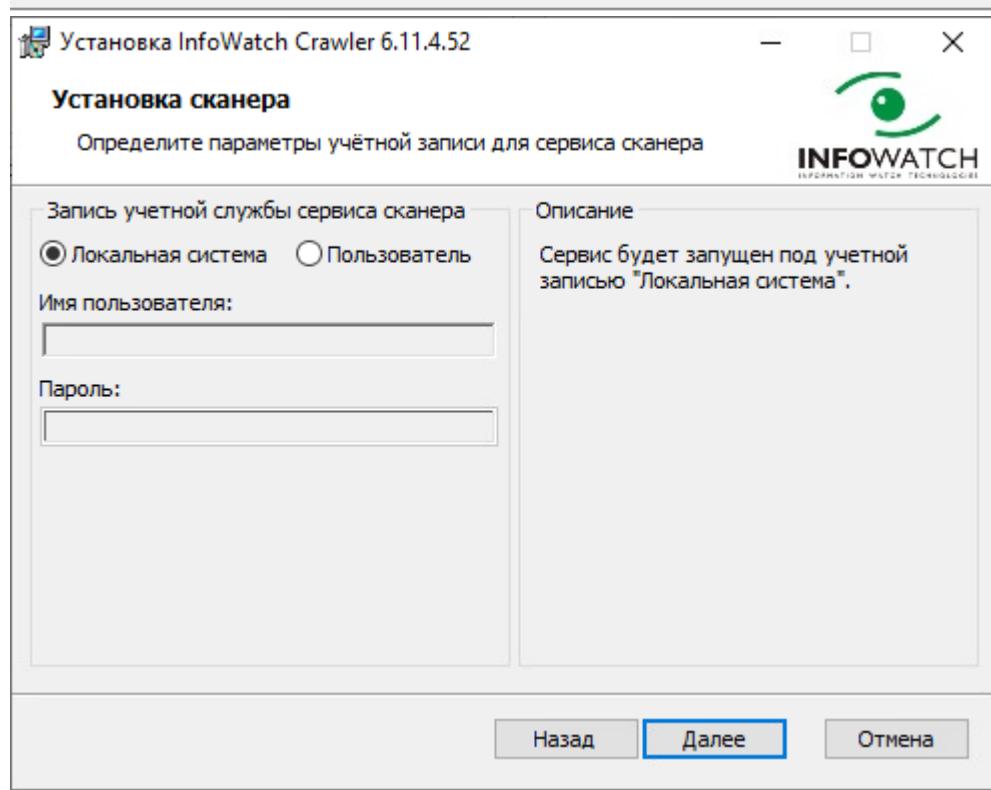
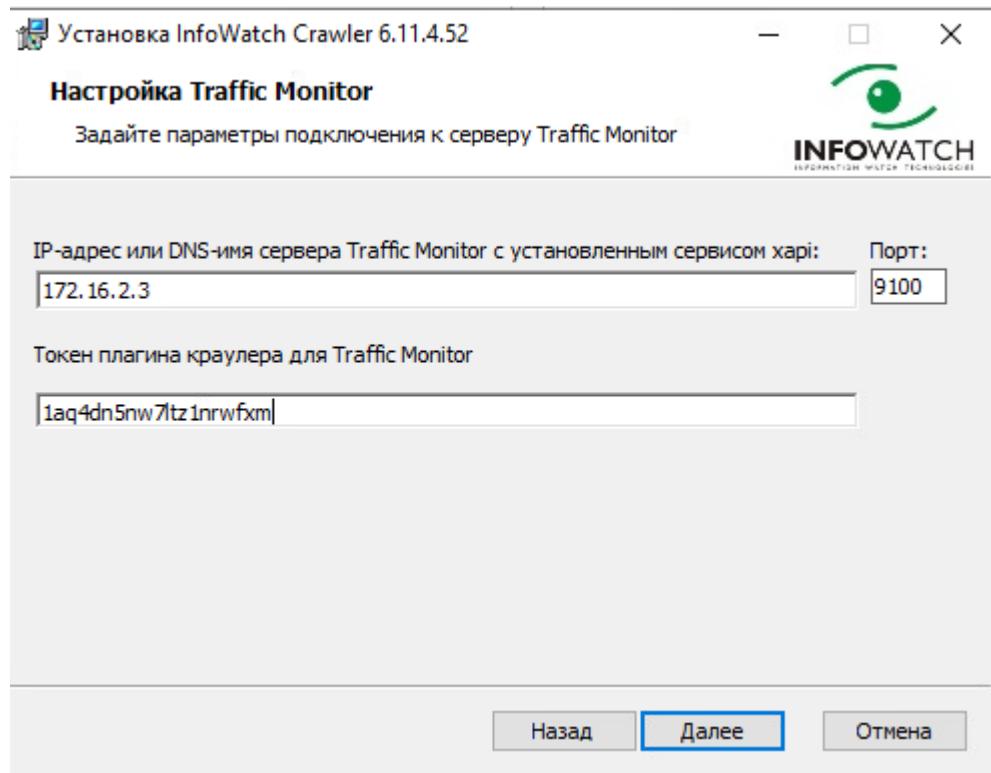
Прием событий Краулер  
Производитель: IW  
Версия 6.11.5

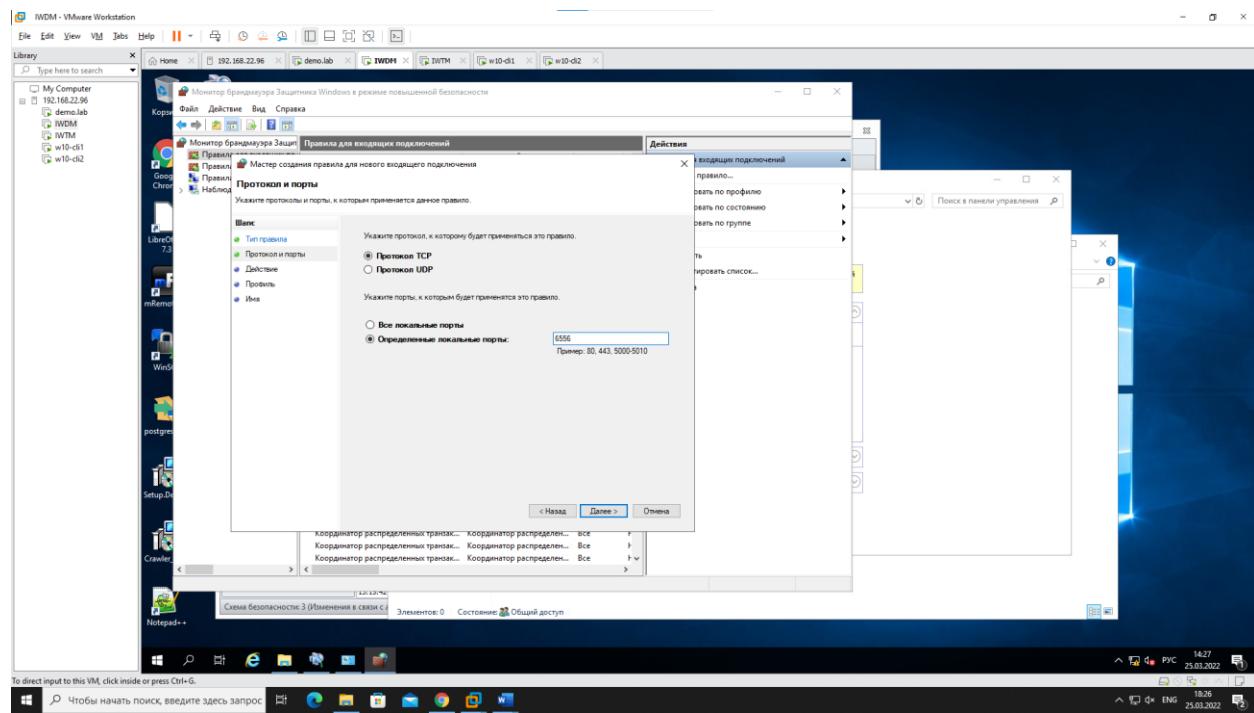
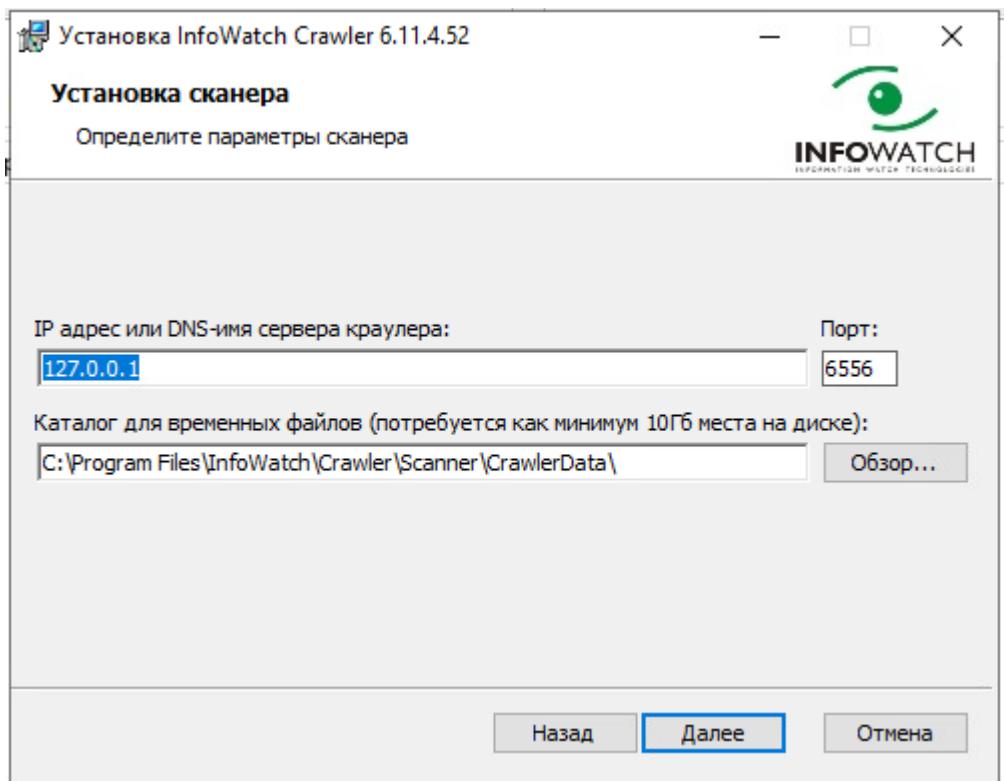
Плагины	Лицензии	Токены
<input type="button" value="+"/> <input type="button" value="○"/> <input type="button" value="×"/>		
Статус	Имя	Содержание
Активный	Token-2	1aq4dn5nw7ltz1nrwfxm

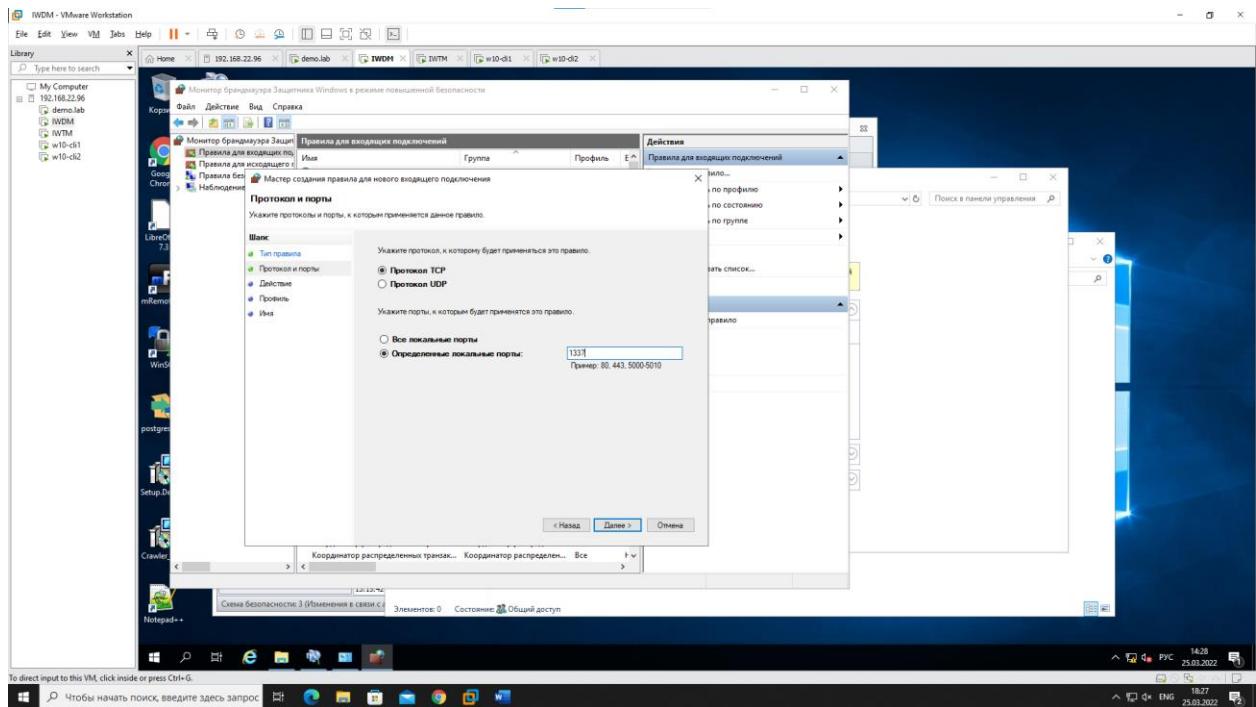
```
[root@iwtm etc]# cd /opt/iw/tm5/etc
```

```
[root@iwtm etc]# nano web.conf
```

```
},
"crawler": {
    "enabled": 1
},
```







```
GNU nano 2.3.1          File: /etc/hosts

127.0.0.1  localhost localhost.localdomain localhost4 localhost4.localdomain4
::1        localhost localhost.localdomain localhost6 localhost6.localdomain6
172.16.2.3  iwtm.demo.lab  iwtm
172.16.2.4  iwdm.demo.lab  iwdm
```

## Задание 6: Проверка работоспособности системы

Необходимо создать проверочную политику на правило передачи, копирования, хранения и буфера обмена (или работы в приложениях), все 4

варианта срабатывания событий для данных, содержащих некий термин,

установить уровень угрозы для всех событий, добавить тег.

Проверить срабатывание всеми четырьмя возможными способами (передачи, копирования, хранения и буфера обмена, хотя бы 1 событие на каждый

тип) с помощью виртуальной машины нарушителя 1 с установленным агентом.

Сделать одну выборку, в которой будет отображено только по одному

событию каждого типа, настроив конструктор выборки вручную.

Зафиксировать выполнение скриншотом выполненной выборки или конструктора выборки.

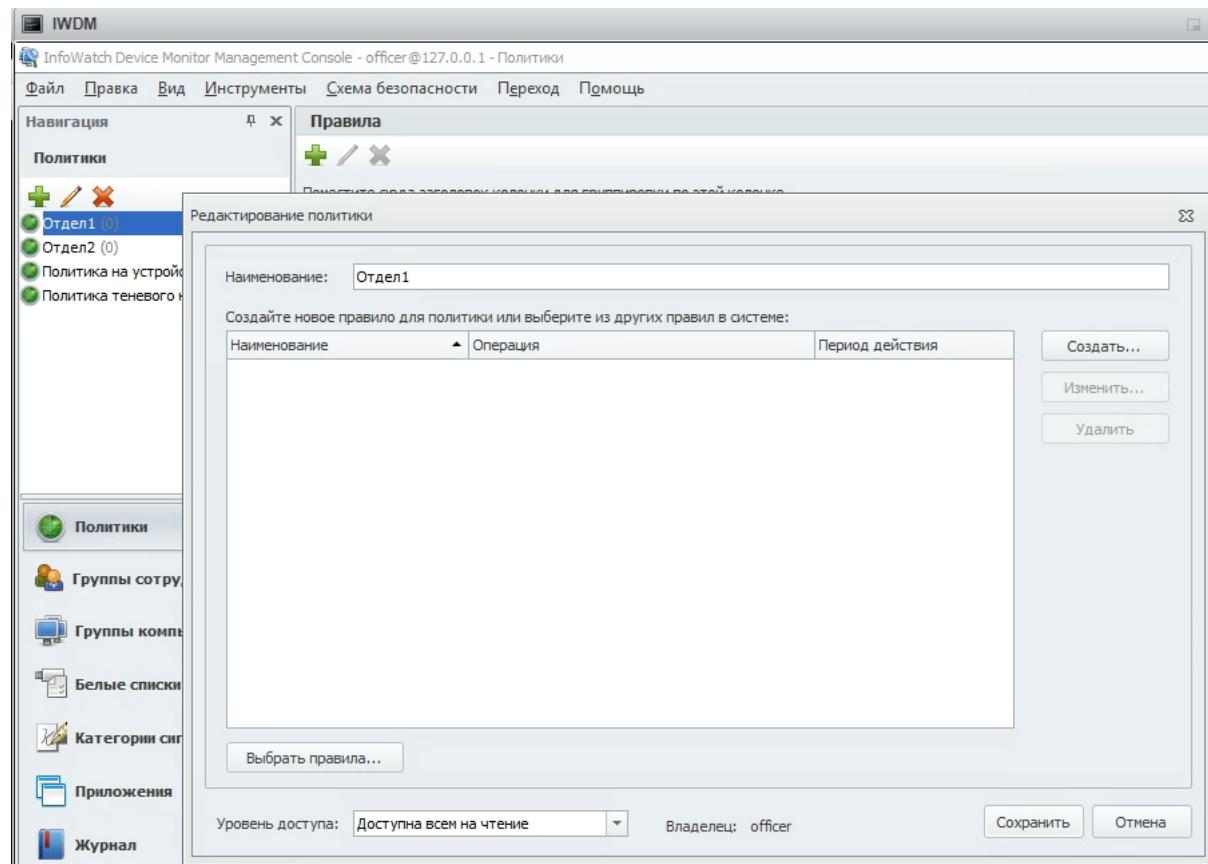
**Не делал!**

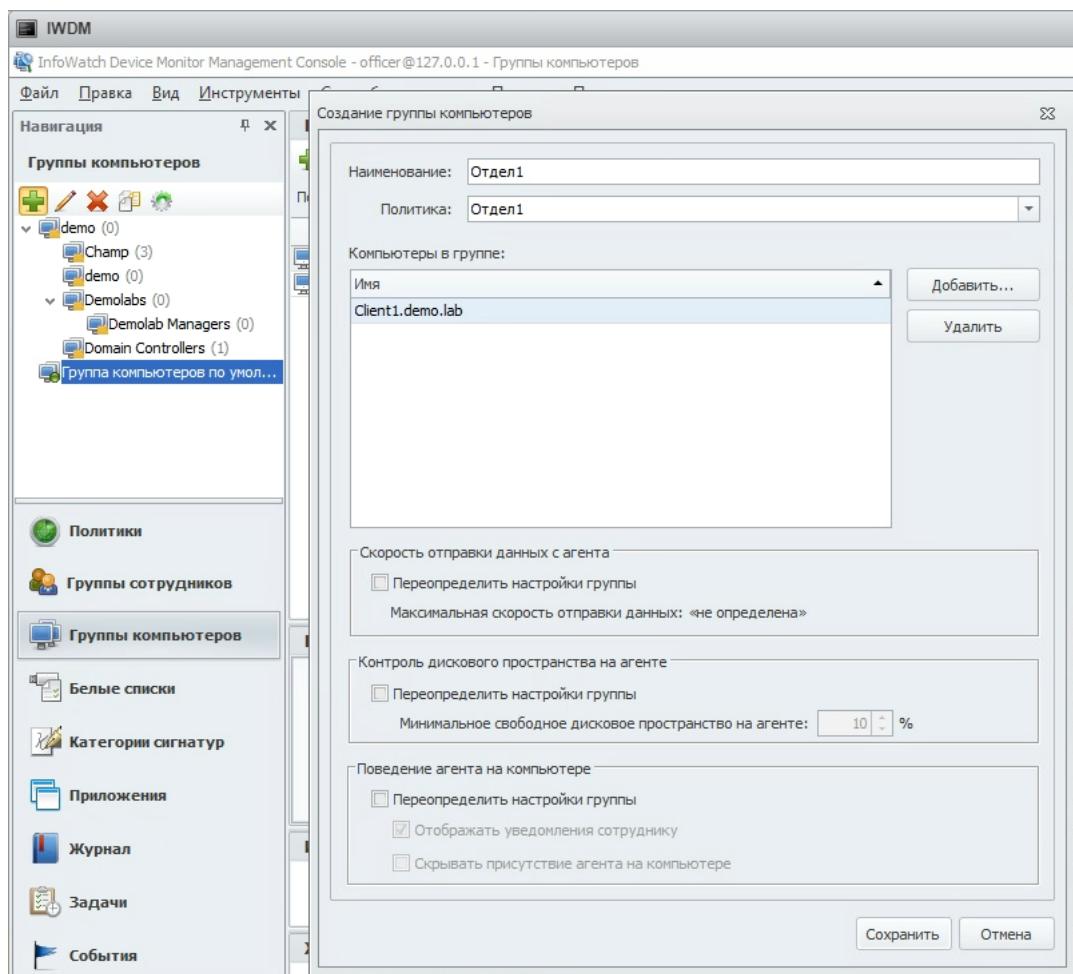
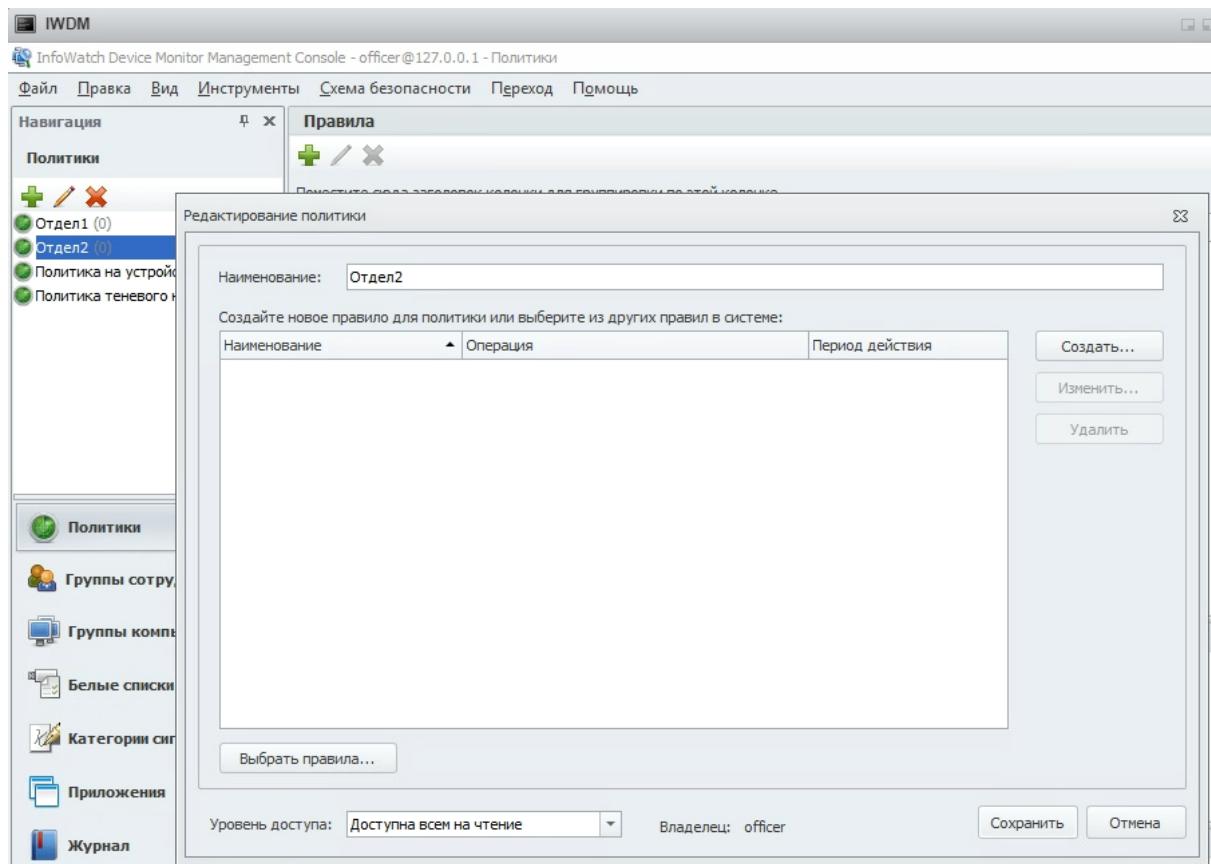
## **Модуль 2.**

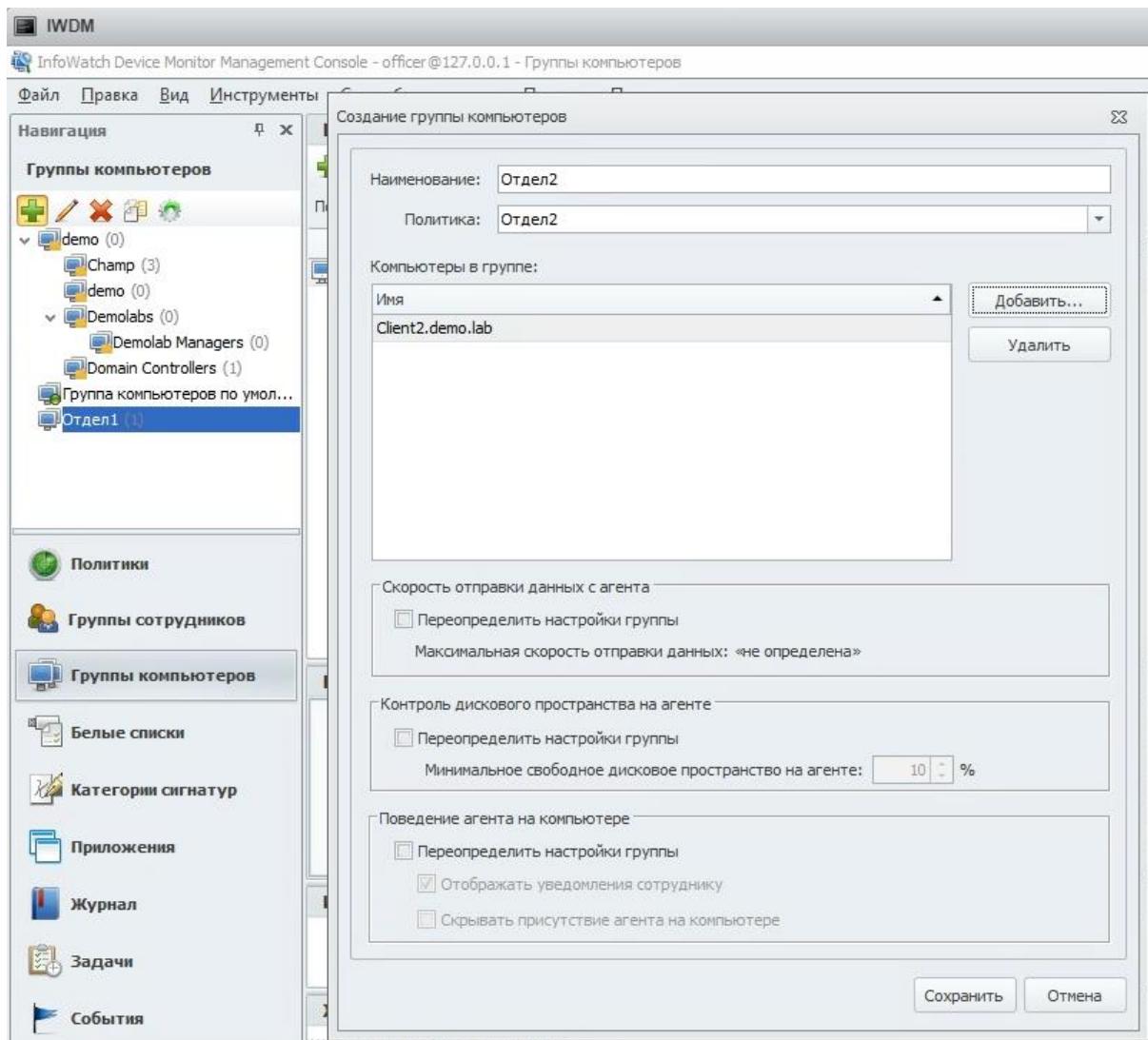
### **Задание 1**

Необходимо создать 2 новых группы компьютеров: «Отдел1» и «Отдел2», а также создать 2 новых политики: «Отдел1» и «Отдел2». Каждая из политик должна применяться только на соответствующие группы. Компьютер 1 необходимо перенести в Отдел1, а компьютер 2 — в Отдел2.

