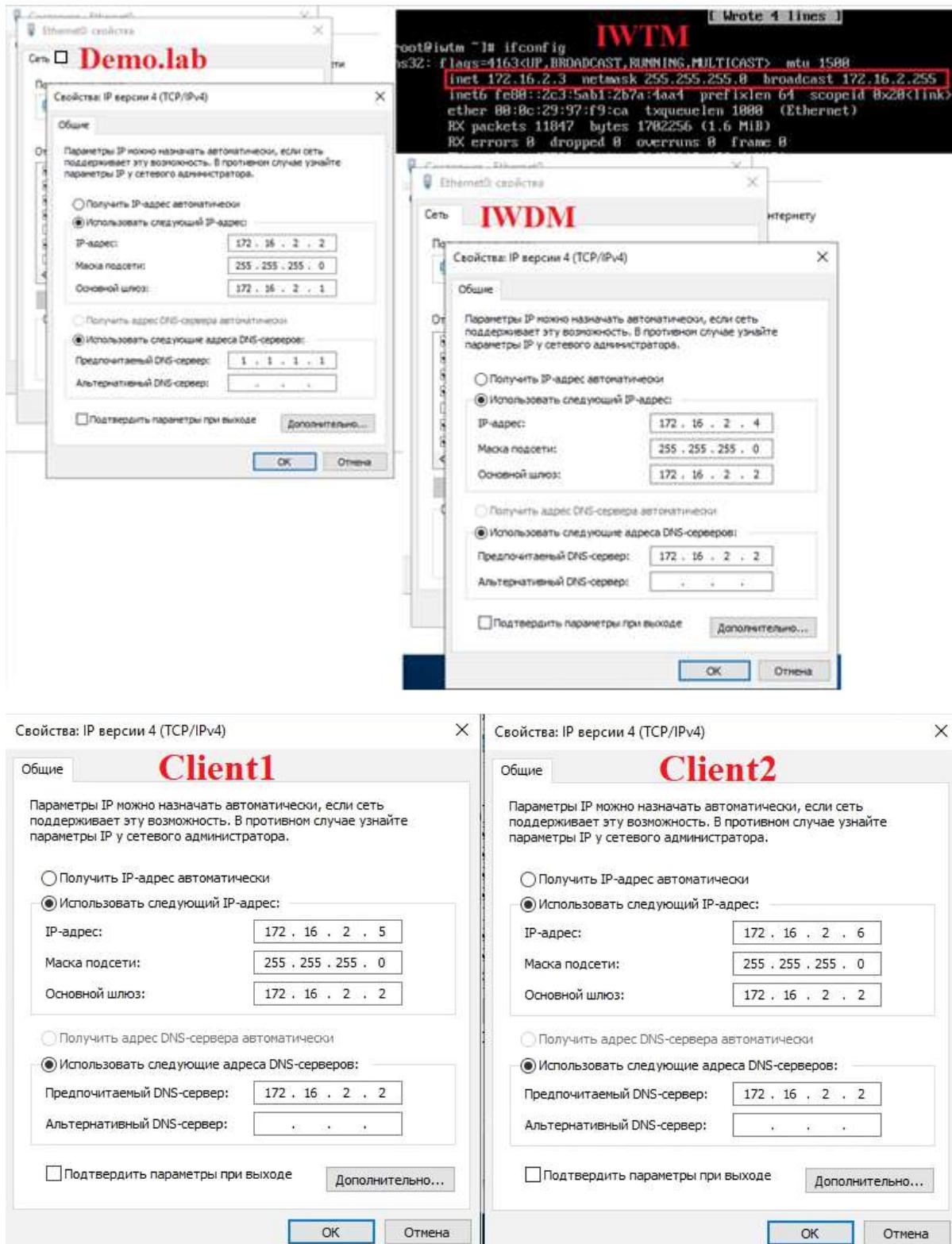


IP-адреса Demo.lab, IWTM, IWDM, Client1, Client2



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: Idap-sync, пароль: xxXX1234, права пользователя домена

Создаем пользователей и добавляем администратору права –

Администратора, Администратора Домена (Domain Admin)

The screenshot shows two instances of the Active Directory Users and Computers snap-in. The left window displays the 'demo.lab' domain structure with several objects listed under 'Champ'. The right window shows the properties of the 'iw-admin' user object, specifically the 'Memberships' tab, where the 'Administrators' group is selected.