Зафиксировать выполнение скриншотом.



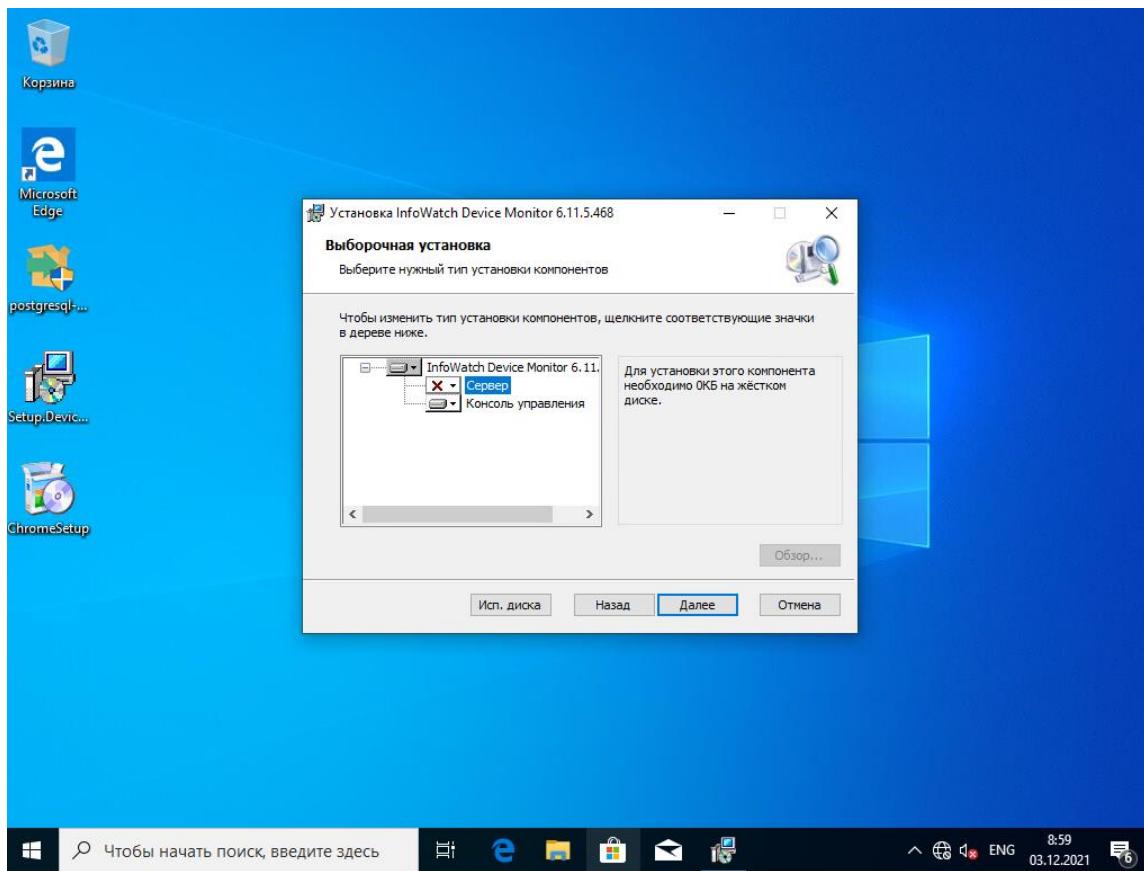




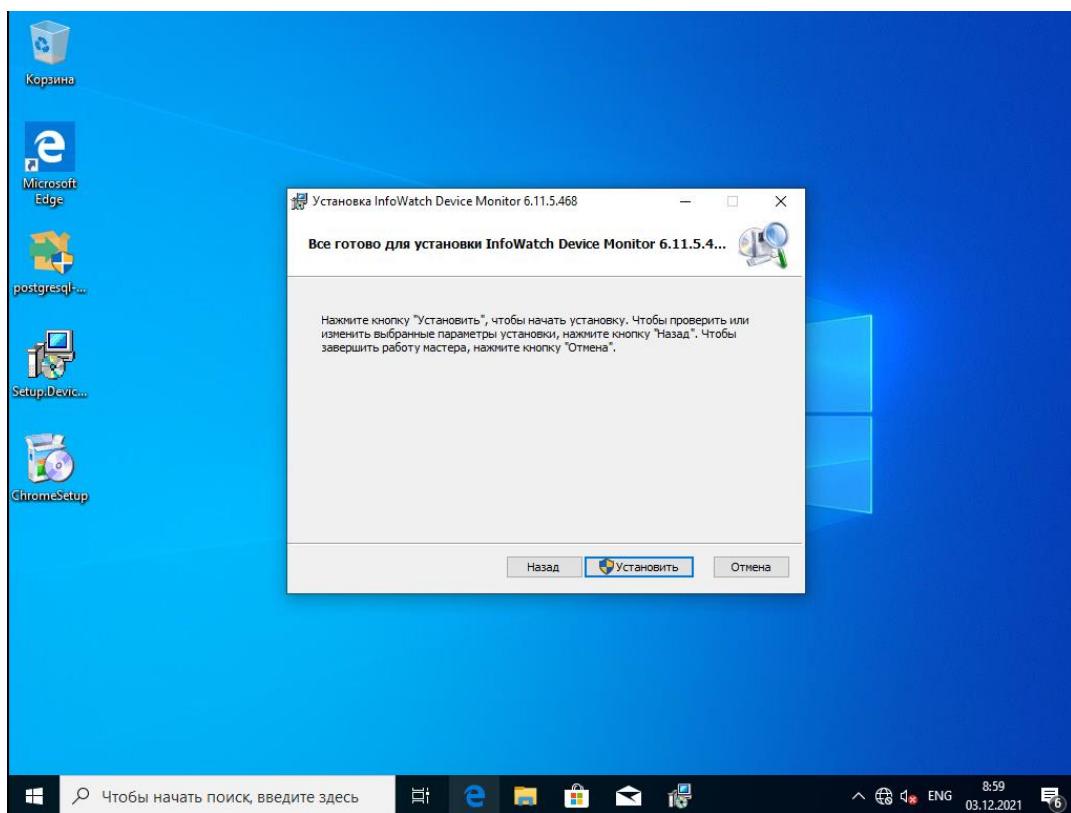
## Задание 2

Для удобства работы офицера безопасности необходимо установить дополнительную консоль управления сервером агентского мониторинга на машину W10-agent1 для удаленного доступа к серверу агентского мониторинга. Следующие правила создаются в политике «Отдел1».

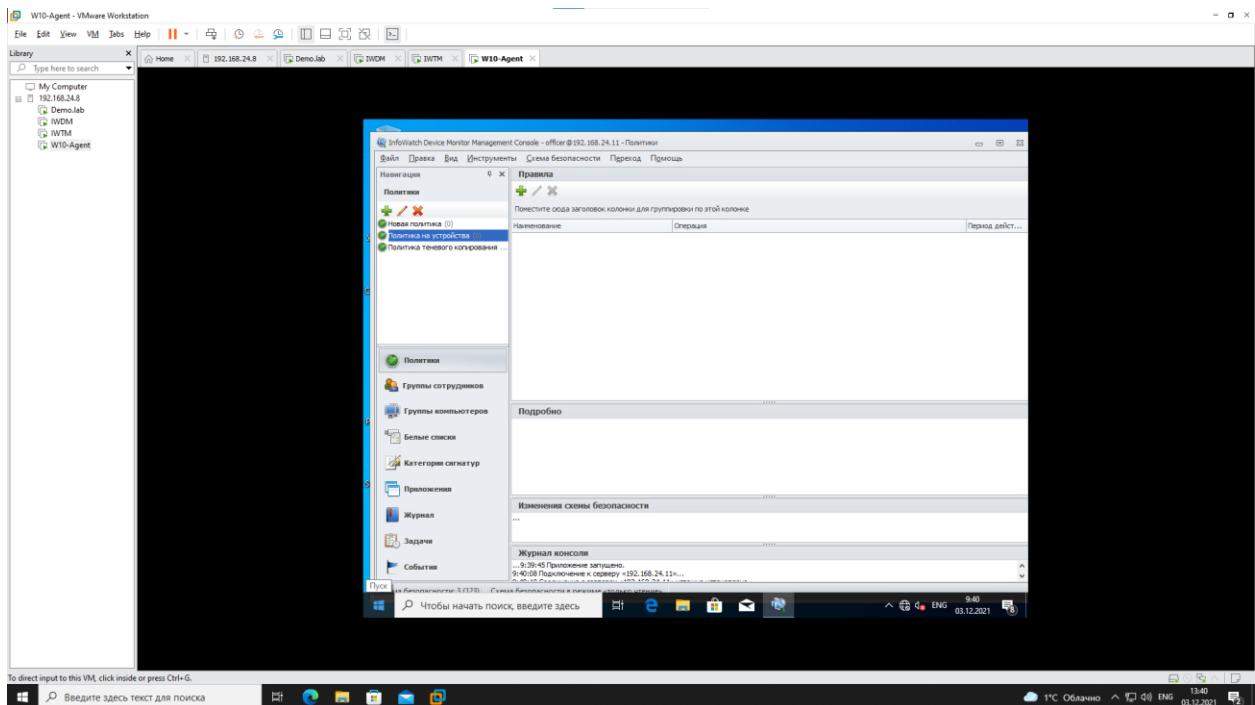
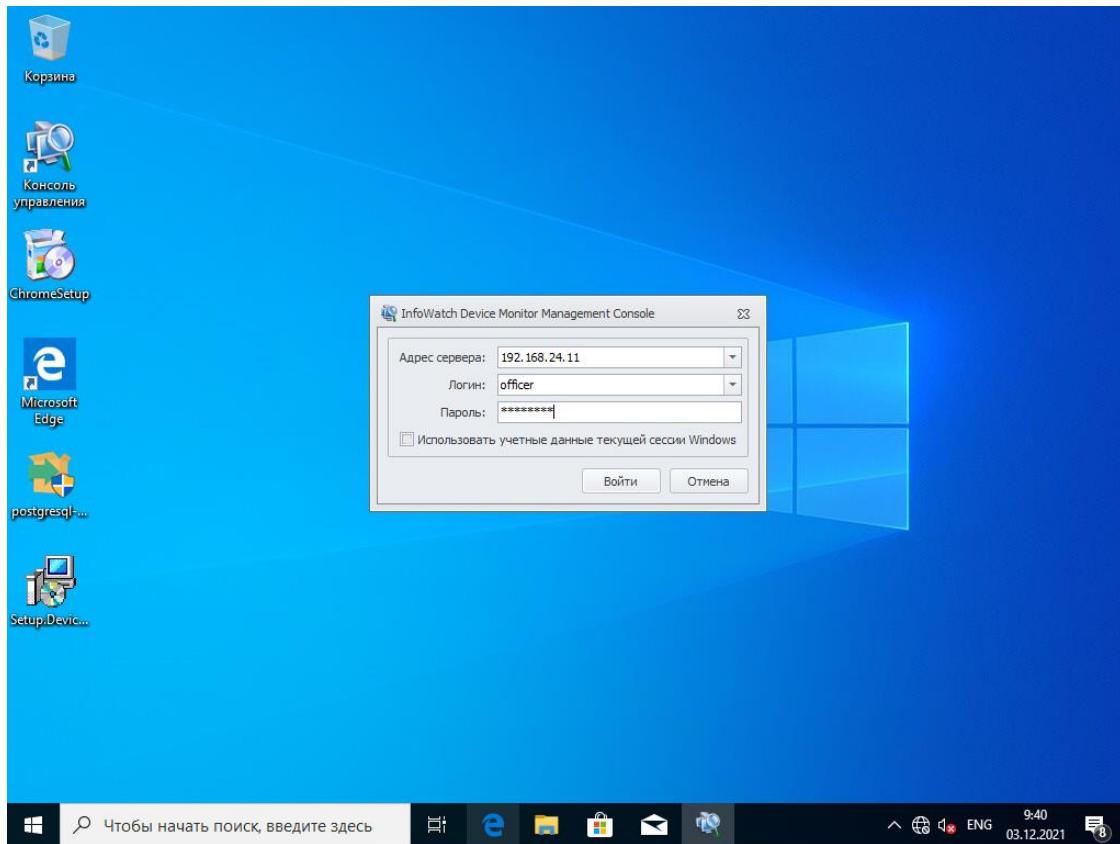
Убираем сервер, оставляем только консоль управления



Установили InfoWatch Device Monitor



Заходим в InfoWatch Monitor Management Console (192.168.24.11, Ip – адрес IWDM)



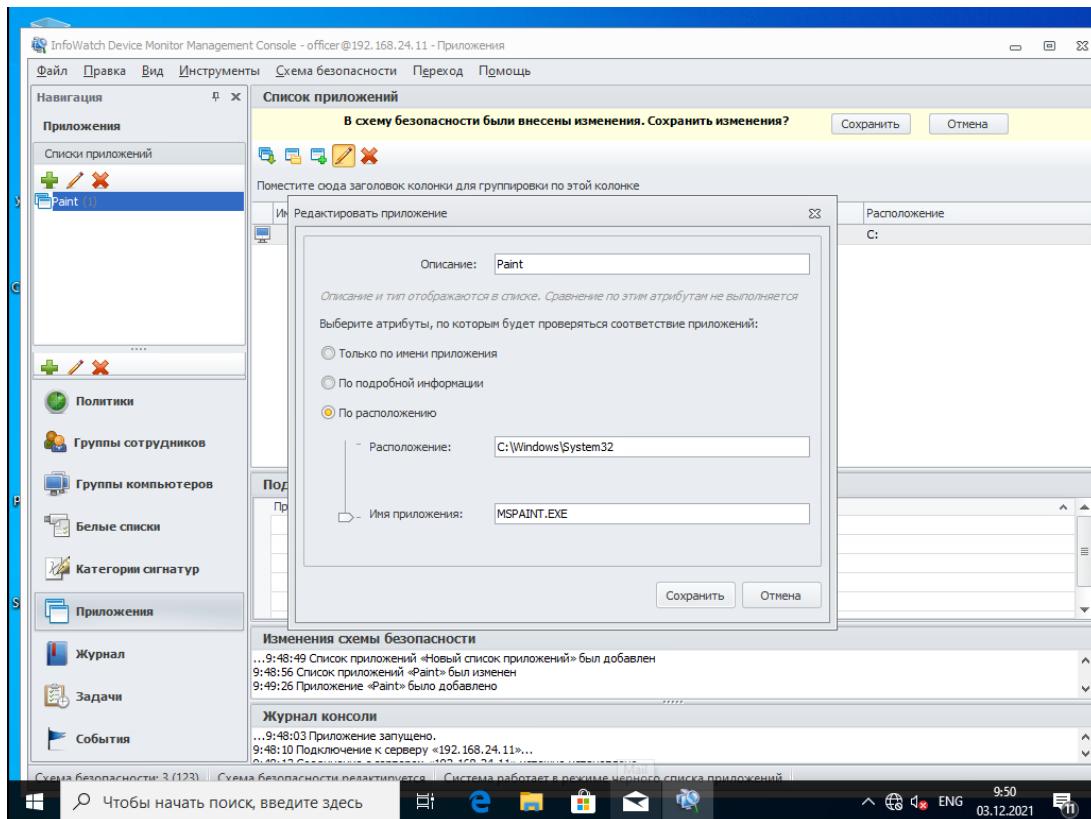
Следующие правила создаются в политике «Отдел1»

## Правило 1

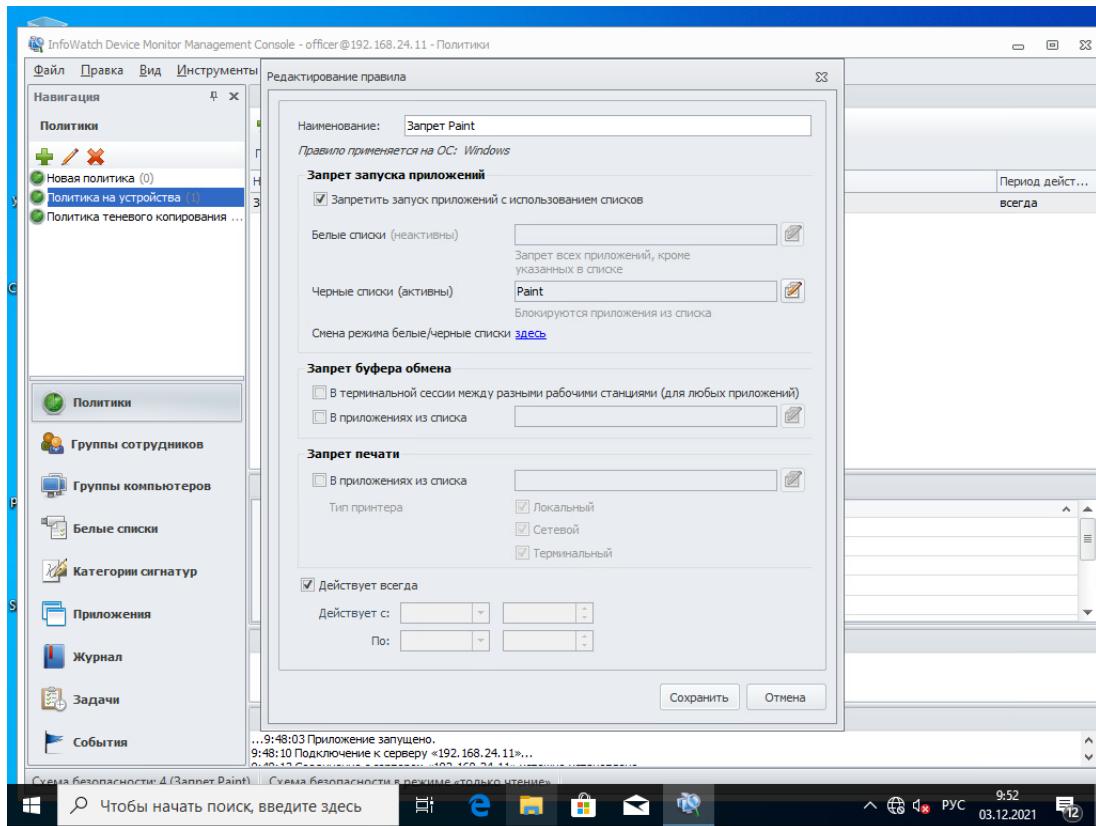
Необходимо запретить пользоваться Microsoft Paint, так как участились случаи подделки печатей компании.

Проверить работоспособность и зафиксировать выполнение скриншотом.

Заходим в приложение, добавляем приложение Paint и редактируем его, указывая путь до программы и имя программы



Переходим в политики, далее переходим в редактирование правил



Задокументировать скриншотами необходимо!

## Правило 2

Необходимо запретить создание снимков экрана в табличных процессорах для предотвращения утечки секретных расчетов и баз данных.  
Проверить работоспособность и задокументировать выполнение скриншотом.

создавать. Для того, чтобы создать и настроить правило, вам необходимо вернуться к разделу «Политики» в Device Monitor Console и перейти к политики «Отдел 1», после чего нажать кнопку «Создать правило...» (не путать с «создать политику...») обозначенную уже привычным зеленым плюсиком.

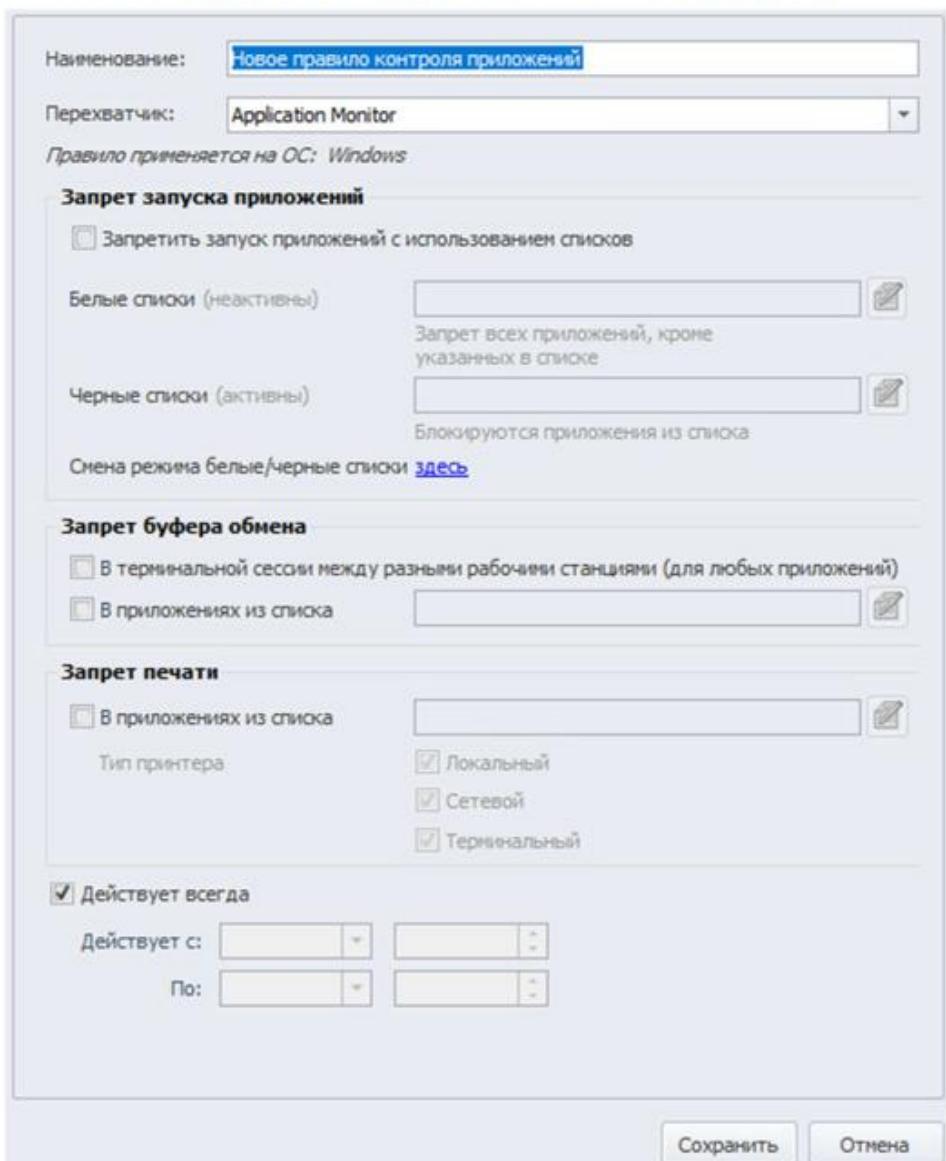


Рисунок 57 – «Создание правила»

Правило 1, требующее запретить создание снимков экрана в табличных процессорах (Excel, Calc) будет использовать Application Monitor. Для того, чтобы запретить запуск какого-либо приложения, его необходимо добавить в список. Для того, чтобы создать список перейдите ко вкладке «Приложения» в Device Monitor Console. Во вкладке «Приложения», вы увидите все приложения, которые запускали на клиентских компьютерах, и информацию о них.

Дата	Компьютер	Пользователь	Имя прилож...	Описание	Название п...	Издатель	Расположение
17.02.2022 1...	W10-CLI1.DEMO.LAB	DEMO\USER...	taskhostw.exe	Host Proces...	Microsoft® ...	O=Microsoft...	c:\windows\system32\
17.02.2022 1...	W10-CLI1.DEMO.LAB	DEMO\USER...	background...	Background ...	Microsoft® ...	O=Microsoft...	c:\windows\system32\
17.02.2022 1...	W10-CLI1.DEMO.LAB	<система>	sppsvc.exe	Microsoft So...	Microsoft® ...	O=Microsoft...	c:\windows\system32\
17.02.2022 1...	W10-CLI1.DEMO.LAB	<система>	SppExtCom...	KMS Connec...	Microsoft® ...		c:\windows\system32\
17.02.2022 1...	W10-CLI1.DEMO.LAB	<система>	RUXIMICS.exe	Reusable UX...	Microsoft® ...	O=Microsoft...	c:\program files\ruxim\
17.02.2022 1...	W10-CLI2.DEMO.LAB	<система>	taskhostw.exe	Host Proces...	Microsoft® ...	O=Microsoft...	c:\windows\system32\
17.02.2022 1...	W10-CLI2.DEMO.LAB	<система>	sppsvc.exe	Microsoft So...	Microsoft® ...	O=Microsoft...	c:\windows\system32\
17.02.2022 1...	W10-CLI2.DEMO.LAB	<система>	SppExtCom...	KMS Connec...	Microsoft® ...		c:\windows\system32\
17.02.2022 1...	W10-CLI2.DEMO.LAB	<система>	sc.exe	Service Con...	Microsoft® ...		c:\windows\system32\
17.02.2022 1...	W10-CLI2.DEMO.LAB	<система>	UpdateNotifi...	Update Noti...	Microsoft® ...	O=Microsoft...	c:\windows\system32\...
17.02.2022 1...	W10-CLI2.DEMO.LAB	<система>	RUXIMICS.exe	Reusable UX...	Microsoft® ...	O=Microsoft...	c:\program files\ruxim\
17.02.2022 1...	W10-CLI2.DEMO.LAB	<система>	CONHOST.EXE	Console Win...	Microsoft® ...		c:\windows\system32\
17.02.2022 1...	W10-CLI2.DEMO.LAB	<система>	RUNDLL32.EXE	Windows ho...	Microsoft® ...		c:\windows\system32\
17.02.2022 1...	W10-CLI2.DEMO.LAB	<система>	GoogleUpd...	Google Inst...	Google Updat...	O=Google L...	c:\program files(x86)\...
17.02.2022 1...	W10-CLI2.DEMO.LAB	DEMO\USER...	CTFMON.EXE	CTF Loader	Microsoft® ...		c:\windows\system32\
17.02.2022 1...	W10-CLI2.DEMO.LAB	DEMO\USER...	EXPLORER....	Windows Ex...	Microsoft® ...	O=Microsoft...	c:\windows\
17.02.2022 1...	W10-CLI2.DEMO.LAB	DEMO\USER...	ShellFvneria	Windows Sh...	Microsoft® ...	O=Microsoft...	c:\windows\system32\

Рисунок 58 – «Протокол приложений»

Поскольку, согласно заданию, необходимо запретить создание скриншотов в Excel или Calc, нужно сначала этот табличный препроцессор открыть на клиентской машине – w10-cli1. Перейдите к соответствующей виртуальной машине и откройте LibreOffice (или Excel). Для того чтобы найти приложения воспользуйтесь поиском Windows: для Excel – введите запрос «Excel»; для Calc – введите запрос «LibreOffice Calc». Откройте табличный препроцессор и дождитесь полного запуска, после чего вернитесь к Device Monitor Console. Обновите вкладку «Приложения» (войдите в любую другую вкладку и вернитесь обратно) и найдите в колонке «Имя приложения» имя «scalc.exe», что соответствует LibreOffice Calc. Кликните по строке правой кнопкой мыши и, в контекстном меню, выберите «Добавить приложение в список вручную» и в открывшемся окне «Создать новый...», назовите новый список произвольным именем (рекомендую называть в соответствии с создаваемым правилом), а затем добавьте приложение в список.

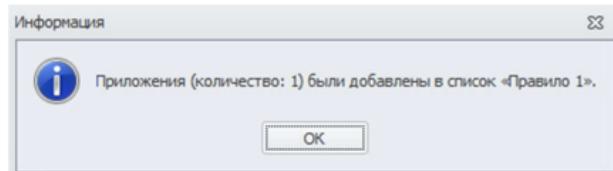


Рисунок 59 – «Успешное добавление приложения»

Вернитесь во вкладку «Политики», выберите политику «Отдел 1» и нажмите уже знакомую кнопку «Создать правило...» и назовите его «Правило 1». В качестве перехватчика установите ScreenShot Control Monitor. Отметьте радиобокс (кружочек для выбора) «Если запущены приложения:» в пункте «Запрещать сотруднику создавать снимок экрана». При отметке радиобокса, вас попросят выбрать список приложений – выберите ранее созданный список «Правило 1». Все должно выглядеть в соответствии с рисунком 60. Сохраните правило. На этом, создание правила 1 окончено, перейдем ко правилу 2.

52

worldskills  
Russia

Типовое конкурсное задание  
Регионального чемпионата цикла 2021-2022 WorldSkills Russia по компетенции  
«Корпоративная защита от внутренних угроз информационной безопасности»

Создание правила

Наименование: Правило 1

Перехватчик: ScreenShot Control Monitor

Правило применяется на ОС: Windows

Запрещать сотруднику создавать снимок экрана

Всегда

Если запущены приложения: Правило 1

Действует всегда

Действует с: [ ] [ ]

По: [ ] [ ]

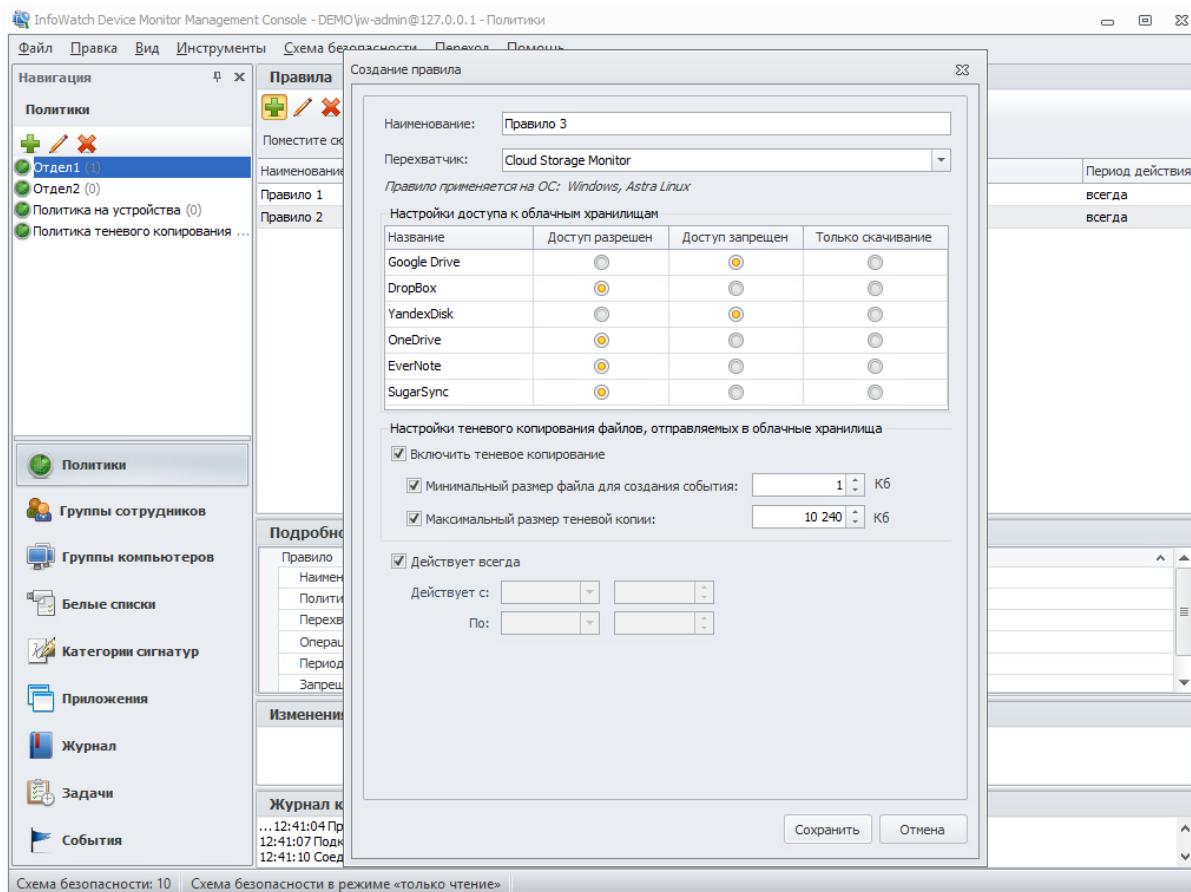
Рисунок 60 – «Правило 1»

Зафиксировать скриншотами необходимо!

### Правило 3

Ограничить доступ к облачным хранилищам GoogleDrive и YandexDisk.

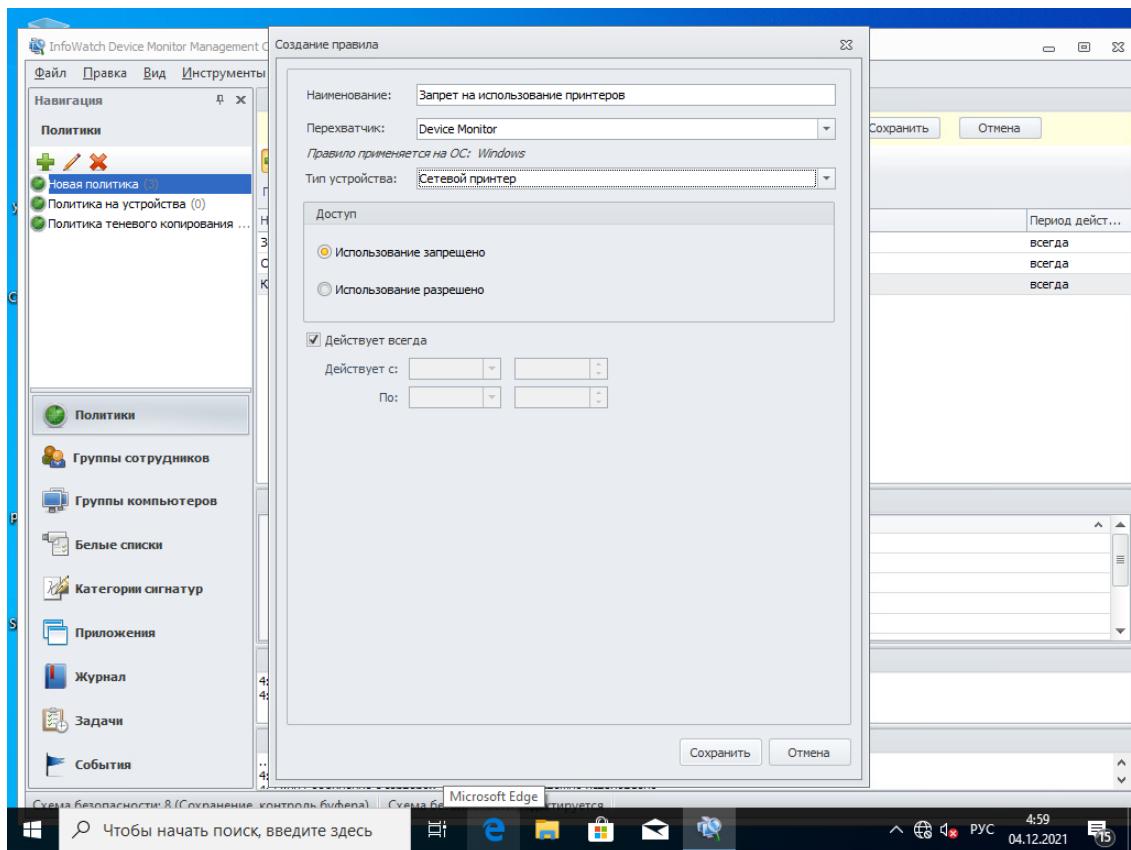
Проверить работоспособность и зафиксировать выполнение



### Правило 4

Необходимо запретить печать на сетевых принтерах.

Задокументировать создание политики скриншотом.



Зафиксировать создание политики скриншотом.

### Правило 5

Необходимо запретить запись файлов на все съёмные носители информации, при этом оставить возможность считывания информации.

Проверить работоспособность и зафиксировать выполнение

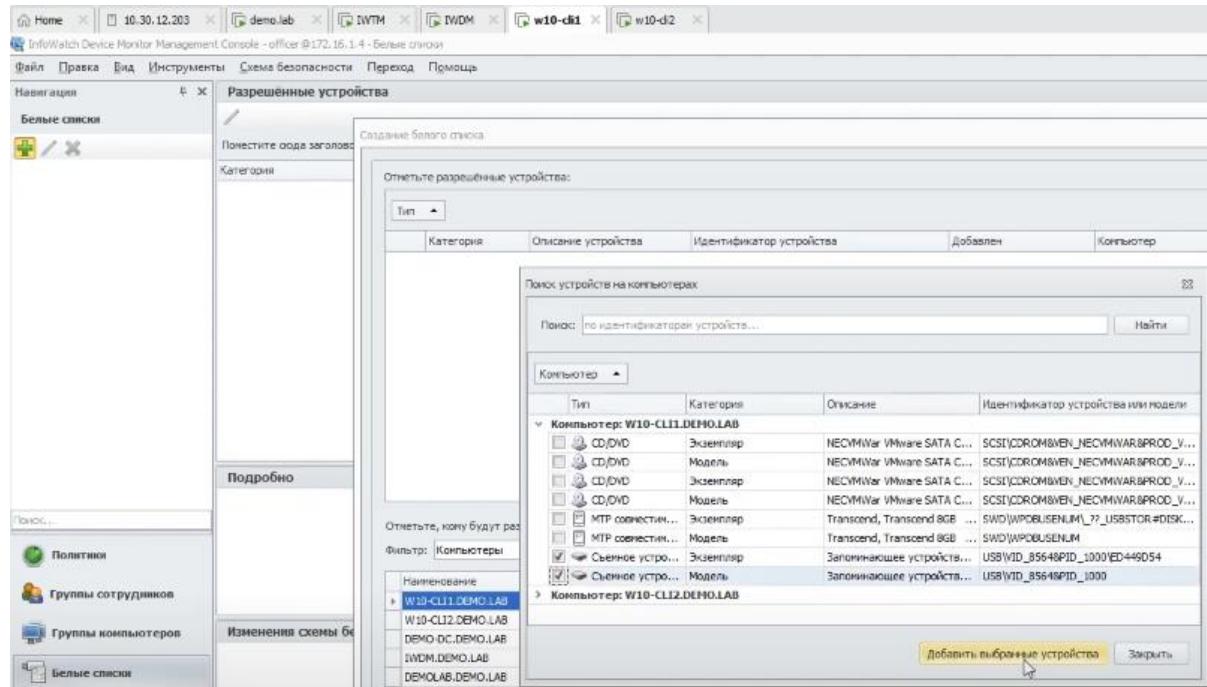
Наименование: Правило 5  
Перехватчик: Device Monitor  
Правило применяется на ОС: Windows  
Тип устройства: Съемное устройство хранения  
Доступ:  
● Нет доступа  
● Только чтение  
☐ Полный доступ на зашифрованные носители  
☐ Использование разрешено

Проверить работоспособность и зафиксировать выполнение

## Правило 6

С учетом ранее созданной блокировки необходимо разрешить использование доверенного носителя информации.

Проверить работоспособность и зафиксировать выполнение

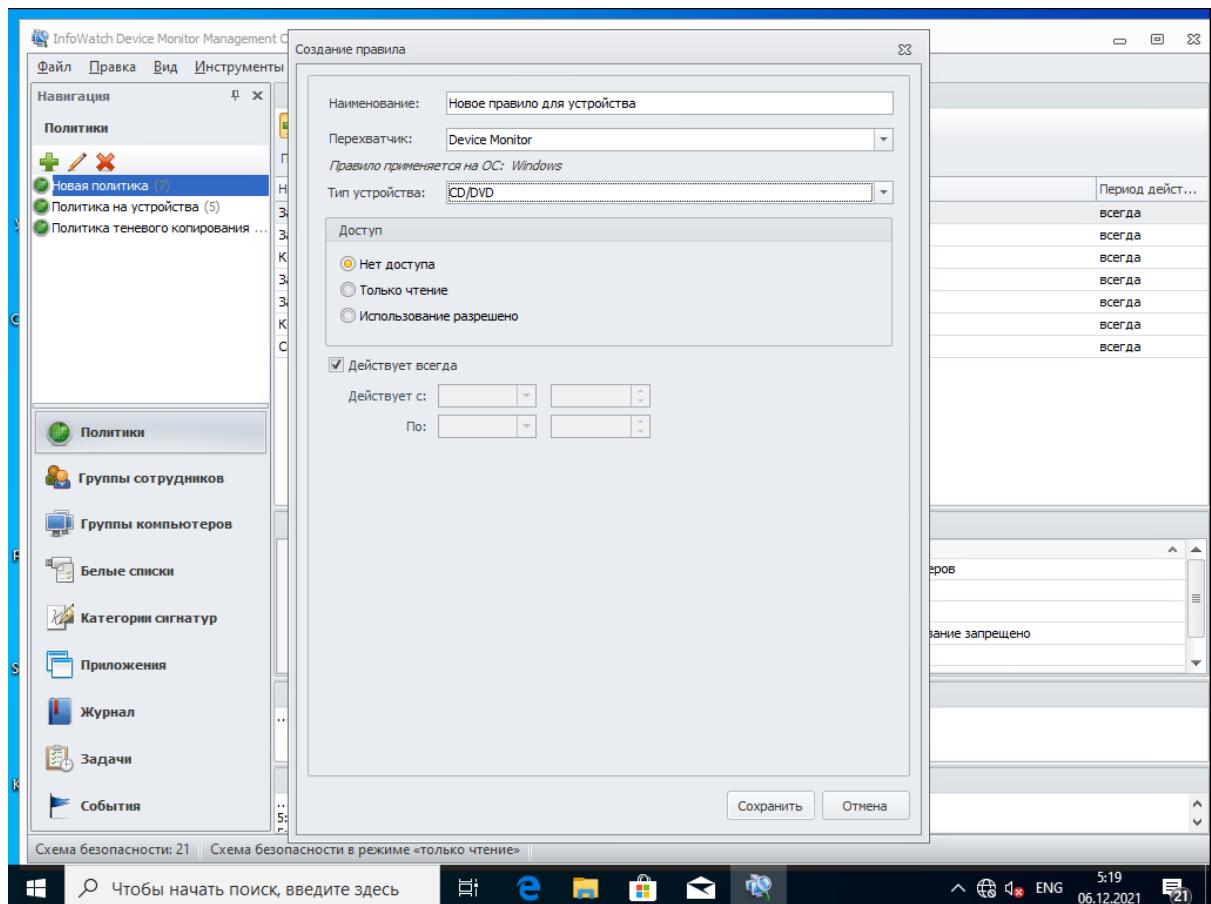


Проверить работоспособность и зафиксировать выполнение!

## Правило 7

Полностью запретить использование CD/DVD-дисковода.

Проверить работоспособность и зафиксировать выполнение



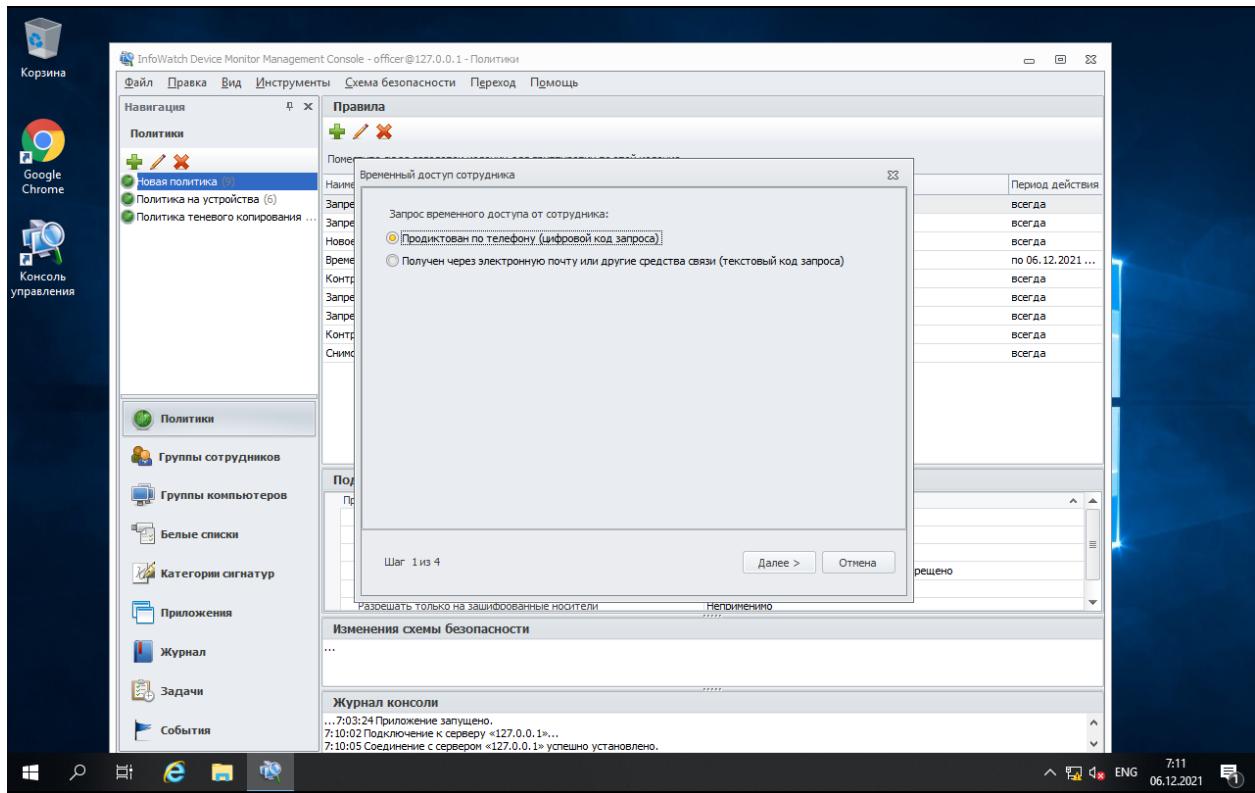
Проверить работоспособность и зафиксировать выполнение!

### Правило 8

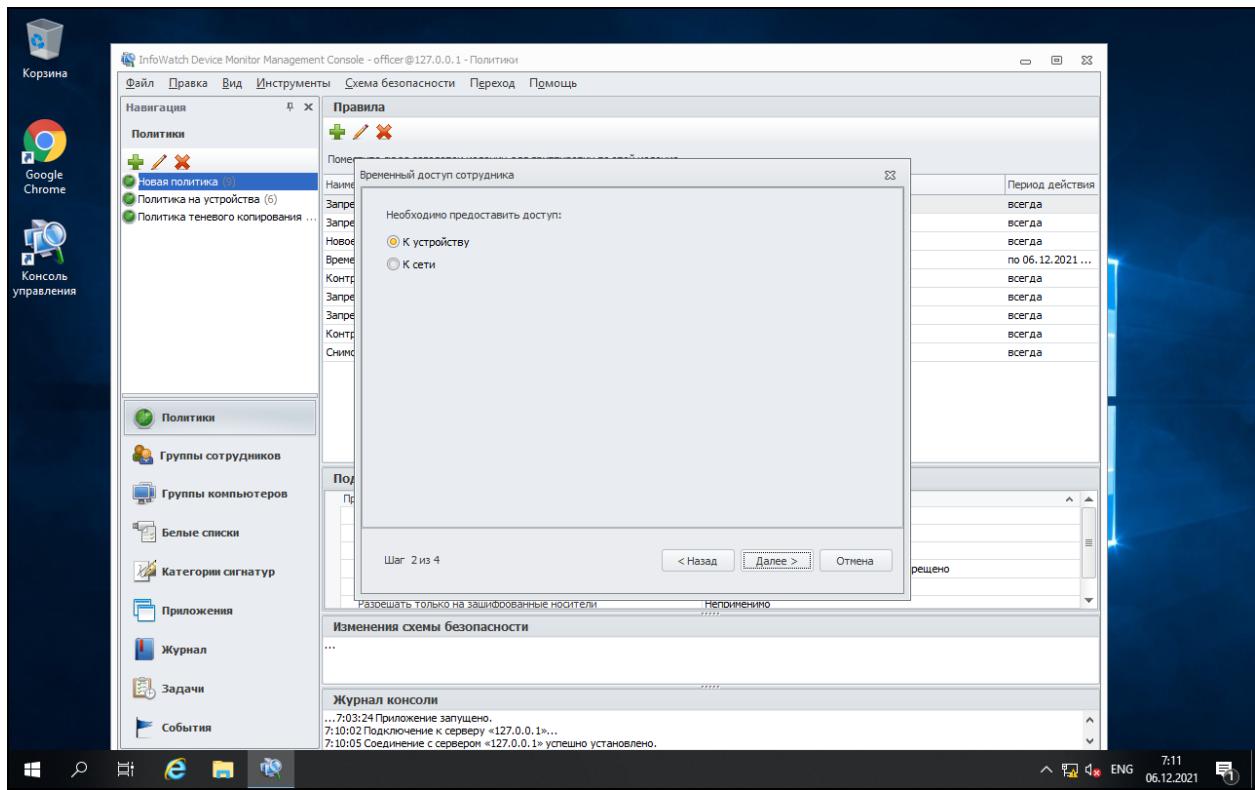
С учетом ранее выполненного запрета необходимо предоставить временный доступ для устройства на 7 минут для пользователя.

Зафиксировать этапы выдачи доступа и работоспособность скриншотами.

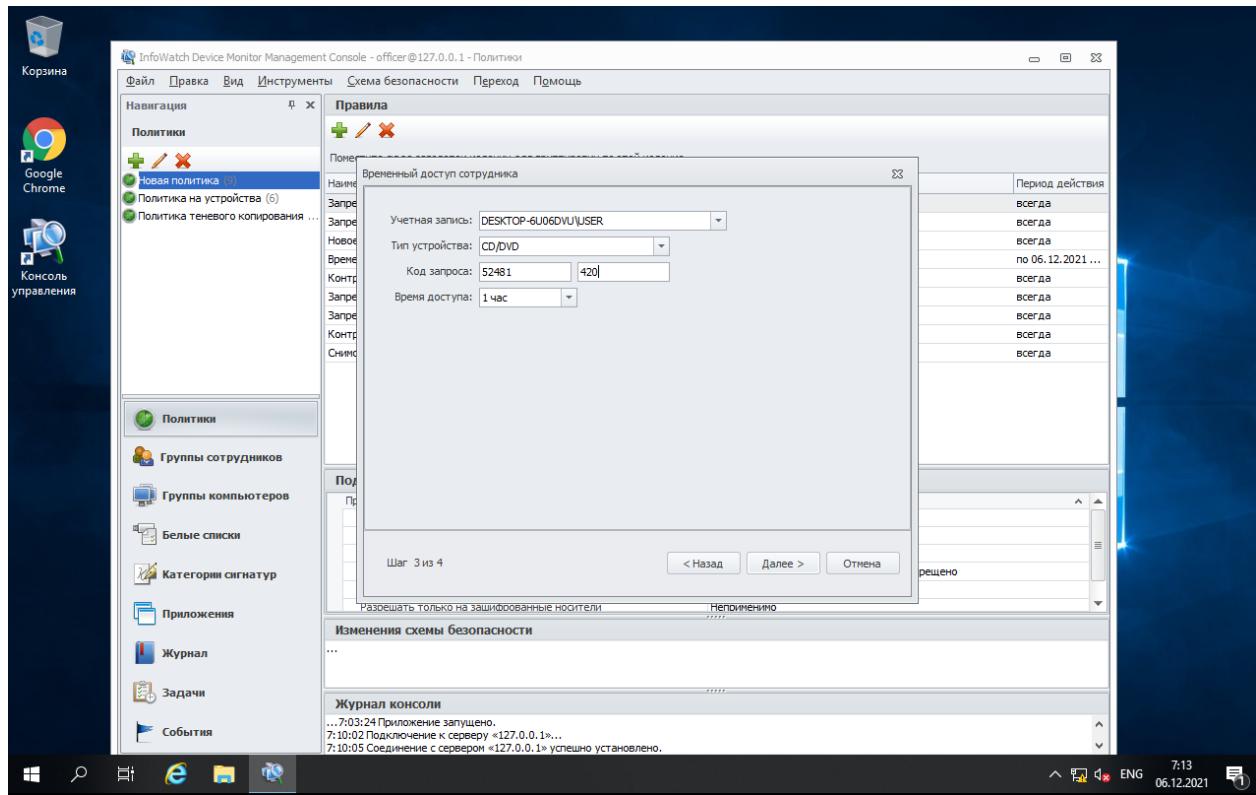
## Выдаем временный доступ сотруднику



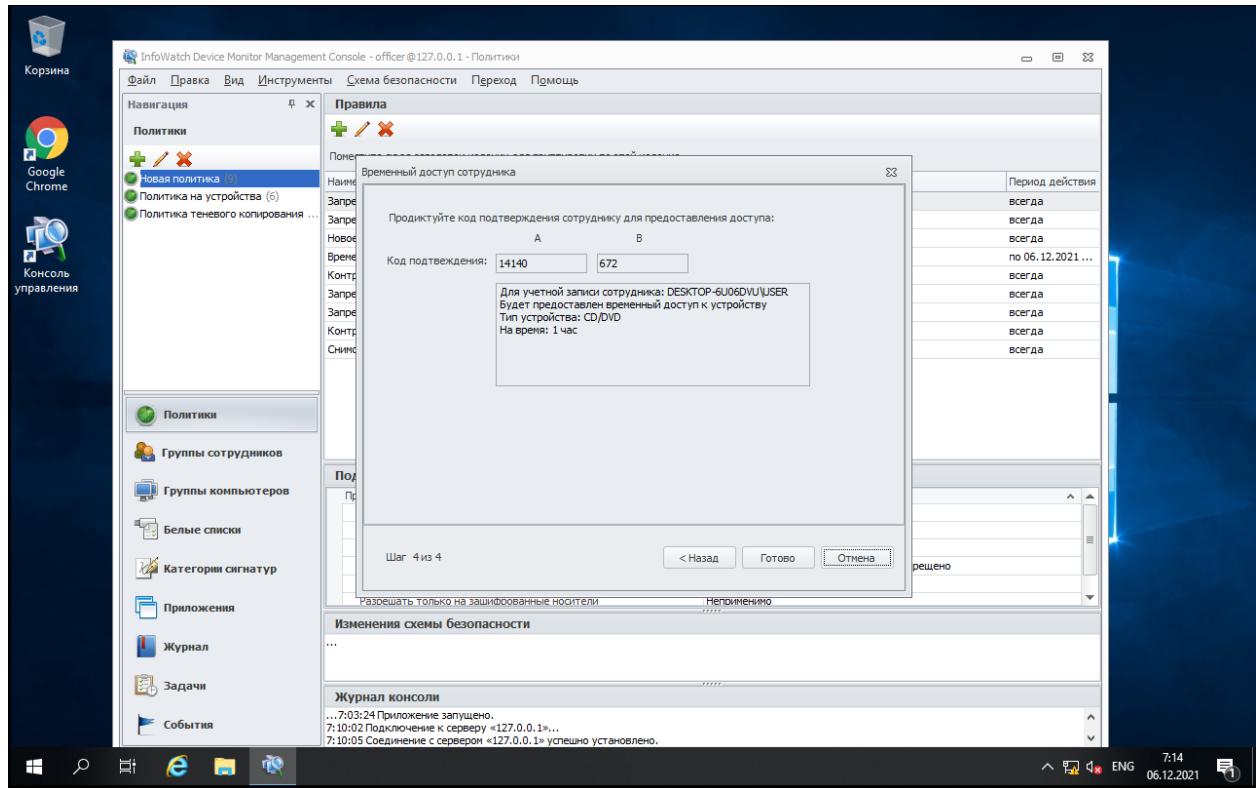
## Предоставляем доступ к устройству



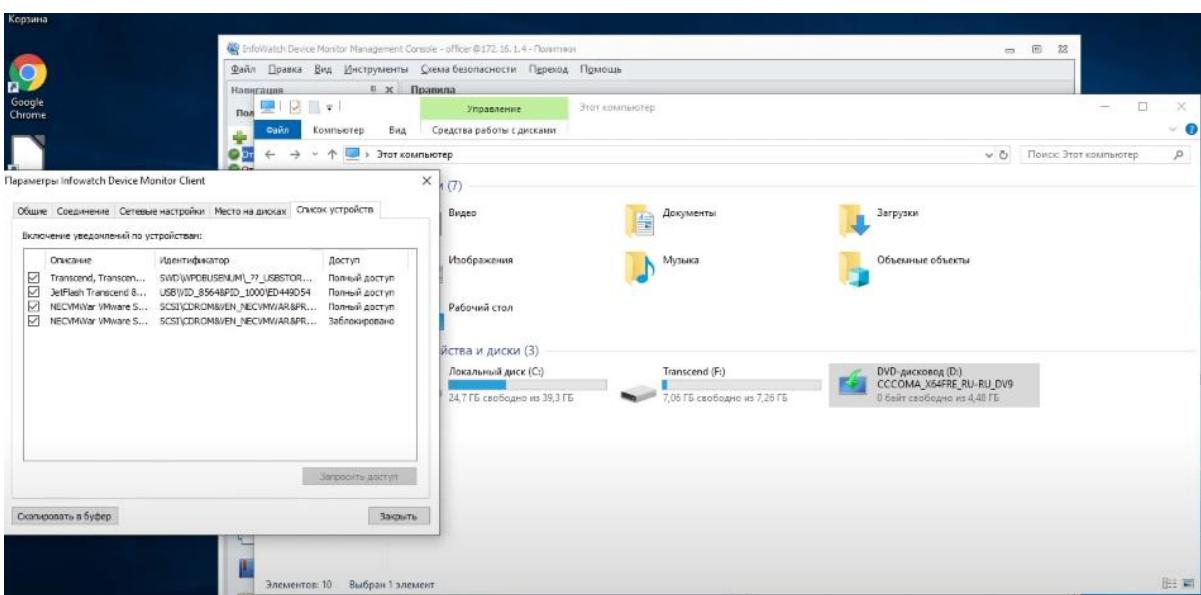
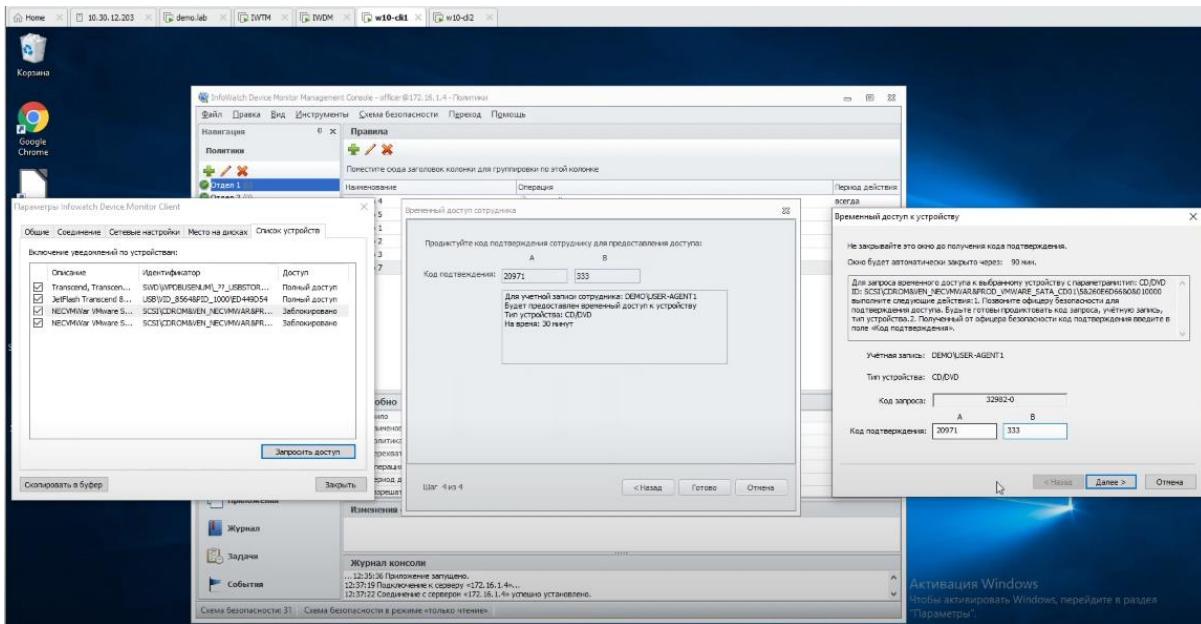
## Выбираем компьютер, время доступа



## Временный доступ



## Скриншотим



Задокументировать этапы выдачи доступа и работоспособность скриншотами.

**Следующие правила создаются в политике «Отдел2».**

Следующие правила создаются в политике «Отдел2».

**Правило 9**

Необходимо поставить на контроль буфер обмена в блокноте и notepad++.

Проверить занесение нескольких событий в WEB-консоль.

Проверить работоспособность и задокументировать выполнение скриншотом.

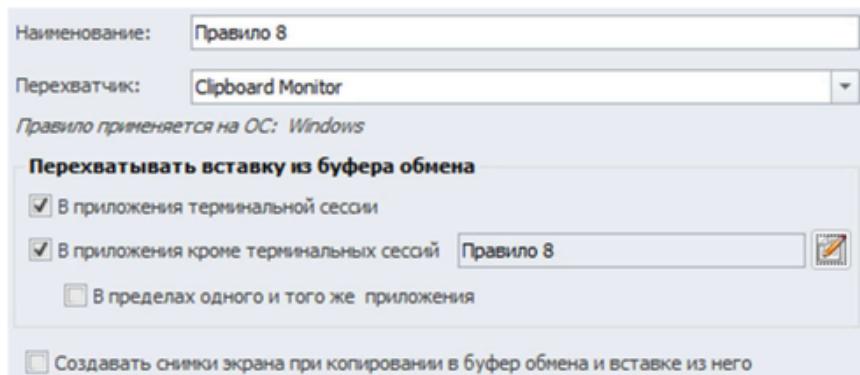
Правило 8 требует от вас поставить на контроль буфер обмена в текстовых препроцессорах (Word, Writer или Wordpad). Как вы понимаете, нужно создать список приложений, а для этого перейти к виртуальной машине w10-cli2. В актуальном на февраль 2022 года образе, есть Writer и WordPad, открыть их нужно

59



Типовое конкурсное задание  
Регионального чемпионата цикла 2021-2022 WorldSkills Russia по компетенции  
«Корпоративная защита от внутренних угроз информационной безопасности»

оба. Что бы открыть их воспользуйтесь поиском Windows: для LibreOffice Writer – LibreOffice Writer, для WordPad – WordPad. Открыв оба приложения, вернитесь к Device Monitor Console. Во вкладке «Приложения» найдите «WORDPAR.exe» и «swriter.exe», после чего создайте список «Правило 8» и добавьте их к списку. Перейдите к политике «Отдел 2» и создайте правило в соответствии с рисунком 69.

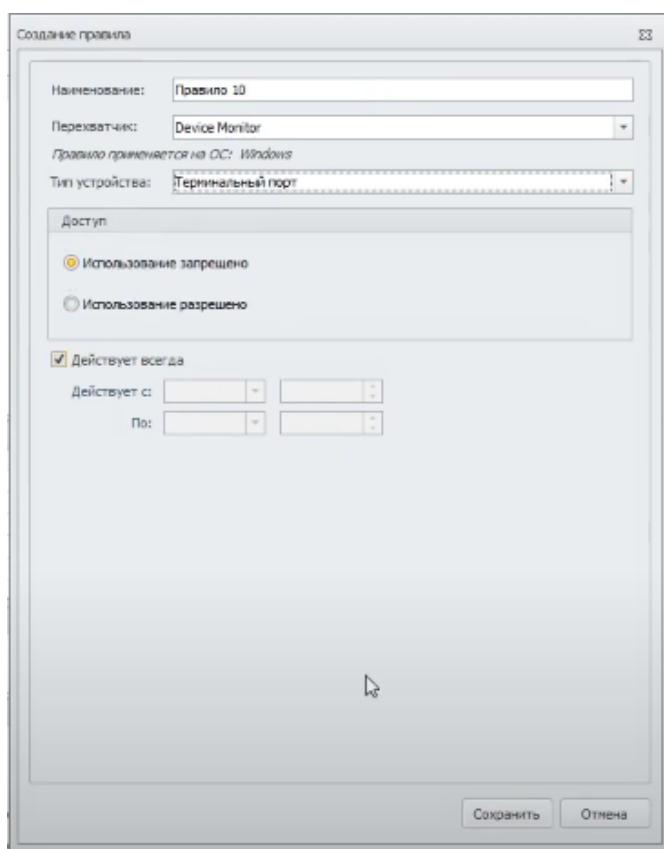
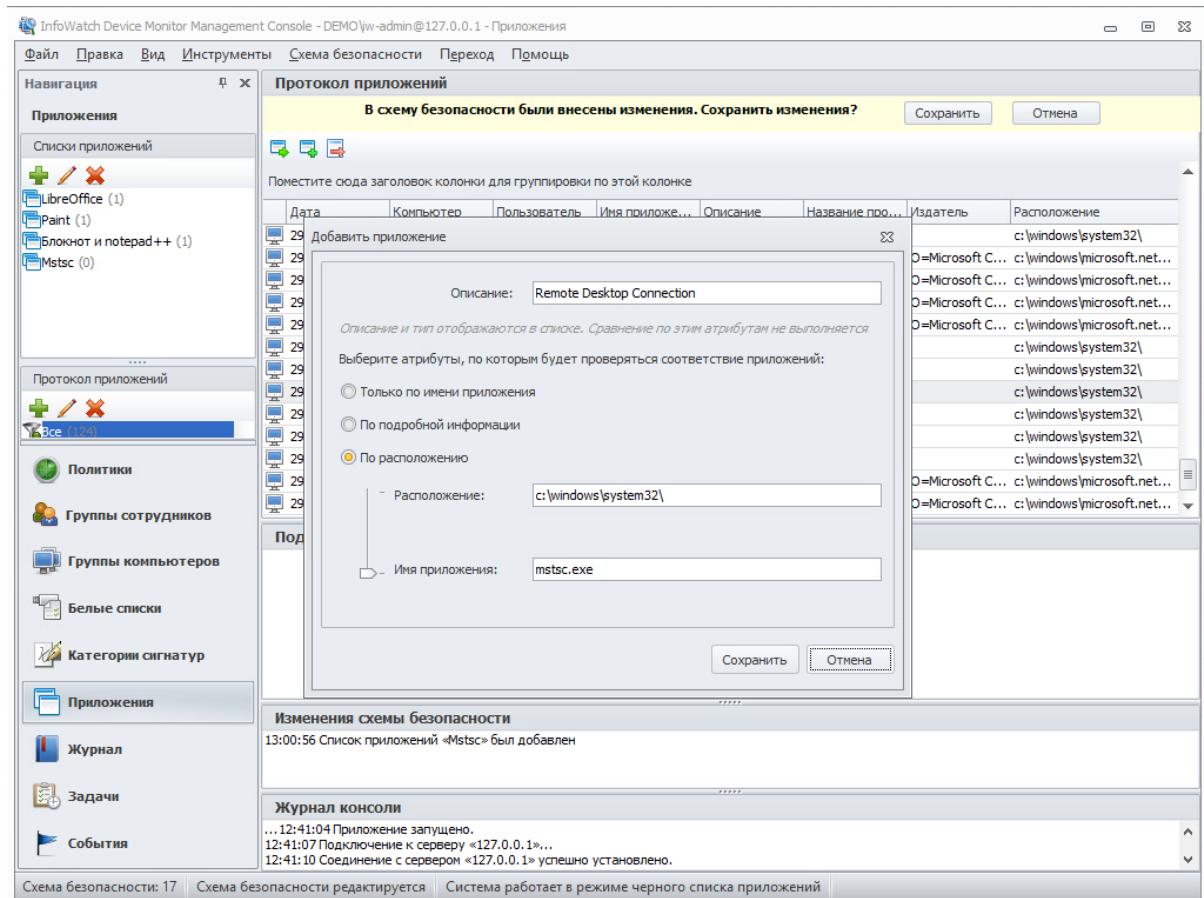


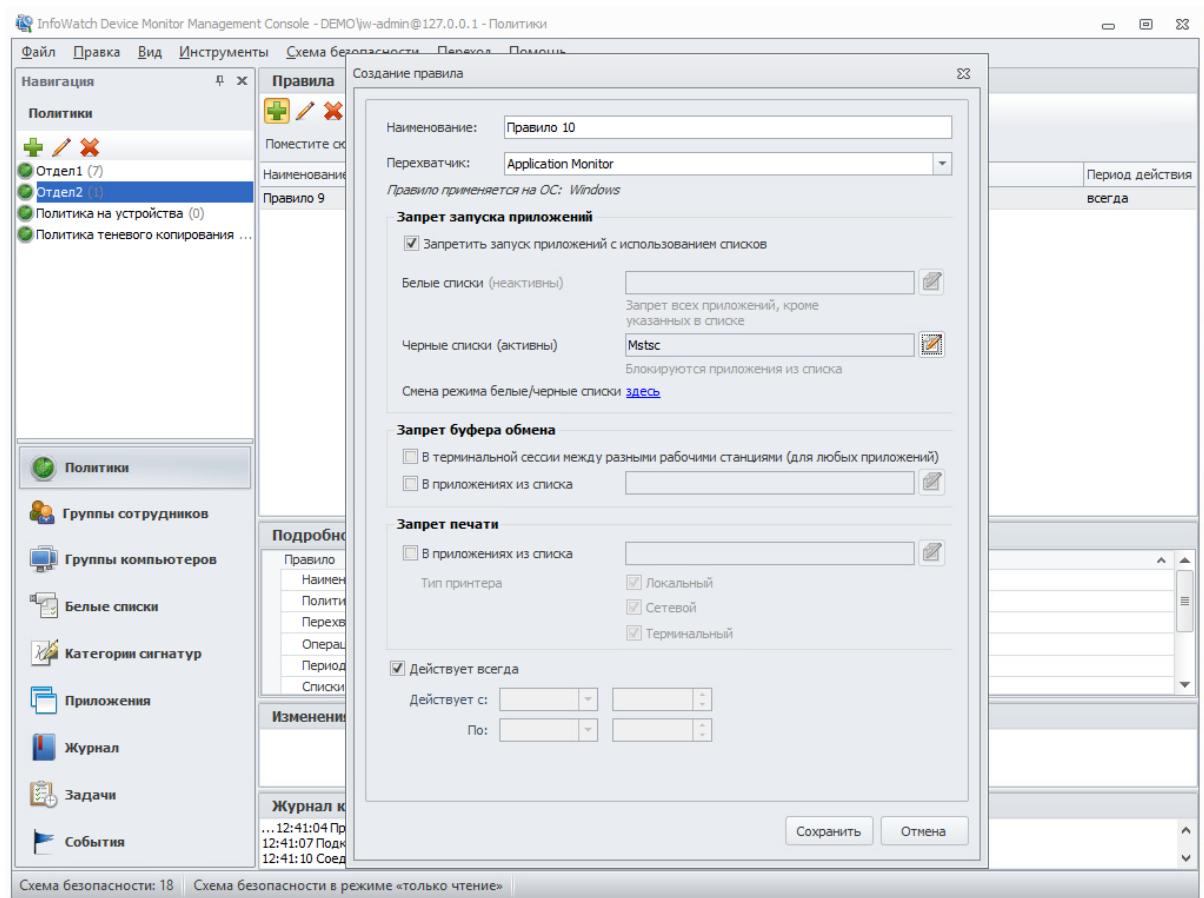
Проверить работоспособность и зафиксировать выполнение скриншотом. Чтобы проверить работоспособность нужно зайти в Device Monitor, затем журнал и там создать фильтр на 1000 записей, только после этого зафиксировать скриншотом

#### Правило 10

Необходимо запретить использовать терминальные сессии для пользователя.

## Проверить работоспособность и зафиксировать выполнение



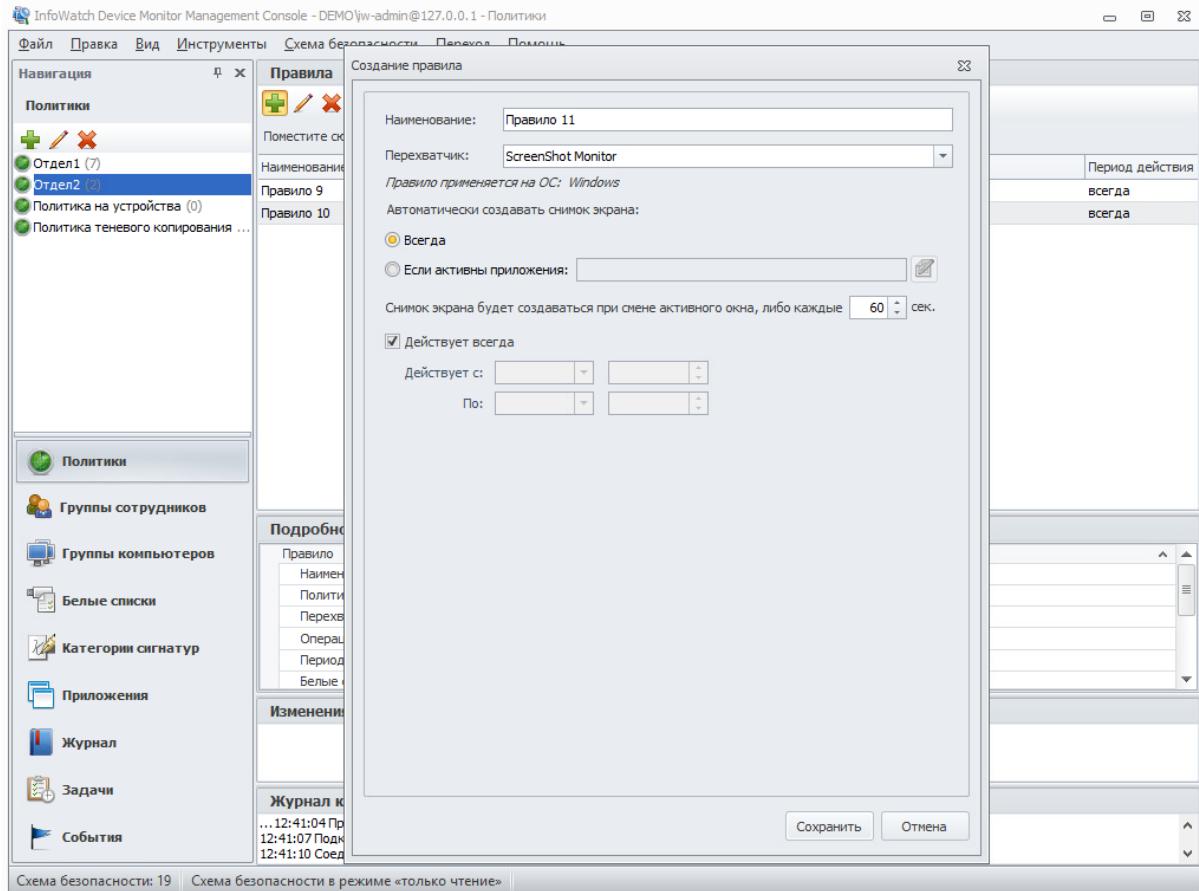


Проверить работоспособность и зафиксировать выполнение!

### Правило 11

Необходимо установить контроль за компьютером потенциального нарушителя путем создания снимков экрана каждые 60 секунд или при смене окна.

Проверить работоспособность и зафиксировать выполнение



Чтобы проверить работоспособность нужно зайти в Device Monitor, затем журнал и там создать фильтр на 1000 записей, только после этого зафиксировать скриншотом

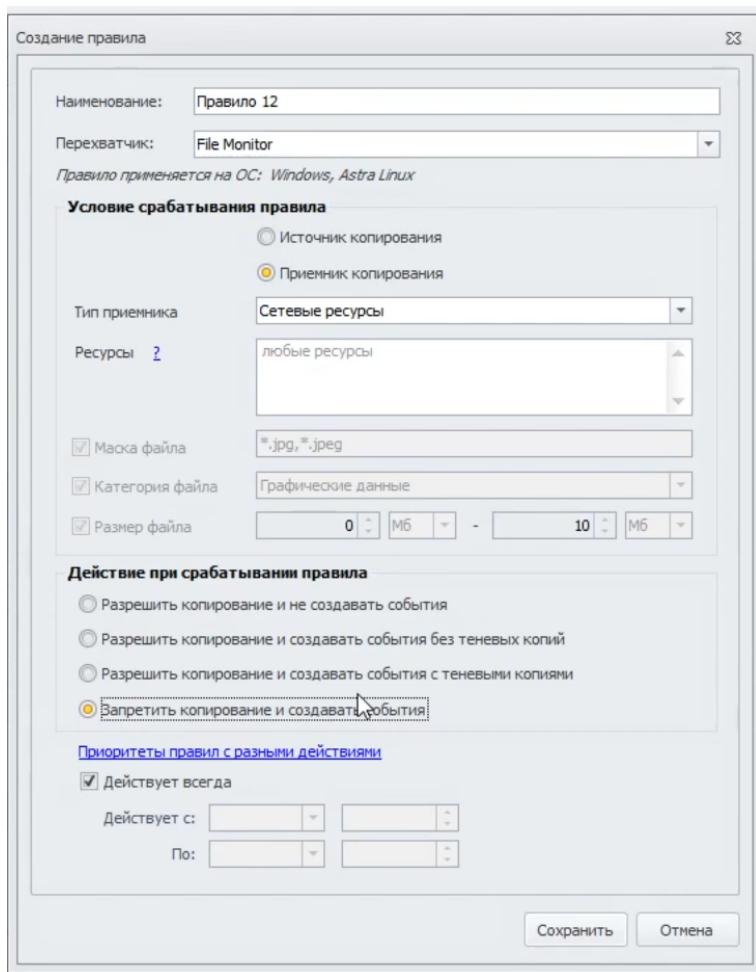
Проверить работоспособность и зафиксировать выполнение

### Правило 12

Запретить передачу файлов с расширением .jpg (.jpeg) на съемные носители информации или в сетевое расположение.

Проверить работоспособность и зафиксировать выполнение

Галочку размер файла можно снять



Проверить работоспособность и зафиксировать выполнение!

## Групповые политики домена

Групповые политики применяются только на компьютер 2, должны быть созданы в домене. Зафиксировать настройку политик скриншотами, при возможности проверки зафиксировать скриншотами проверку политик (например запрет запуска).

### Групповая политика 1

Настроить политику паролей и блокировки: Максимальный срок действия пароля - 30 дней, Минимальная длина пароля - 8, пароль должен отвечать требованиям сложности, Блокировка учетной записи при повторном вводе неверного пароля (3 раза), продолжительность блокировки 15 минут.

## Зафиксировать настройки политики скриншотами.

Редактор управления групповыми политиками

Файл Действие Вид Справка

Политика Групповая политика 1 [DEN]

Конфигурация компьютера

Политики

- Конфигурация программ
- Конфигурация Windows
  - Политика разрешения и запрета
  - Сценарии (запуск/завершение)
  - Развернутые принтеры
- Параметры безопасности
  - Политики учетных записей
    - Политика паролей
    - Политика блокировки
    - Политика Kerberos
  - Локальные политики
  - Журнал событий
  - Группы с ограниченными правами
  - Системные службы
  - Реестр
  - Файловая система
  - Политики проводника
  - Монитор брандмауэра
    - Политики диспетчера политики
  - Политики беспроводной сети
  - Политики открытого доступа

Политика

Параметр политики
Не определено
Не определено
30 дн.
8 зн.
29 дн.
Включен
Не определено

Редактор управления групповыми политиками

Файл Действие Вид Справка

Политика Групповая политика 1 [DEN]

Конфигурация компьютера

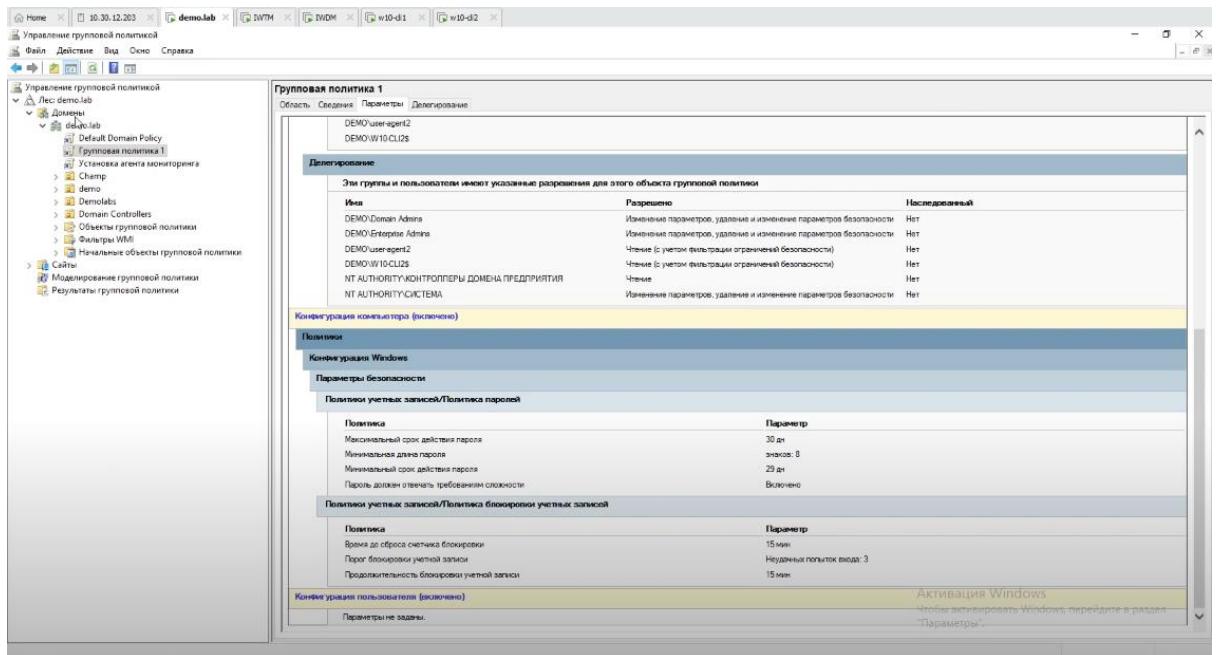
Политики

- Конфигурация программ
- Конфигурация Windows
  - Политика разрешения и запрета
  - Сценарии (запуск/завершение)
  - Развернутые принтеры
- Параметры безопасности
  - Политики учетных записей
    - Политика блокировки
    - Политика Kerberos
  - Локальные политики
  - Журнал событий
  - Группы с ограниченными правами
  - Системные службы
  - Реестр
  - Файловая система
  - Политики проводника
  - Монитор брандмауэра
    - Политики диспетчера политики
  - Политики беспроводной сети
  - Политики открытого доступа

Политика

Параметр политики
15 мин.
3 ошибок входа в систему
15 мин.

## Скриншот



Зафиксировать настройки политики скриншотами.

## Групповая политика 2

Запретить запуск приложений по списку: PowerShell, ножницы, сведения о системе.

Зафиксировать настройки политики и выполнение скриншотами.

Конфигурация пользователя → Политики → Административные шаблоны → Система

Включаем политики → “Не запускать указанные приложения Windows”

Don't run specified Windows applications

Comment:

Enabled

Not Configured

Disabled

Supported on:

At least Windows 2000

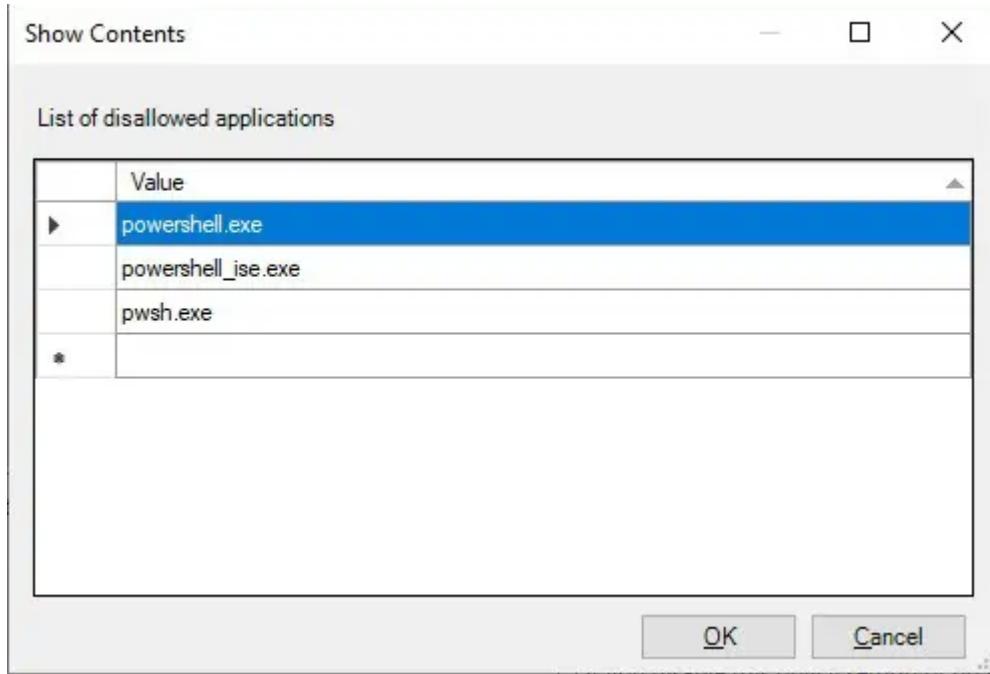
Options:

List of disallowed applications Show...

Prevents Windows from running the applications listed in the policy setting.

If you enable this policy setting, it prevents Windows from running the applications listed in the policy setting.

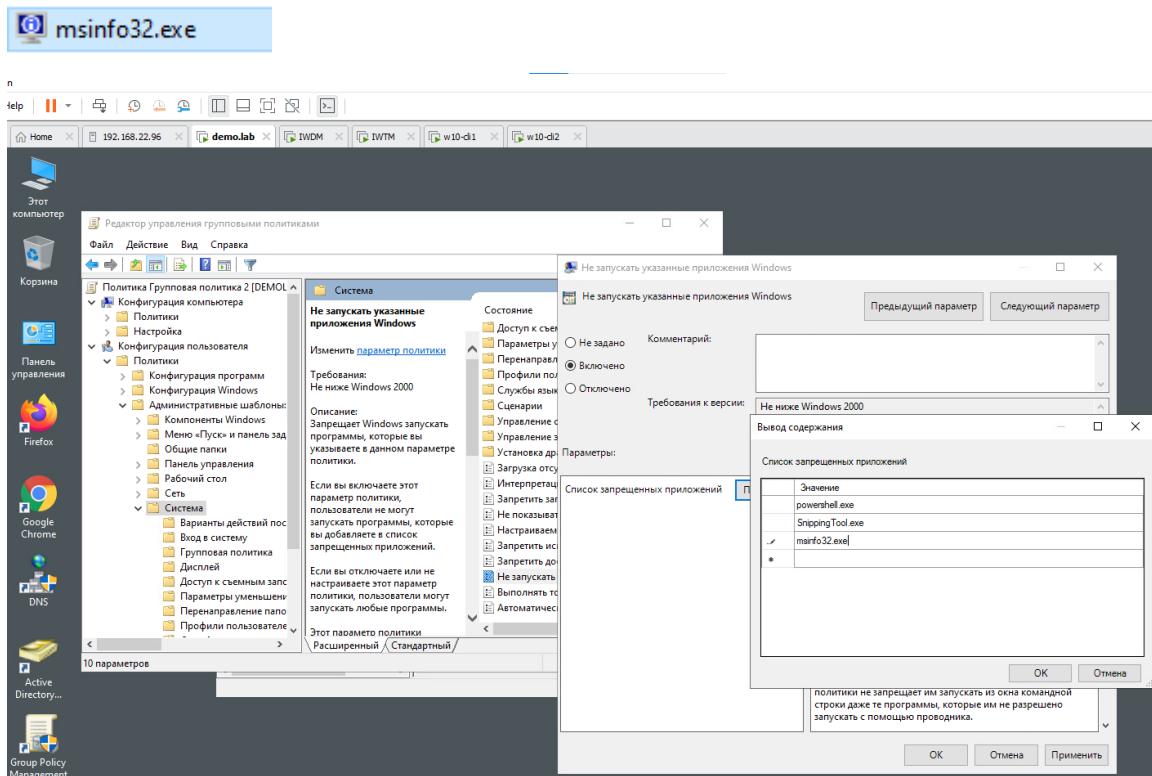
Нажимаем кнопку → Показать и вводим список команд, запускающих PowerShell



Также вводим ножницы

SnippingTool.exe

И сведения о системе



Зафиксировать настройки политики и выполнение скриншотами.

### Групповая политика 3

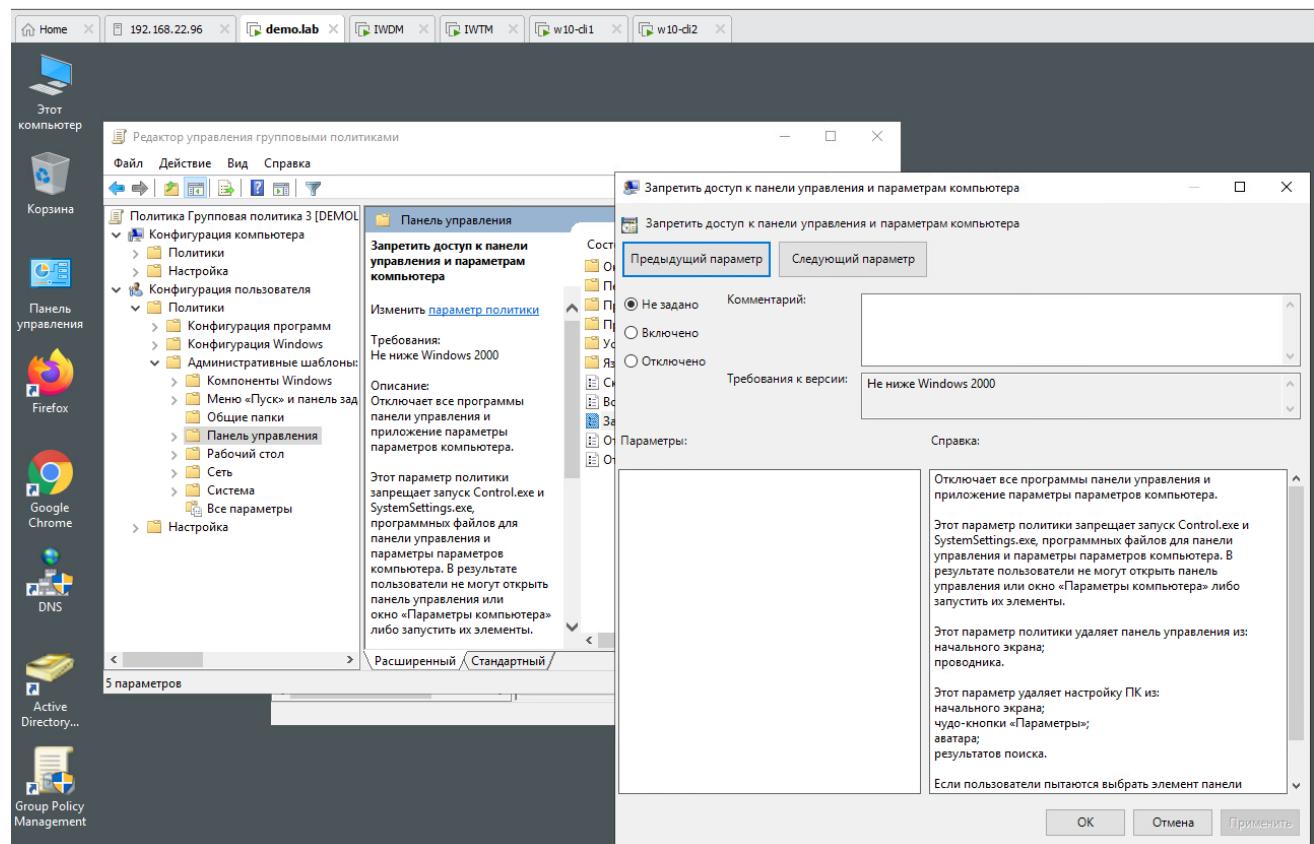
Запретить использование панели управления стандартными политиками.

Зафиксировать настройки политики и выполнение скриншотами.

Создаем новую политику безопасности переходим к её редактированию

Конфигурация пользователя → Политики → Административные шаблоны  
→ Панель управления

Здесь нужно включить политику → “Запретить доступ к панели управления”



Зафиксировать настройки политики и выполнение скриншотами.

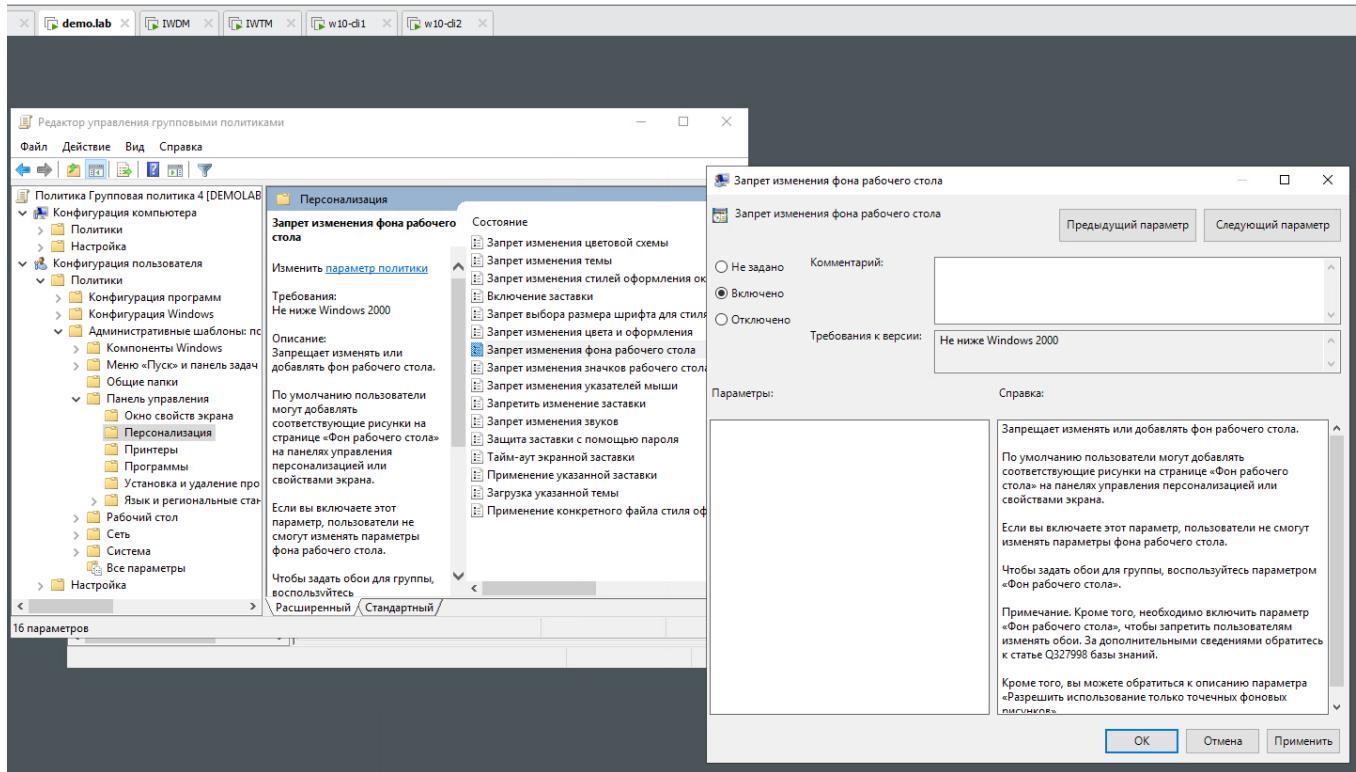
## Групповая политика 4

Запретить пользователю самостоятельно менять обои рабочего стола.

Зафиксировать настройки политики и выполнение скриншотами.

Конфигурация пользователя → Административные шаблоны – Панель управления – Персонализация.

Здесь нужно включить политику → “Запрет изменения фона рабочего стола”



Зафиксировать настройки политики и выполнение скриншотами.

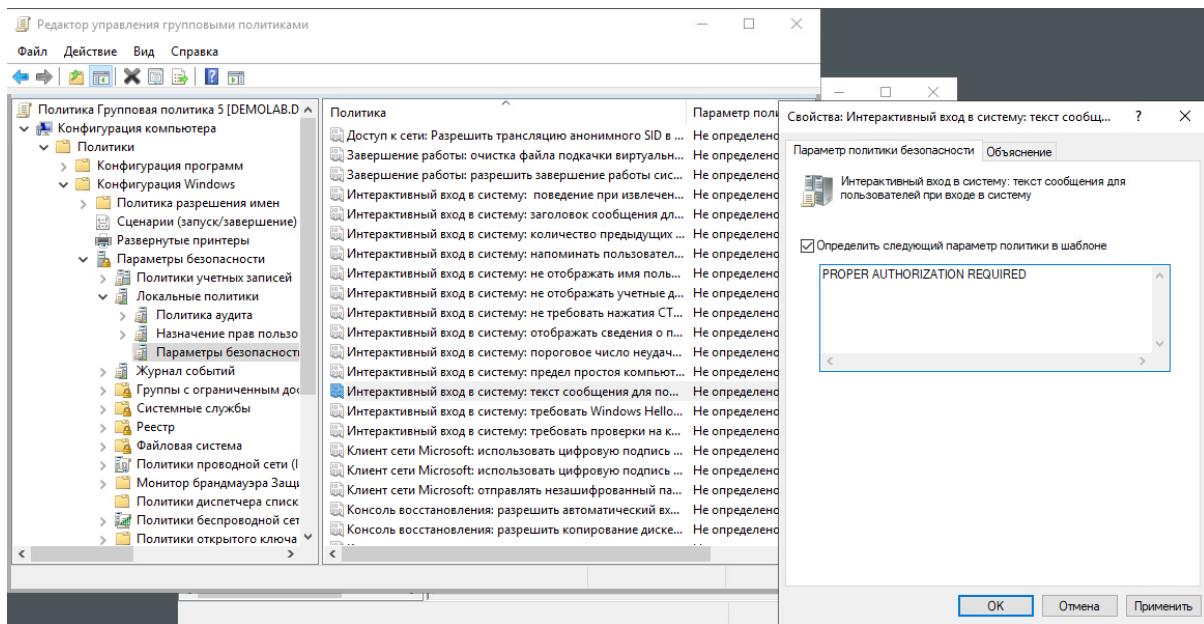
## Групповая политика 5

Настроить дополнительные параметры системы, согласно которым при входе на компьютер 2 отображается сообщение с именем сервера авторизации.

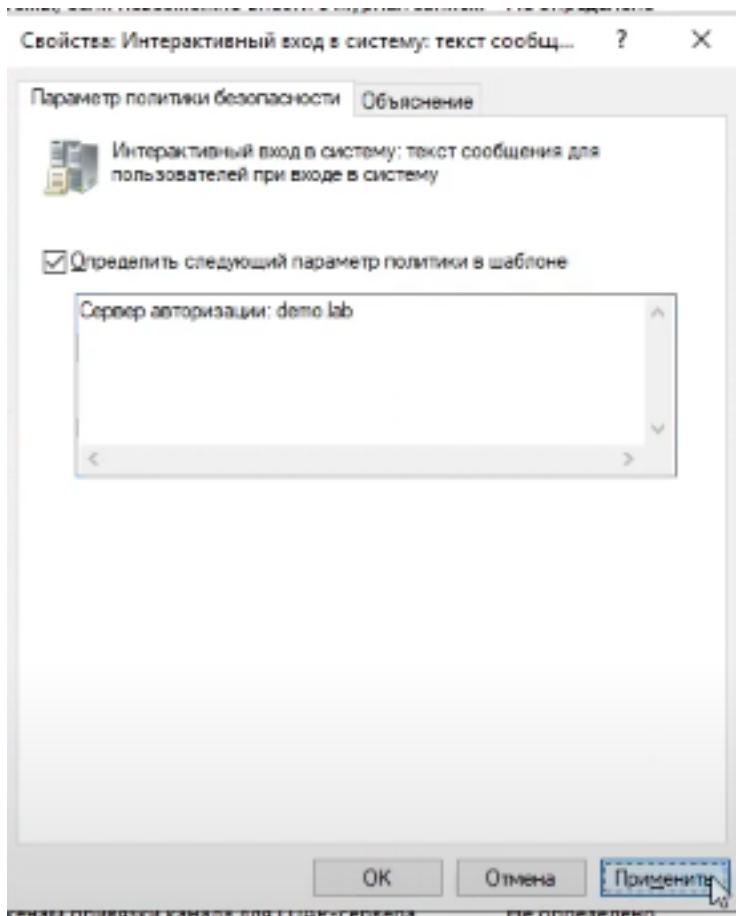
Зафиксировать настройки политики и выполнение скриншотами.

Создаем новую политику безопасности переходим к её редактированию

## Переходим по пути в → Параметры безопасности



Включаем следующий элемент настройки и вводим нужный текст → “сообщение с именем сервера авторизации” – Сервер авторизации: demo.lab

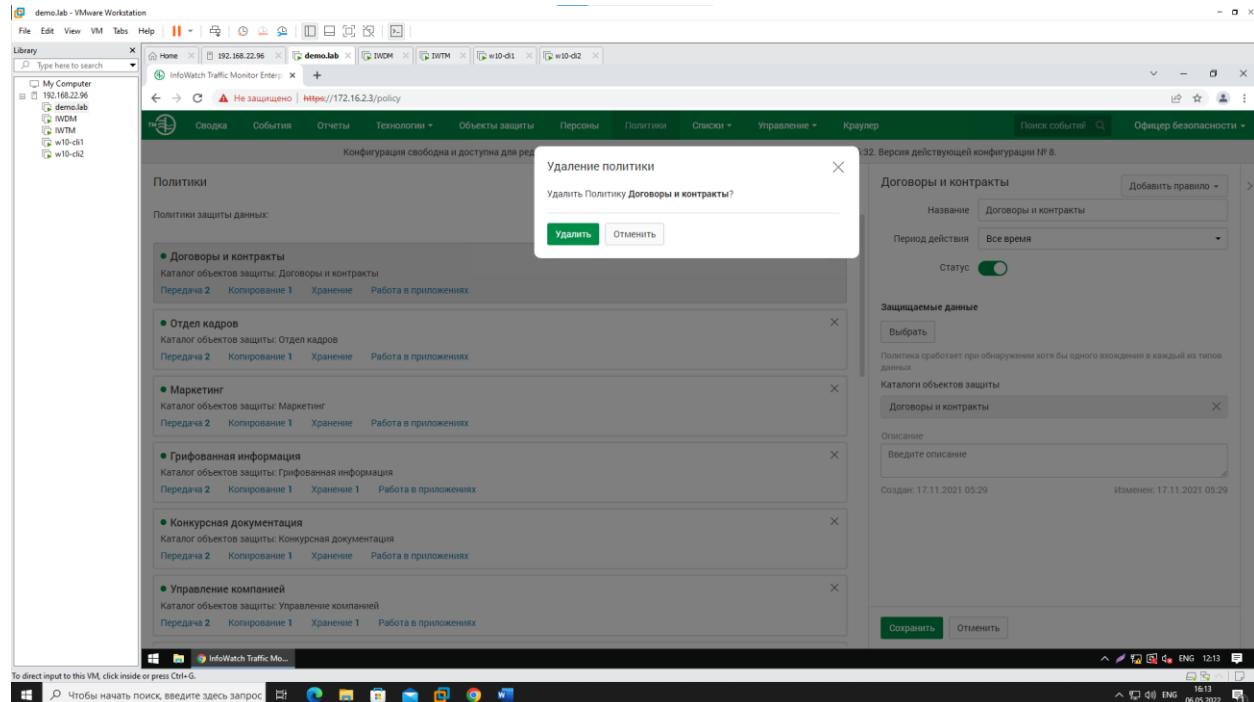


Зафиксировать настройки политики и выполнение скриншотами.

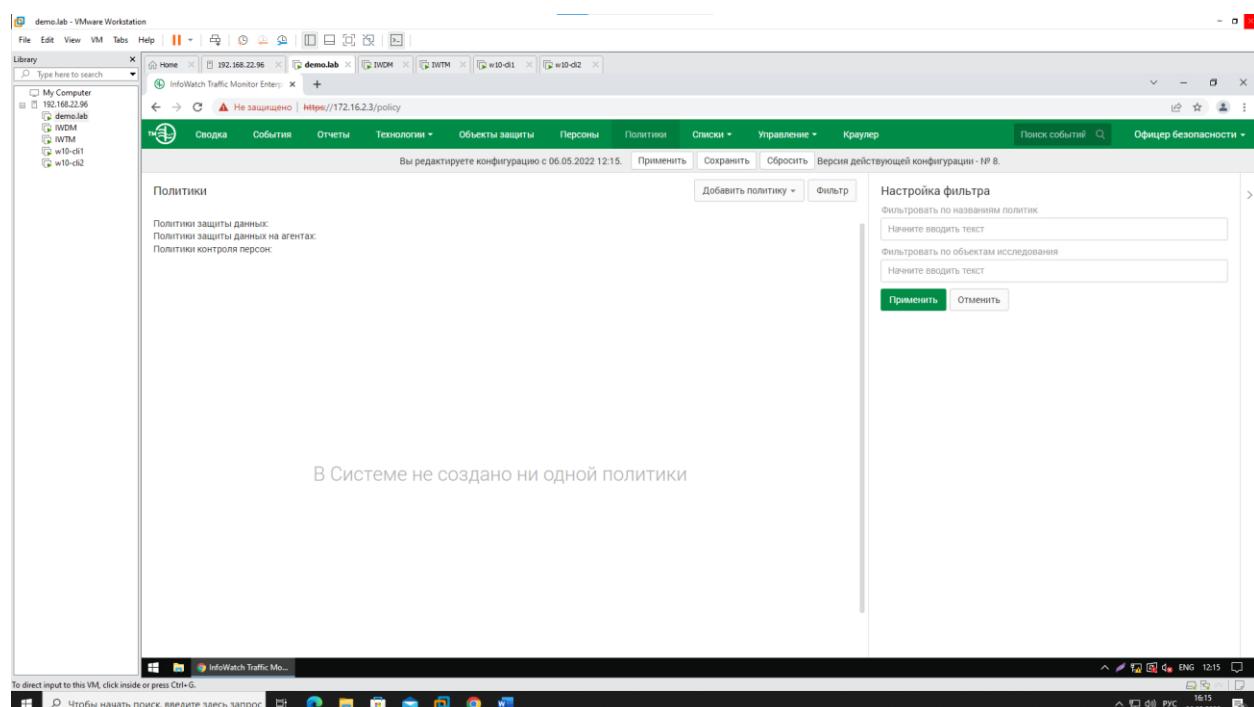
После всего этого применяем групповые политики через cmd → gpupdate /force и смотрим результат: запускаем панель управления на агенте2 и фиксируем работу политики

## Модуль 3

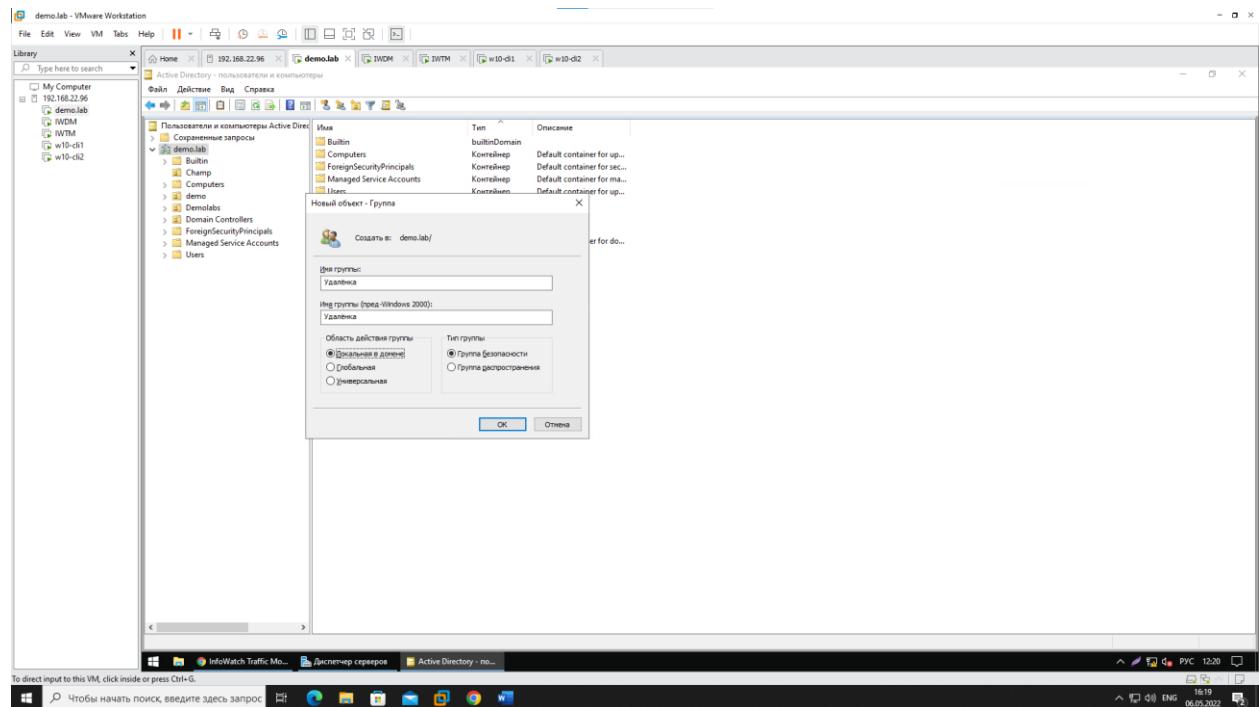
### Удаляем все стандартные политики



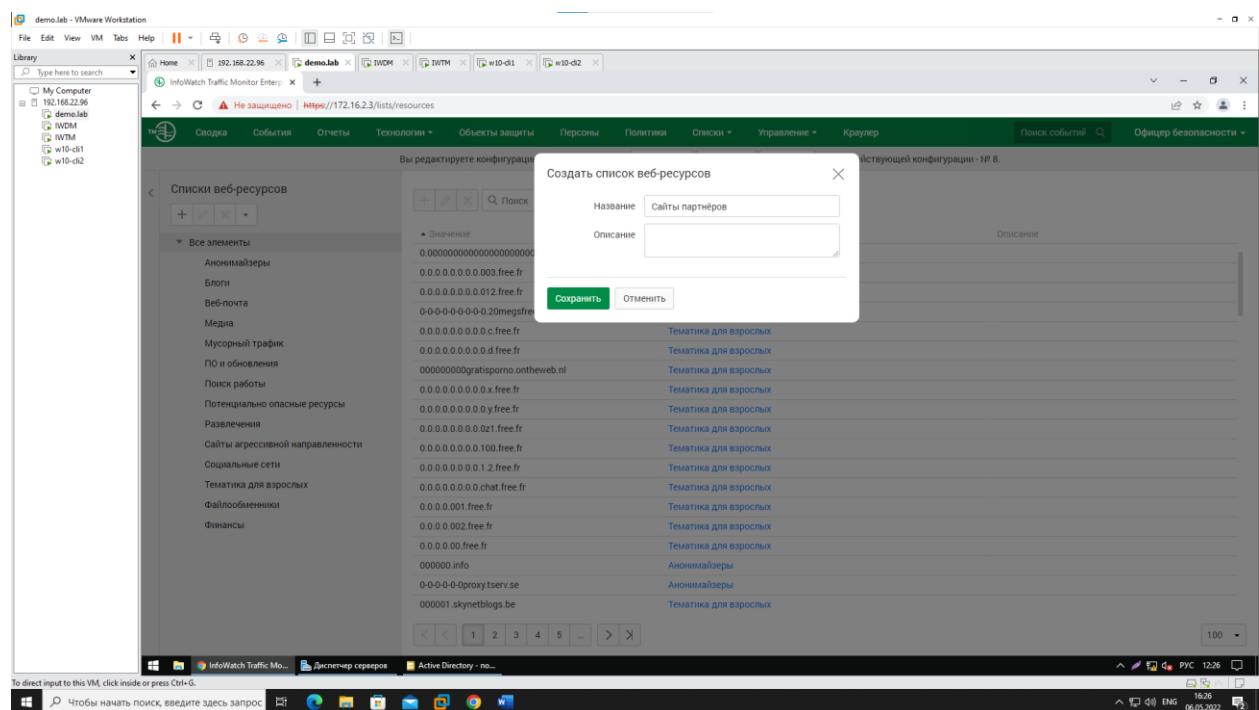
После удаления выглядит вот так



## Создаем локальную группу с название – удалёнка



## Создаем список веб ресурсов (Списки – Веб-ресурсы)



## Добавляем веб-ресурсы

The screenshot shows the InfoWatch Traffic Monitor Enterprise software interface. A modal dialog box titled 'Добавить веб-ресурс' (Add Web Resource) is open in the center. It contains two input fields: 'Значение' (Value) with the text 'rt.ru' and 'Описание' (Description). At the bottom are two buttons: 'Сохранить' (Save) and 'Отменить' (Cancel). The background shows the main application window with a navigation bar and various tabs. On the left, there's a sidebar with a tree view of resource types under 'Списки веб-ресурсов' (Web Resource Lists). The main pane displays a list of websites under 'Сайты партнёров' (Partnership Websites), which includes 'infotechs.ru', 'rt.ru', and 'vmware.com'. The status bar at the bottom indicates the date and time as '06.05.2022 12:15'.

## Задание 4

### Периметр компании

The screenshot shows the 'Редактирование' (Editing) screen for a perimeter named 'Компания'. The left sidebar lists 'Периметры' (Perimeters) with a '+' button and a 'Список' (List) button. The main panel displays the following fields:

- Название:** Компания
- Почтовый домен:** @ demo.lab
- Список веб-ресурсов:** Сайты партнёров
- Группа персон:** Удалёнка
- Описание:** Персоны и компьютеры компании. Используется для контроля информации, передаваемой за периметр компании.

At the bottom, it shows 'Создан: 17.11.2021 05:29' and 'Изменен: 17.11.2021 05:29'. There are 'Сохранить' (Save) and 'Отменить' (Cancel) buttons.

### Исключение из перехвата

The screenshot shows the 'Редактирование' (Editing) screen for an exclusion rule named 'Исключить из перехвата'. The left sidebar lists 'Периметры' (Perimeters) with a '+' button and a 'Список' (List) button. The main panel displays the following fields:

- Название:** Исключить из перехвата
- Персона:** Kornilov V. Fedosej
- Описание:** Если включена политика 'Исключить из перехвата', то почтовые сообщения, отправленные входящими в данный периметр персонами,

At the bottom, it shows 'Создан: 17.11.2021 05:29' and 'Изменен: 17.11.2021 05:29'. There are 'Сохранить' (Save) and 'Отменить' (Cancel) buttons.

## Политика 3

Технологии – Эталонные документы, создаем политику в эталонных документах

The screenshot shows the 'InfoWatch Traffic Monitor Enterprise' application window. The main menu bar includes 'Сводка', 'События', 'Отчеты', 'Технологии', 'Объекты защиты', 'Персоны', 'Политики', 'Списки', 'Управление', and 'Краулер'. A warning message 'Не защищено' is displayed at the top. The left sidebar shows 'Каталоги эталонных документов' with options for '+', 'Пометка', 'Удаление', and 'Поиск по каталогам'. Below this is a tree view with 'Все элементы' expanded, showing 'Автоматические эталонные документы...' and 'Эталонные документы'. The right side displays a 'Создать' (Create) dialog box for a new policy. The 'Название' field is filled with 'Политика 3'. There are two slider controls for 'Порог цитируемости для текстовых данных' (set at 10%) and 'Порог цитируемости для бинарных данных' (set at 50%). An 'Описание' (Description) text area is present but empty. At the bottom of the dialog are 'Создать' (Create) and 'Отменить' (Cancel) buttons.

На основе всех типов данных

The screenshot shows the same 'InfoWatch Traffic Monitor Enterprise' interface. The main menu bar and warning message are identical. The left sidebar shows 'Каталоги эталонных документов' with '+', 'Пометка', 'Удаление', and 'Поиск по каталогам'. Below this is a tree view with 'Все элементы' expanded, showing 'Автоматические эталонные документы...' and 'Эталонные документы'. The right side shows the details for the 'Политика 3' policy. It has a '+' button and a trash bin icon. Below the policy name are two items: 'На основе текстовых данных' and 'На основе всех типов данных'.

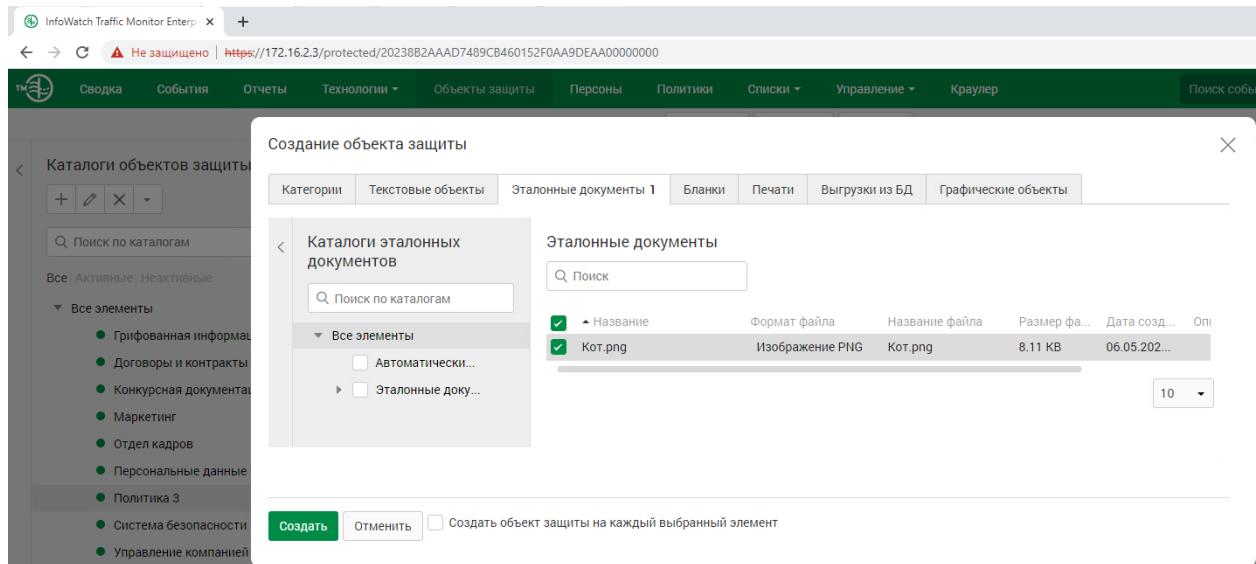
## Добавляем картинку котика

The screenshot shows the 'Catalogs of standard documents' section. A file named 'Kot.png' has been uploaded as an 'Image' type file. A modal window titled 'Загрузка технологий' (Technology upload) shows the file 'Кот.png' has been saved.

## Добавляем объекты защиты

The screenshot shows the 'Catalogs of protection objects' section. A new category named 'Политика 3' is being created. The 'Status' toggle is turned on. The 'Description' field is empty. The 'Create' button is visible at the bottom of the dialog.

После создания объекта защиты под названием – Политика 3, переходим в неё и создаем так объект (“+”)



Создание объекта защиты

Каталоги объектов защиты

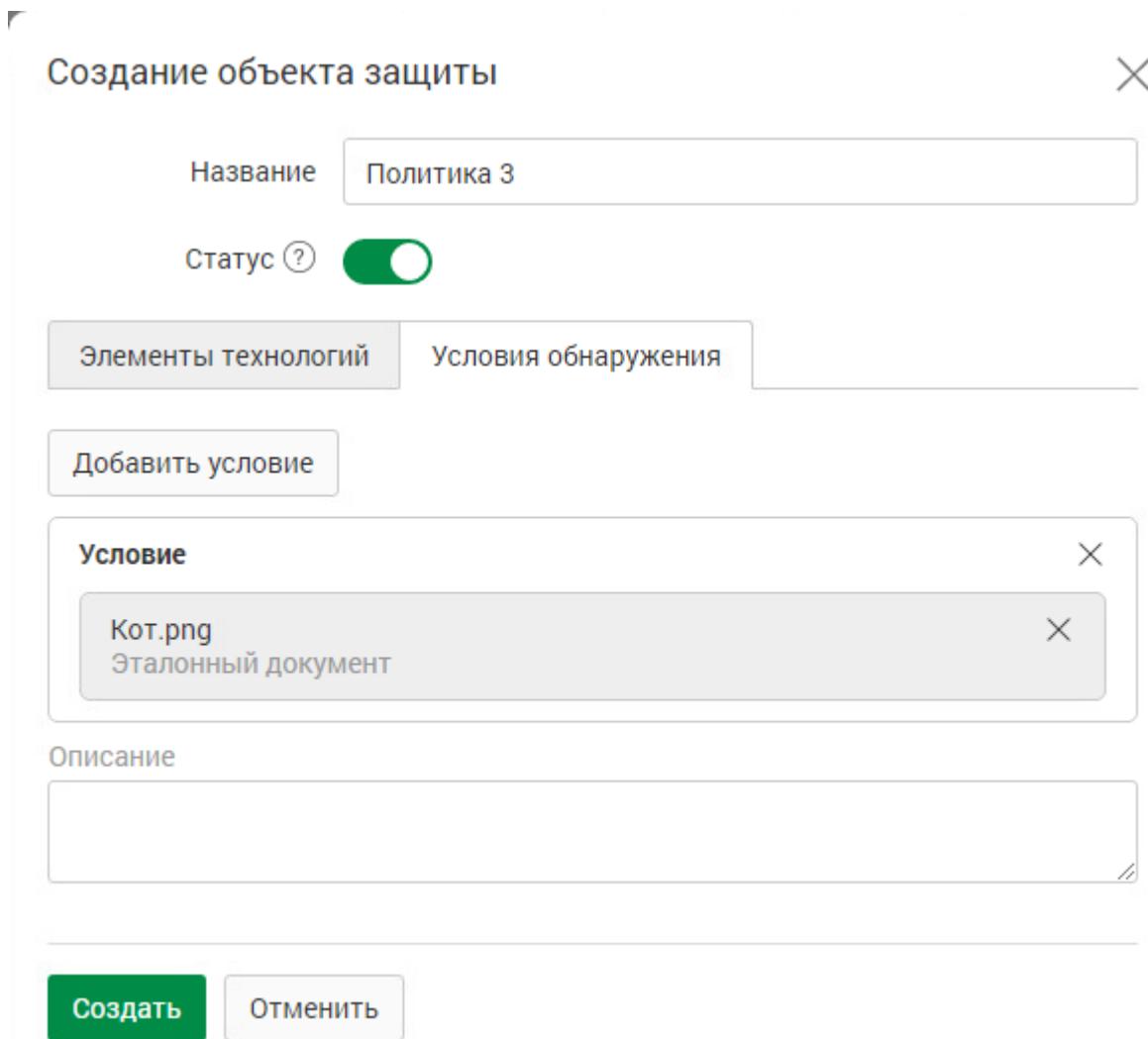
Каталоги эталонных документов

Эталонные документы

Кот.png

Создать Отменить

Условием – выбираем кортику Кота



Создание объекта защиты

Название Политика 3

Статус

Элементы технологий Условия обнаружения

Добавить условие

Условие

Кот.png  
Эталонный документ

Описание

Создать Отменить

Вот так

Вы редактируете конфигурацию с 06.05.2022 12:15. Применить Сохранить Сбросить Версия действующей конфигурации - № 9.

Каталоги объектов защиты

Политика 3

Название	Элементы технологий	Дата создания	Дата изменения	Описание
Политика 3	Кот.png	06.05.2022 13:07	06.05.2022 13:07	

Список элементов:

- Грифованная информация
- Договоры и контракты
- Конкурсная документация
- Маркетинг
- Отдел кадров
- Персональные данные
- Политика 3

Списки – Теги, создаем новый тег

InfoWatch Traffic Monitor Enterprise x +

← → C ▲ Не защищено | https://172.16.2.3/lists/tag

Сводка События Отчеты Технологии Объекты защиты Персоны Политики Списки Управление Крауд

Вы редактируете конфигурацию

Управление тегами

С помощью тегов удобно группировать объекты, хранящиеся в Системе, и собирать статистику по ним.

+ Название

VIP На рассмотрение

Создать тег

Название: Политика 3

Цвет:

Описание

Сохранить Отменить

Переходим в политики, создаем политику защиты данных

Home x 192.168.22.96 x demo.lab x IWM x IWTM x w10-d1 x w10-d2 x

InfoWatch Traffic Monitor Enterprise x +

← → C ▲ Не защищено | https://172.16.2.3/policy

Сводка События Отчеты Технологии Объекты защиты Персоны Политики Списки Управление Крауд Поиск событий Офицер безопасности

Вы редактируете конфигурацию с 06.05.2022 12:15. Применить Сохранить Сбросить Версия действующей конфигурации - № 9.

Политики

Добавить политику Фильтр

Политики защиты данных:

Политика защиты данных

Политика на любые данные

Передача Копирование Хранение Работа в приложениях

Политика защиты данных

Добавить правило

Название: Политика защиты данных

Период действия: Все время

Статус:

Защищаемые данные

Выбрать

Политика действует на любые данные, пока не сделан выбор

Описание

Введите описание

Создан: 06.05.2022 13:10 Изменен: 06.05.2022 13:10

Сохранить Отменить

## Добавляем правило передачи

The screenshot shows the 'Правило передачи' (Delivery Rule) configuration screen in the InfoWatch Traffic Monitor Enterprise web interface. The left panel displays a list of delivery rules, with one rule selected: 'Политика защиты данных' (Data Protection Policy). The right panel contains several tabs: 'Компьютеры' (Computers), 'Отправители' (Senders), 'Получатели' (Recipients), 'Дни действия правила' (Rule validity days), 'Часы действия правила' (Rule validity hours), 'Действия при срабатывании правила' (Actions when rule triggers), and 'Сохранить' (Save). The 'Отправители' tab is active, showing 'Любой отправитель' (Any sender) and 'Любой получатель' (Any recipient). The 'Получатели' tab shows 'CLIENT1', 'CLIENT2', 'DEMO-DC', 'DEMOLAB', and 'IWDM'. The 'Дни действия правила' tab shows 'Любой день недели' (Any day of the week). The 'Часы действия правила' tab shows '0:00 - 0:00'. The 'Действия при срабатывании правила' tab includes options like 'Начните вводить текст' (Start typing text) for 'Оставить почтовое уведомление' (Leave a mail notification), 'Заблокировать' (Block), 'Низкий' (Low) for 'Уровень нарушения' (Violation level), and 'Политика 3' (Policy 3) for 'Событие типа' (Event type). The 'Сохранить' (Save) button is at the bottom right.

## Политика 5

Переходим в объекты защиты и создаем новый объект защиты

The screenshot shows the 'Создать' (Create) dialog for a new protection object. The 'Название' (Name) field is filled with 'Политика 5'. The 'Статус' (Status) switch is turned on. The 'Описание' (Description) field is empty. At the bottom are 'Создать' (Create) and 'Отменить' (Cancel) buttons. The background shows the 'Объекты защиты' (Protection objects) section of the interface, where a catalog of protection objects is listed under 'Каталоги объектов защиты' (Protection object catalogs). The catalog includes categories like 'Финансы' (Finance), 'Управление компанией' (Company management), and 'Грифы конфиденциальности' (Confidentiality stamps).

## Добавляем

### Создание объекта защиты

Категории	Текстовые объекты	Эталонные документы	Бланки	Печати	Выгрузки из БД	Графические объекты
<input type="text"/> Поиск						
<input type="checkbox"/>	▲ Название		Дата создания		Описание	
<input checked="" type="checkbox"/>	Кредитная карта	17.11.2021 05:29		Система срабатывает на изображение лицевой стороны б...		
<input type="checkbox"/>	Паспорт гражданина РФ	17.11.2021 05:29		Система срабатывает на изображение главного разворота...		

10

**Создать****Отменить** Создать объект защиты на каждый выбранный элемент

## Добавляем

### Создание объекта защиты

Категории	Текстовые объекты 2	Эталонные документы	Бланки	Печати	Выгрузки из БД	Графические объекты
-----------	---------------------	---------------------	--------	--------	----------------	---------------------

Каталоги текстовых объектов		Текстовые объекты			
<input type="text"/> Поиск по каталогам		<input type="text"/> Поиск			
<input type="checkbox"/>	▲ Название		Дата создания	Страна	Описание
<input checked="" type="checkbox"/>	Номер кредитной карты	17.11.2021 05:29	Мировое сообщество	Номер кредитной карты	
<input checked="" type="checkbox"/>	Номер кредитной карты (16циф)	17.11.2021 05:29	Мировое сообщество	Номер кредитной карты	

10

**Создать****Отменить** Создать объект защиты на каждый выбранный элемент

## Важно! Ставим снизу галочку

Создание объекта защиты

Категории Текстовые объекты 2 Эталонные документы Бланки Печати Выгрузки из БД Графические объекты

Каталоги текстовых объектов

Помощь по каталогам

Все элементы Текстовые объе...

Текстовые объекты

Поиск

Название Дата создания Страна Описание

Номер кредитной карты 17.11.2021 05:29 Мировое сообщество Номер кредитной карты

Номер кредитной карты (16 циф... 17.11.2021 05:29 Мировое сообщество Номер кредитной карты

К < 1 2 3 4 > >

10

Создать Отменить  Создать объект защиты на каждый выбранный элемент

## Вот так выглядит

InfoWatch Traffic Monitor Enterprise

← → ⚡ Не защищено | https://172.16.2.3/protected/9A251692C314A79AC402666D5176AF900000000

Сводка События Отчеты Технологии Объекты защиты Персоны Политики Списки Управление Краудр

Поиск событий Офицер безопасности

Вы редактируете конфигурацию с 06.05.2022 12:15. Применить Сохранить Сбросить Версия действующей конфигурации - № 9.

Каталоги объектов защиты

Помощь по каталогам

Все Активные Невидимые

Все элементы

- Графическая информация
- Договоры и контракты
- Конкурсная документация
- Маркетинг
- Отдел кадров
- Персональные данные
- Политика 3
- Политика 5

Политика 5

Название Элементы технологии Дата создания Дата изменения Описание

Графический объект: Кредитная карта Кредитная карта 06.05.2022 13:18 06.05.2022 13:18

Текстовый объект: Номер кредитной карты Номер кредитной карты 06.05.2022 13:18 06.05.2022 13:18

Текстовый объект: Номер кредитной карты (16 цифр) Номер кредитной карты (16 цифр) 06.05.2022 13:18 06.05.2022 13:18

## Переходим, списки – теги, создаем новый тег

InfoWatch Traffic Monitor Enterprise

← → ⚡ Не защищено | https://172.16.2.3/lists/tag

Сводка События Отчеты Технологии Объекты защиты Персоны Политики Списки Управление Краудр

Вы редактируете конфигурацию с 06.05.2022 12:15. Применить Сохранить Сбросить Версия действующей конфигурации - № 9.

Управление тегами

С помощью тегов удобно группировать объекты, хранящиеся в Системе, и собирать статистику по ним.

Название Цвет Описание

+ VIP На рассмотрение Политика 3

Создать тег

Название Помощь по каталогам

Цвет

Описание

Сохранить Отменить

## Создаем новую политику защиты данных, защищаемые данные – указывает политика нашу

The screenshot shows the 'Politički' (Policy) section of the InfoWatch Traffic Monitor Enterprise web interface. A new policy is being created, titled 'Политика защиты данных #1'. The 'Защищаемые данные' (Protected data) section is visible, showing a selected category 'Политика 5'. The 'Описание' (Description) field contains the placeholder 'Введите описание' (Enter description). The status bar at the bottom right indicates the creation date and time: 'Создан: 06.05.2022 13:19' and 'Изменен: 06.05.2022 13:19'.

## Правило передачи

The screenshot shows the 'Правило передачи' (Transmission Rule) section of the InfoWatch Traffic Monitor Enterprise web interface. A new rule is being created, titled 'Правило передачи'. The 'Направление маршрута' (Route direction) is set to '→ В одну сторону' (One-way). The 'Компьютеры' (Computers) field lists 'CLIENT1' and 'CLIENT2'. The 'Действия при срабатывании правила' (Actions on rule trigger) section includes actions like 'Отправить почтовое уведомление' (Send email notification) and 'Назначить событию вердикт' (Assign verdict to event). The status bar at the bottom right indicates the creation date and time: 'Создан: 06.05.2022 13:19' and 'Изменен: 06.05.2022 13:19'.

Вот так должно получится

The screenshot shows the InfoWatch Traffic Monitor Enterprise web interface. The top navigation bar includes links for 'Сводка', 'События', 'Отчеты', 'Технологии', 'Объекты защиты', 'Персоны', 'Политики', 'Списки', 'Управление', 'Краулер', 'Поиск событий', and 'Офицер безопасности'. A message at the top states: 'Вы редактируете конфигурацию с 06.05.2022 12:15.' Below this, there are two policy sections: 'Политика 5' and 'Политика 2'. Each section has tabs for 'Передача 1', 'Копирование', 'Хранение', and 'Работа в приложениях'. The 'Правило передачи' (Transmission Rule) panel on the right defines a rule for 'CLIENT1' to 'CLIENT2' with various conditions like 'Направление маршрута' (One-way/Both ways), 'Тип события' (Type), and 'Дни действия правила' (Any day of the week). The 'Действия при срабатывании правила' (Actions on rule trigger) panel defines actions like 'Отправить почтовое уведомление' (Email notification) and 'Назначить событию вердикт' (Assign verdict). Buttons for 'Сохранить' (Save) and 'Отменить' (Cancel) are at the bottom.

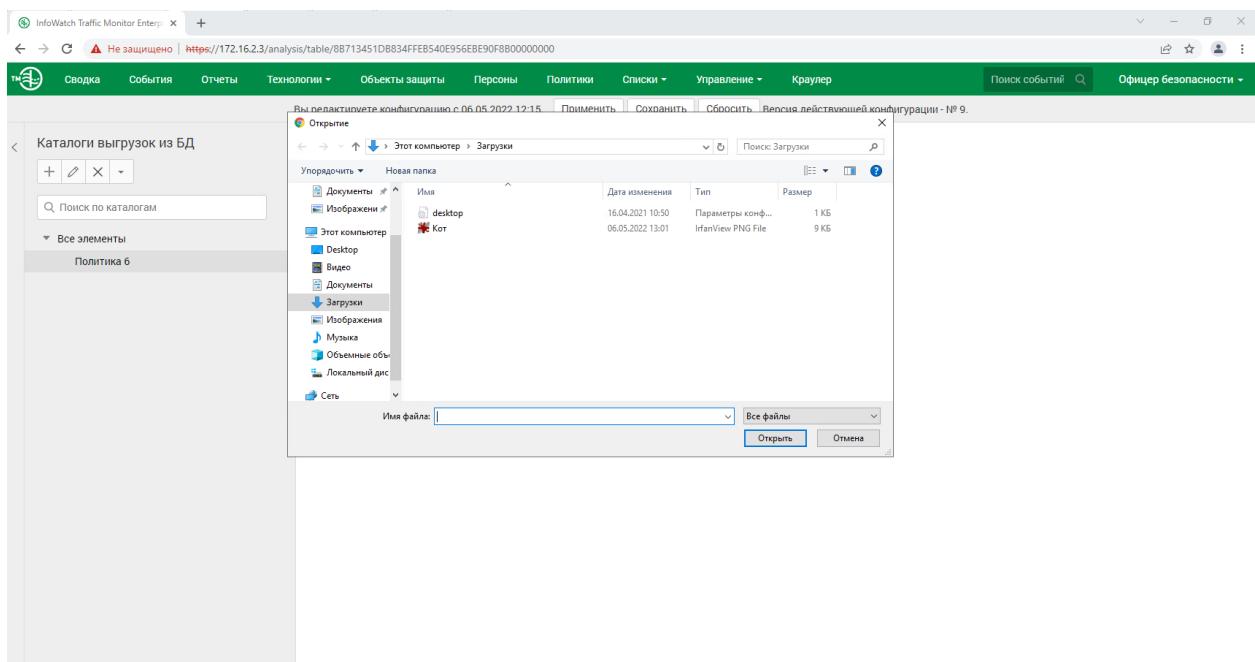
## Политика 6

Переходим, технологии – выгрузки из бд

Создаем каталог

The screenshot shows the 'Каталоги выгрузок из БД' (Export Catalogs) section of the InfoWatch Traffic Monitor Enterprise interface. On the left, there's a sidebar with a search bar and a 'Все элементы' (All elements) button. On the right, a 'Создать' (Create) dialog box is open, prompting for 'Название' (Name) and 'Описание' (Description). The 'Название' field contains 'Политика 6'. The 'Описание' field has the placeholder 'Добавить описание' (Add description). At the bottom of the dialog are 'Создать' (Create) and 'Отменить' (Cancel) buttons.

## Выгрузка из БД



Создайте каталог выгрузок «Политика 3». Откройте созданный каталог и с помощью кнопки «+», загрузите в него выгрузку из БД. Затем, выберите загруженную выгрузку и нажмите кнопку «редактировать», изображенную в виде карандаша. Измените условие по умолчанию, чтобы оно совпало с условием, изображенным на рисунках 85 и 86.

Редактировать ×

Название	Выгрузка из БД.csv
Название файла	Выгрузка из БД.csv
Формат файла	text/csv

Режим обновления: Ручной

Условие обнаружения

+		
Название условия	Правило	Минимальное ко...
Условие по зада...		5

Описание

Введите описание

Создан: 22.02.2022 07:38      Изменен: 22.02.2022 07:38

Рисунок 85 – «Условие выгрузки из БД»

Название условия Условие по заданию

Минимальное количество строк 5

Условие обнаружения **5 + 7 + 10 + 14 + 16 + 18**

**Сохранить** Отменить

Рисунок 85 – «Условие выгрузки из БД»

Создайте тег «Политика 3». Перейдите к политикам и создайте «Политику 3» (политика защиты данных), в качестве защищаемых данных выберите каталог объектов защиты «Политика 3». Создайте новое правило передачи в соответствии с рисунком 86.

Правило передачи

Направление маршрута → В одну сторону ⇡ В оба направления

Тип события Тип

Компьютеры Начните вводить текст +

Отправители ? = Начните вводить текст +

Получатели ? = Начните вводить текст +

Дни действия правила Любой день недели

Часы действия правила 0:00 - 0:00

Действия при срабатывании правила

Отправить почтовое уведомление Начните вводить текст +

Назначить событию вердикт Разрешить

Назначить событию уровень нарушения Низкий

Назначить событию теги Политика 3

Назначить отправителю статус Выберите статус

Удалить событие

Рисунок 86 – «Правило передачи политики 3»

## Модуль 4

The screenshot displays two windows of the InfoWatch Traffic Monitor Enterprise software running on a Windows host.

**Top Window: Role Creation**

The main pane shows a list of roles:

Название	Пользователи	Описание
Администратор	administrator, iwtm-officer, officer	Представлена роль админ
Офицер безопасности	iwtm-officer, officer	Представлена роль офице

A modal window titled "Создание роли" (Create Role) is open, showing the configuration for a new role named "DLP".

Название	Название	Пользователи	Описание
DLP			

The "Редактирование запросов" (Edit queries) checkbox is selected. Other checkboxes like "Просмотр панелей" (View panels), "Выполнение запросов и просмотр событий" (Execute queries and view events), and "Редактирование отчетов" (Edit reports) are also present but not selected.

**Bottom Window: User Creation**

The main pane shows a list of users:

Логин	Название	Email	Роль	Области видимости	Описание
iwtm-officer	iwtm-officer	iwtm@officer.ru	Администратор	VIP, Полный дос	
administrator	Administrator		Администратор		Представлена
officer	Офицер безопасности		Администратор	Полный доступ	Представлена

A modal window titled "Создание пользователя" (Create User) is open, showing the configuration for a new user named "DLP-user".

Логин	Статус	Email
DLP-user	Активен	DLP@mail.ru

The "Выбор роли" (Select Role) sub-modal is open, showing the "DLP" role selected.

Название	Пользователи	Описание
DLP		

**Taskbar and Status Bar**

The taskbar shows several icons including File Explorer, Task View, Start, Taskbar settings, and a search bar. The status bar at the bottom right indicates the date and time as "29.04.2022 13:30".

demo.lab - VMware Workstation

Library Type here to search

My Computer 192.168.22.96 demo.lab iWDM iWTM w10-d1 w10-d2

Home 192.168.22.96 demo.lab iWDM iWTM w10-d1 w10-d2

InfoWatch Traffic Monitor Enterprise

Сводка События Отчеты Технологии Объекты защиты Персоны Политики Списки Управление Краулер Поиск событий Выгрузки Офицер безопасности

Управление доступом Пользователи

Роли

Области видимости

Логин Название Email Роли Области видимости Описание

iwtm-officer iwtm-officer ivtmm@officer.ru Администратор VIP, Полный дос...

administrator Администратор Администратор Предоставлено...

officer Офицер безопасности Администратор Полный доступ Предоставлено...

Создание пользователя

Логин DLP-user

Статус Активен

Email DLP@mail.ru

Полное имя DLP-user

Роль DLP X

Области видимости Не выбрано

Описание Описание

Пароль \*\*\*\*

Подтверждение пароля \*\*\*\*

Сохранить Отменить

## Удаляем все сводки

demo.lab - VMware Workstation

Library Type here to search

My Computer 192.168.22.96 demo.lab iWDM iWTM w10-d1 w10-d2

Home 192.168.22.96 demo.lab iWDM iWTM w10-d1 w10-d2

InfoWatch Traffic Monitor Enterprise

Сводка События Отчеты Технологии Объекты защиты Персоны Политики Списки Управление Краулер Поиск событий Выгрузки Офицер безопасности

Сводка

+ Сводка за последние 7 дней

Динамика нарушений за период

Без учета правил 23.04.2022 - 29.04.2022

Топ нарушителей

Без учета правил 23.04.2022 - 29.04.2022

Для выбранного периода данные отсутствуют

Для выбранного периода данные отсутствуют

Динамика статусов за период

Без учета правил 23.04.2022 - 29.04.2022

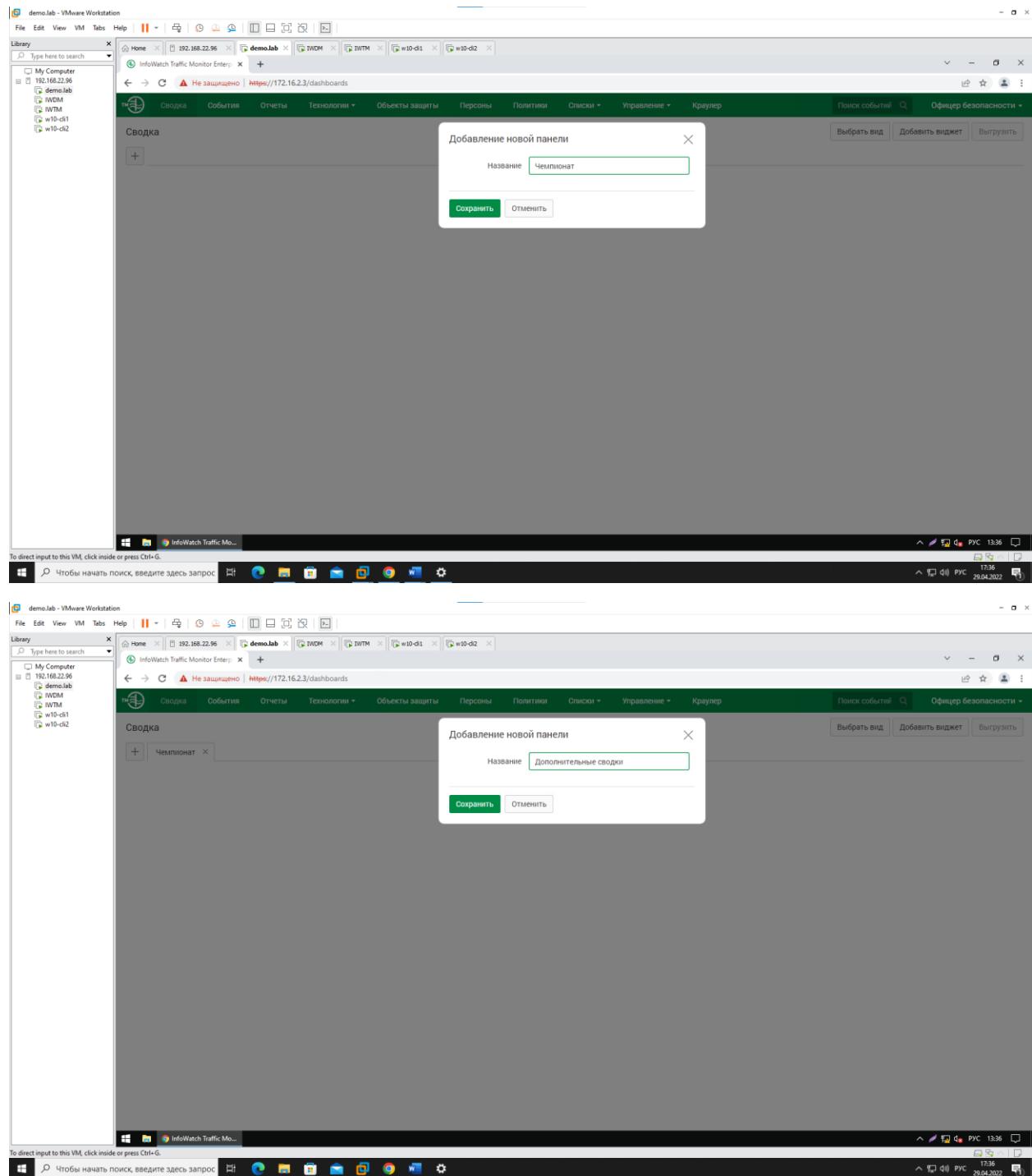
Статусы	Персоны	Компьютеры
Новый	5	3

Статистика по каталогам объектов защиты

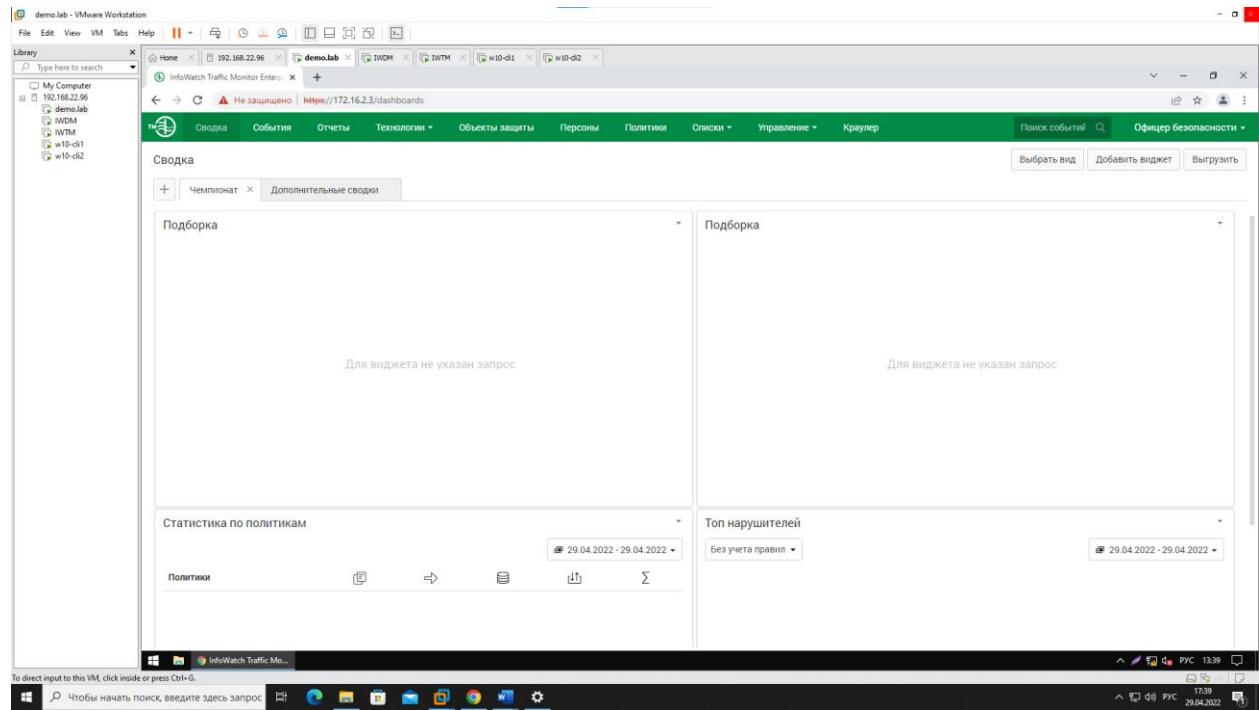
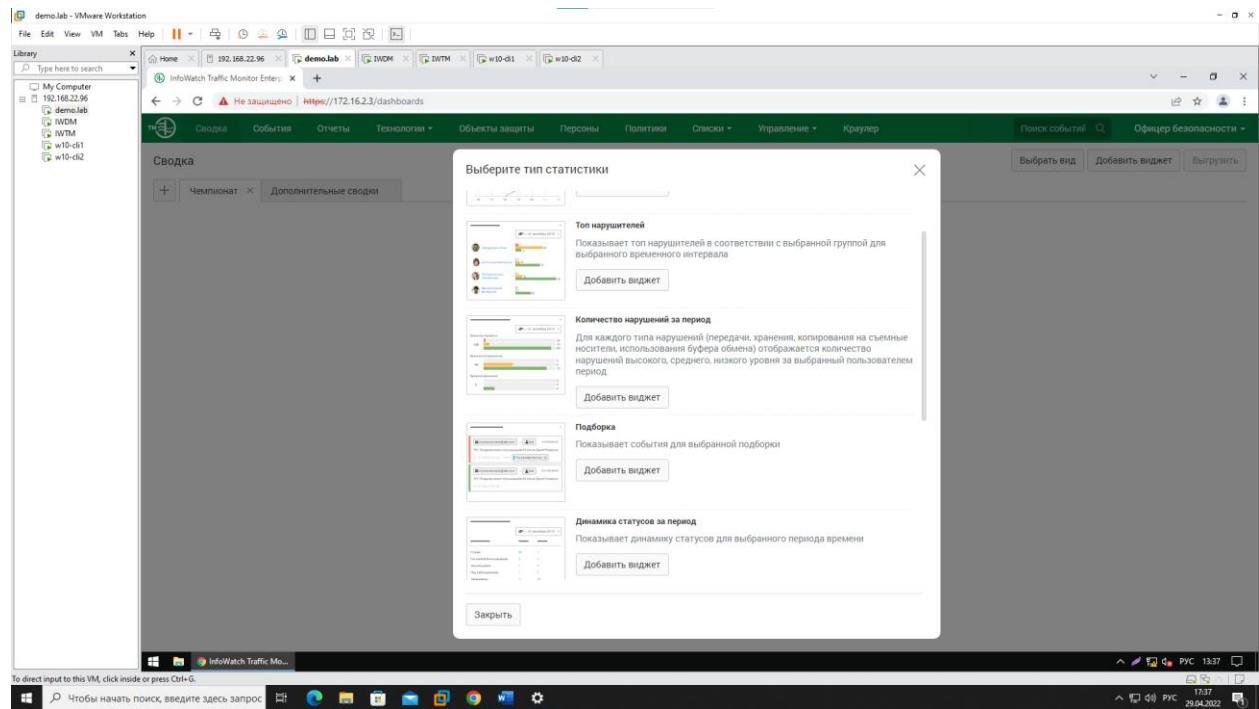
Без учета правил 23.04.2022 - 29.04.2022

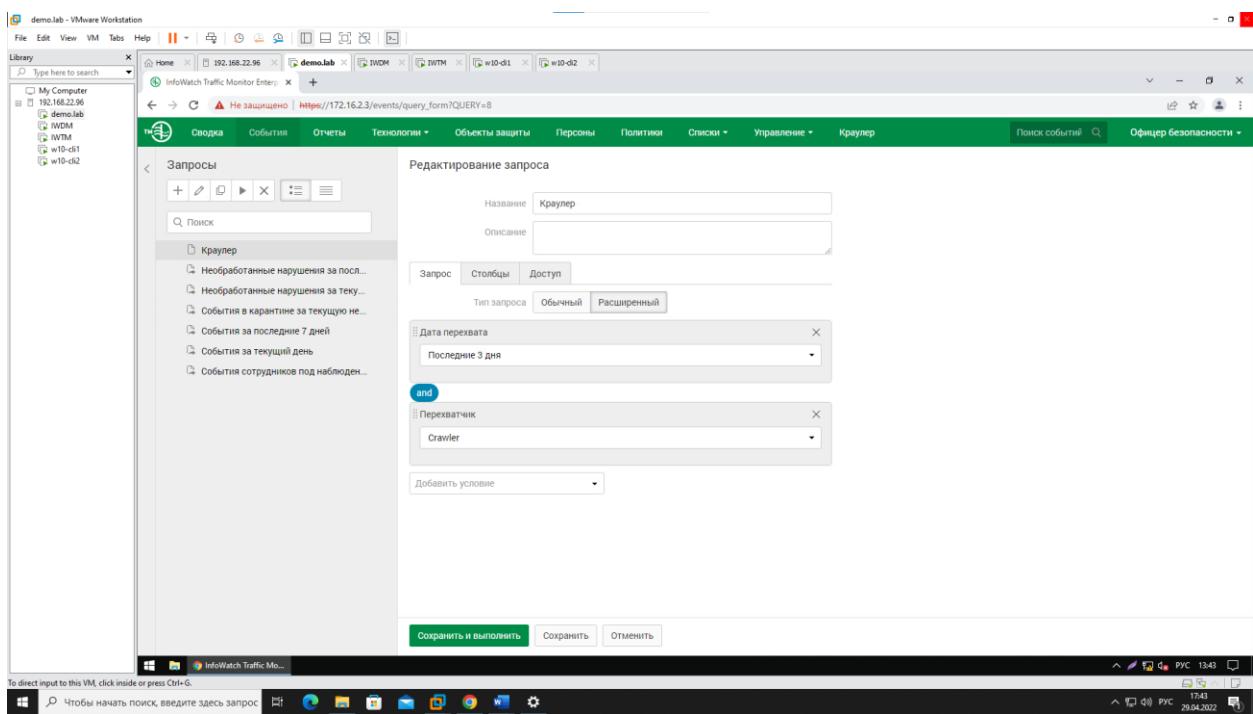
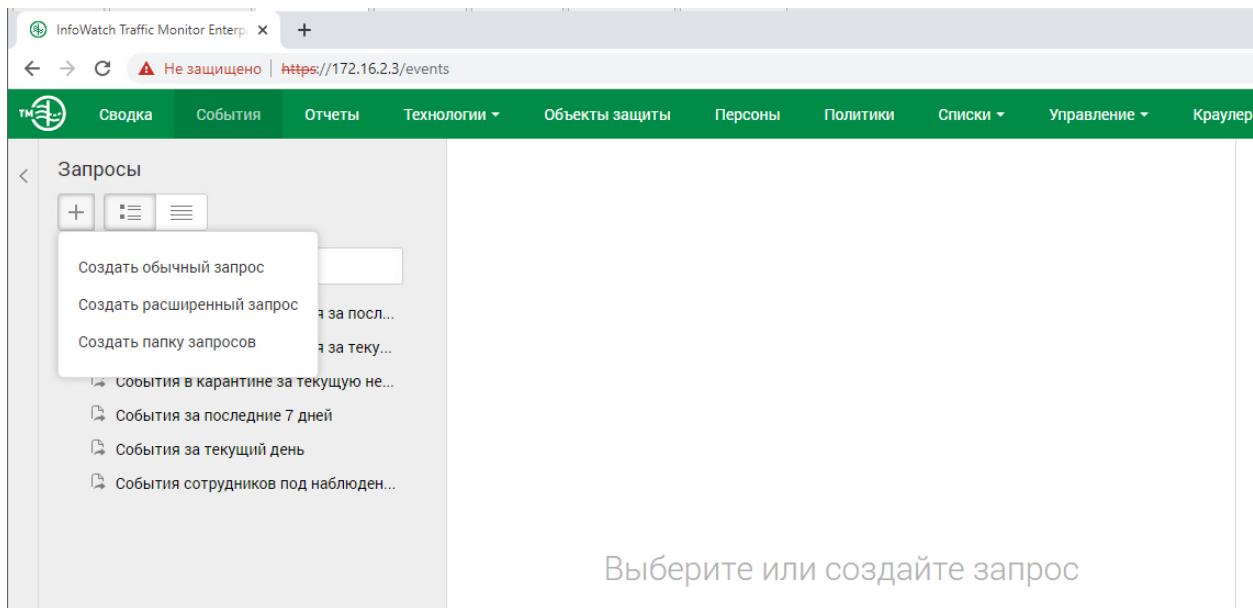
Каталог объекта защиты

13:35 13:35 29.04.2022

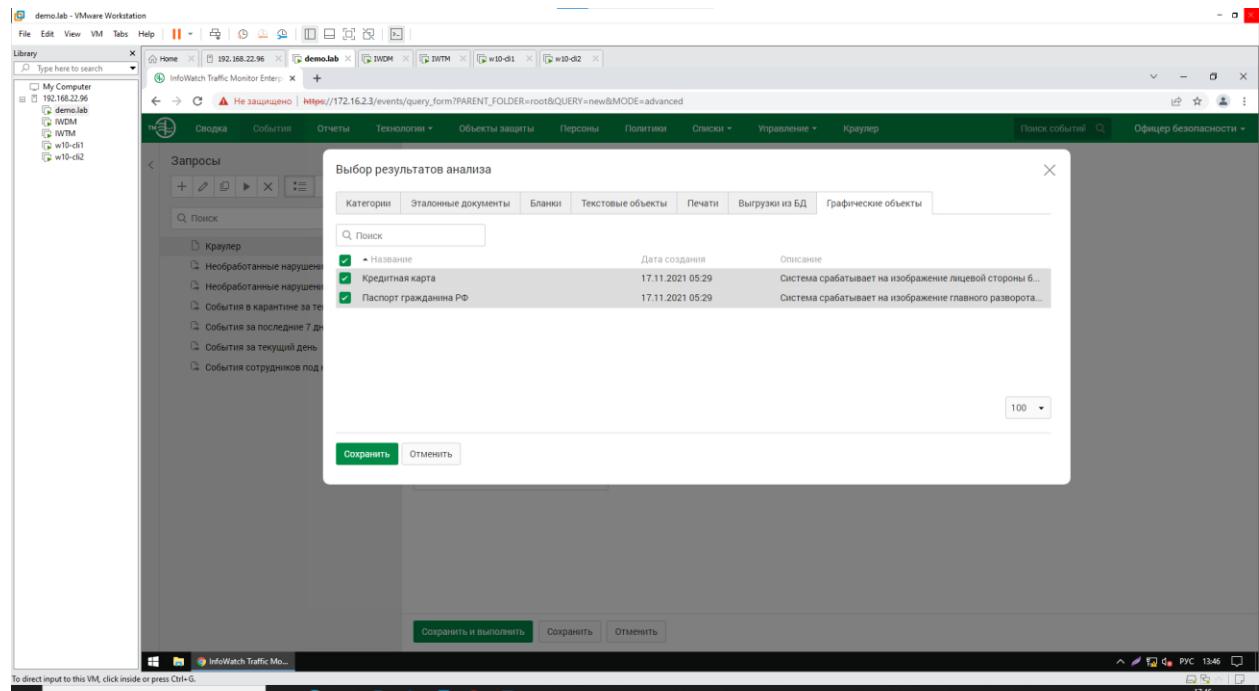


## Добавляем подборку





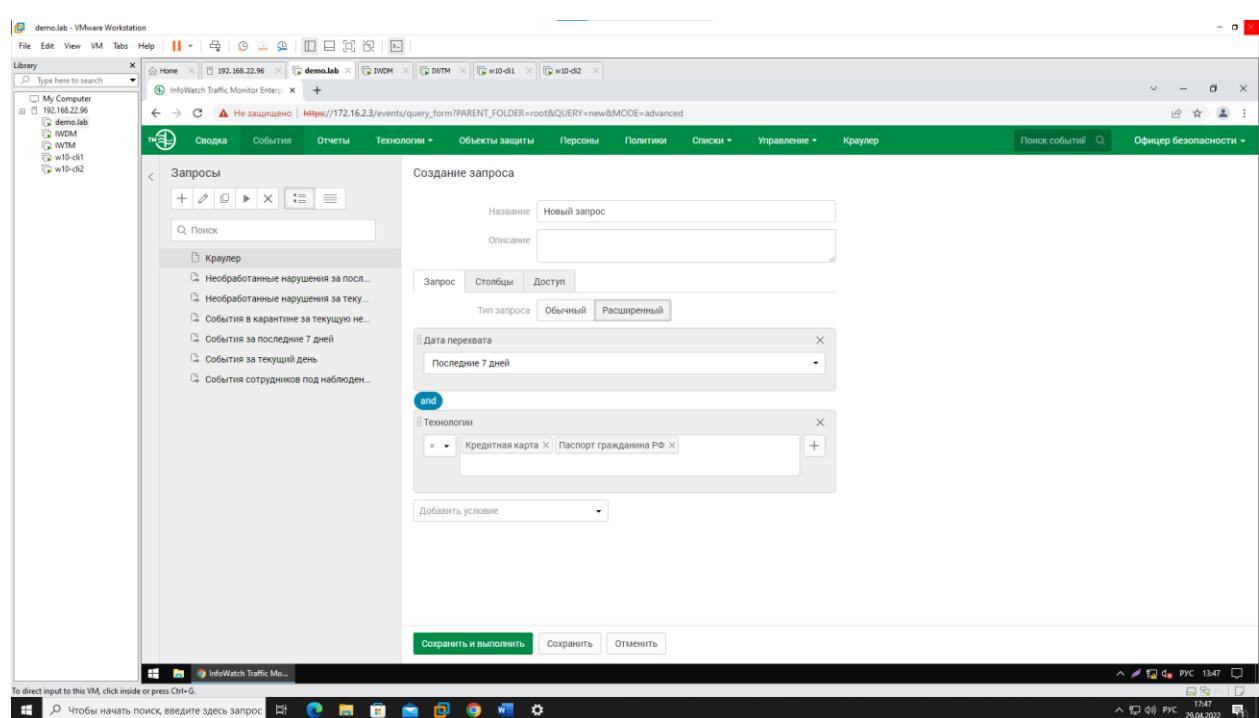
## Добавляем условие – технологии



Выбор результатов анализа

Категория	Название	Дата создания	Описание
<input checked="" type="checkbox"/>	Название	17.11.2021 05:29	Система срабатывает на изображение лицевой стороны 6...
<input checked="" type="checkbox"/>	Кредитная карта	17.11.2021 05:29	Система срабатывает на изображение главного разворота...
<input checked="" type="checkbox"/>	Паспорт гражданина РФ	17.11.2021 05:29	

Сохранить Отменить

Создание запроса

Название: Новый запрос

Описание:

Запрос Столбцы Доступ

Тип запроса: Обычный [Расширенный]

Дата перехвата: Последние 7 дней

and

Технологии: Кредитная карта | Паспорт гражданина РФ

Добавить условие

Сохранить и выполнить Сохранить Отменить

## Сводка

+ Чемпионат × Дополнительные сводки

### Общие настройки виджета

Название Краулер

Интервал обновления: Не обновлять ▾

Подборка Краулер X ▾

Событий на странице

**Сохранить** **Отменить**

### Общие настройки виджета

Название Технологии

Интервал обновления: Не обновлять ▾

Подборка Новый запрос X ▾

Событий на странице

**Сохранить** **Отменить**

### Общие настройки виджета

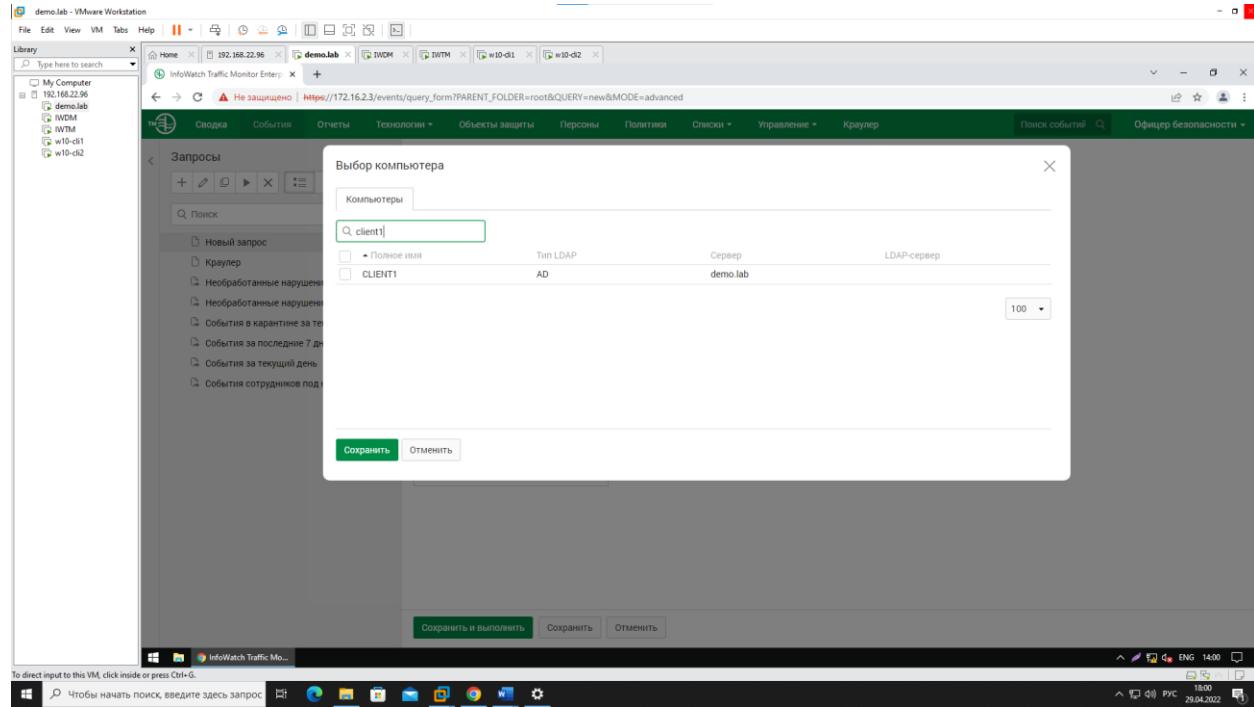
Название	Статистика по политикам
Интервал обновления:	Не обновлять ▾
Период:	Текущий месяц ▾
Политики	Начните вводить текст <input type="text"/> <span>+</span>
<span>Сохранить</span> <span>Отменить</span>	

### Общие настройки виджета

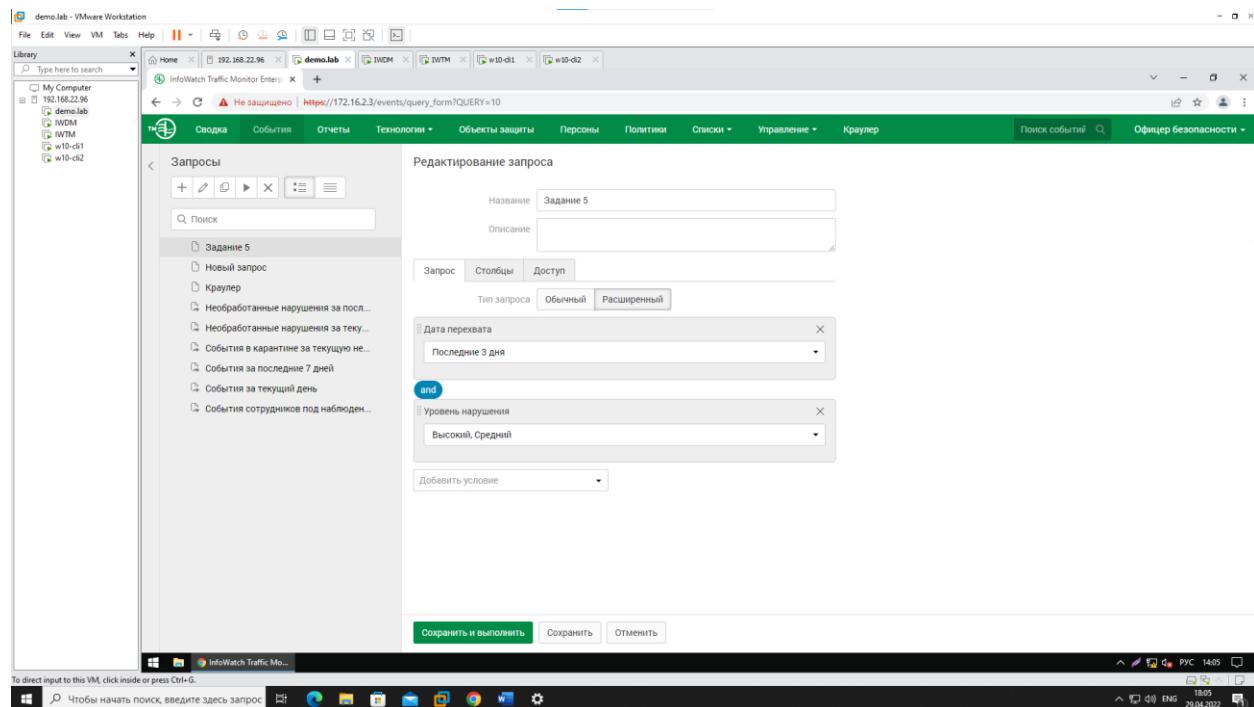
Название	Топ нарушителей
Интервал обновления:	Не обновлять ▾
Период:	Последние 30 дней ▾
Количество нарушителей	10 <span>▲</span> <span>▼</span>
Группы	Введите название группы <input type="text"/> <span>+</span>
Статусы	Выберите статус <input type="text"/> <span>+</span>
<span>Сохранить</span> <span>Отменить</span>	

## Задание 5

Добавляем компьютеры нарушителей – client1 и client2



Добавляем уровень нарушения – высокий и средний



### Общие настройки виджета

Название	Отображение нарушений от обоих компьютеров
Интервал обновления:	Не обновлять ▾
Подборка	Задание 5 <span style="float: right;">×</span> ▾
Событий на странице	<span style="float: right;">▲ ▾</span>

Сохранить Отменить

### Задание 4

#### Дополнительные сводки

### Общие настройки виджета

Название	Высокий уровень угрозы на копирования
Интервал обновления:	Не обновлять ▾
Подборка	Задание 4 <span style="float: right;">×</span> ▾
Событий на странице	<span style="float: right;">▲ ▾</span>

Сохранить Отменить

demo.lab - VMware Workstation

File Edit View VM Tabs Help

Library Type here to search

My Computer 192.168.2.96 demo.lab IWDW IWTM w10-d1 w10-d2

Home Не защищено https://172.16.2.3/events/query\_form?PARENT\_FOLDER=root&QUERY=new&MODE=advanced

Сводка События Отчеты Технологии Объекты защиты Персоны Политики Списки Управление Краупер Поиск событий Офицер безопасности

Запросы + Новый запрос Задание 5

Краупер Новый запрос Задание 5 Необработанные нарушения за посещение Необработанные нарушения за текущую неделю События в карантине за текущую неделю События за последние 7 дней События за текущий день События сотрудников под наблюдением

Создание запроса

Название: Задание 4

Описание:

Запрос Столбцы Доступ

Тип запроса: Обычный Расширенный

Дата перехода: Последние 7 дней

and Уровень нарушения: Высокий

and Тип нарушений: Нарушение копирования

Добавить условие

Сохранить и выполнить Сохранить Отменить

To direct input to this VM, click inside or press Ctrl+G.

Чтобы начать поиск, введите здесь запрос

Последние 18:09 29.04.2022

demo.lab - VMware Workstation

File Edit View VM Tabs Help

Library Type here to search

My Computer 192.168.2.96 demo.lab IWDW IWTM w10-d1 w10-d2

Home Не защищено https://172.16.2.3/events/query\_form?PARENT\_FOLDER=root&QUERY=new&MODE=advanced

Сводка События Отчеты Технологии Объекты защиты Персоны Политики Списки Управление Краупер Поиск событий Офицер безопасности

Сводка Чемпионат Дополнительные сводки

Краупер Подборка Технологии Подборка

Выбрать вид Добавить виджет Выгрузить

Статистика по политикам Статистика по политикам 01.04.2022 - 30.04.2022 Без учета правил 31.03.2022 - 29.04.2022

Политики

Статистика по нарушителям Топ нарушителей Без учета правил 31.03.2022 - 29.04.2022

Поиск событий ENG 14:39

Чтобы начать поиск, введите здесь запрос

Последние 18:39 29.04.2022