Left Window (Active Directory - Пользователи и компьютеры):

Имя	Тип	Описание
CLIENT1	Компьютер	
CLIENT2	Компьютер	
IWDM	Компьютер	
iw-admin	Пользователь	
iwtm-officer	Пользователь	
Idap-sync	Пользователь	
user-agent1	Пользователь	
user-agent2	Пользователь	

Right Window (Active Directory - Пользователи и компьютеры):

Properties of user 'iw-admin'

Memberships tab:

Имя	Папка доменных служб Active Directory
Administrators	demo.lab/Builtin
Domain Admins	demo.lab/Users
Domain Users	demo.lab/Users

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.

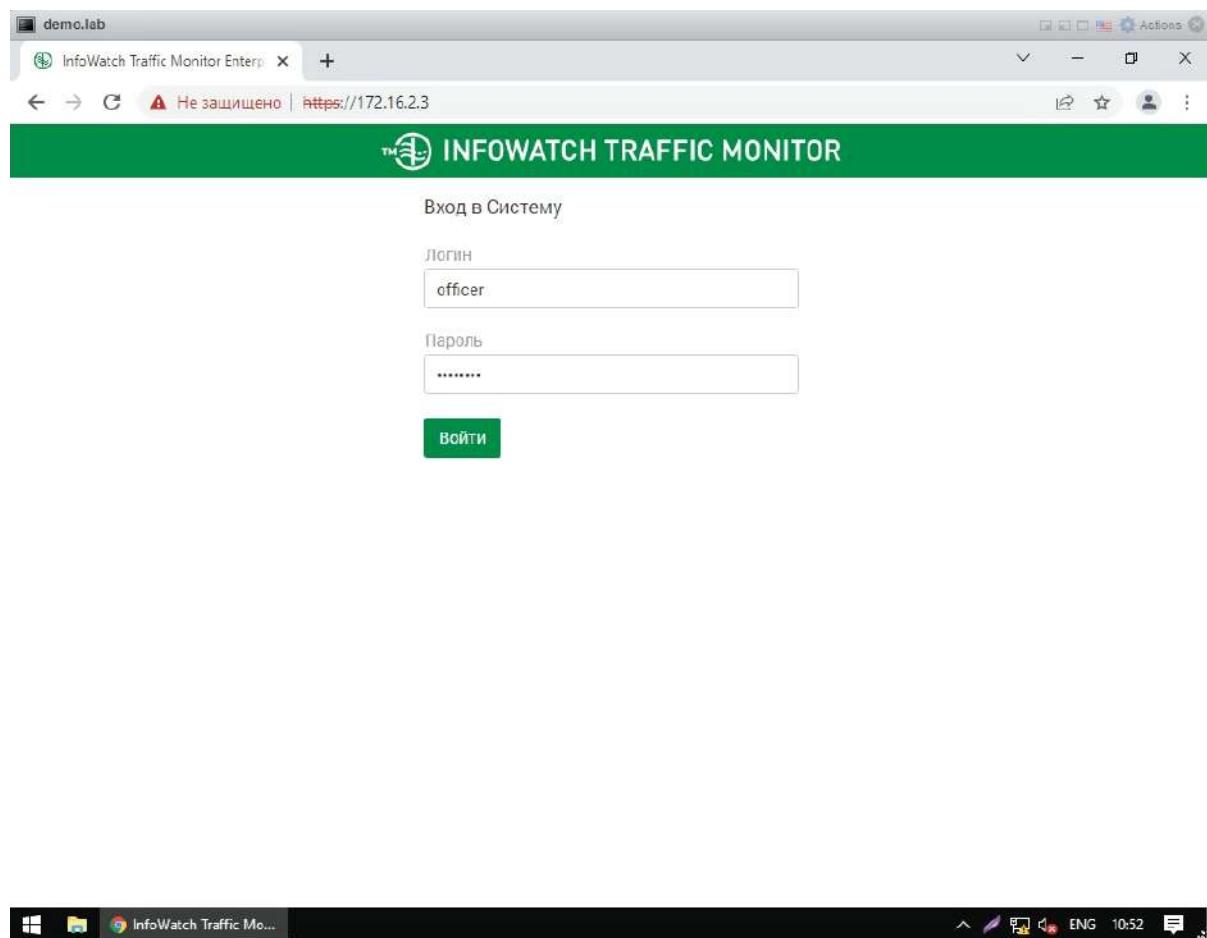
Для входа в веб-консоль необходимо настроить использование ранее

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

LDAP-серверы

+ | Edit | X | ▾

Demo.lab

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					
Пользователи							
Роли							
Области видимости							
<input type="checkbox"/>		iw-admin	Название	Email	Роль	Области видимости	Описание
<input type="checkbox"/>		iwtn-officer	iwtn-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`.

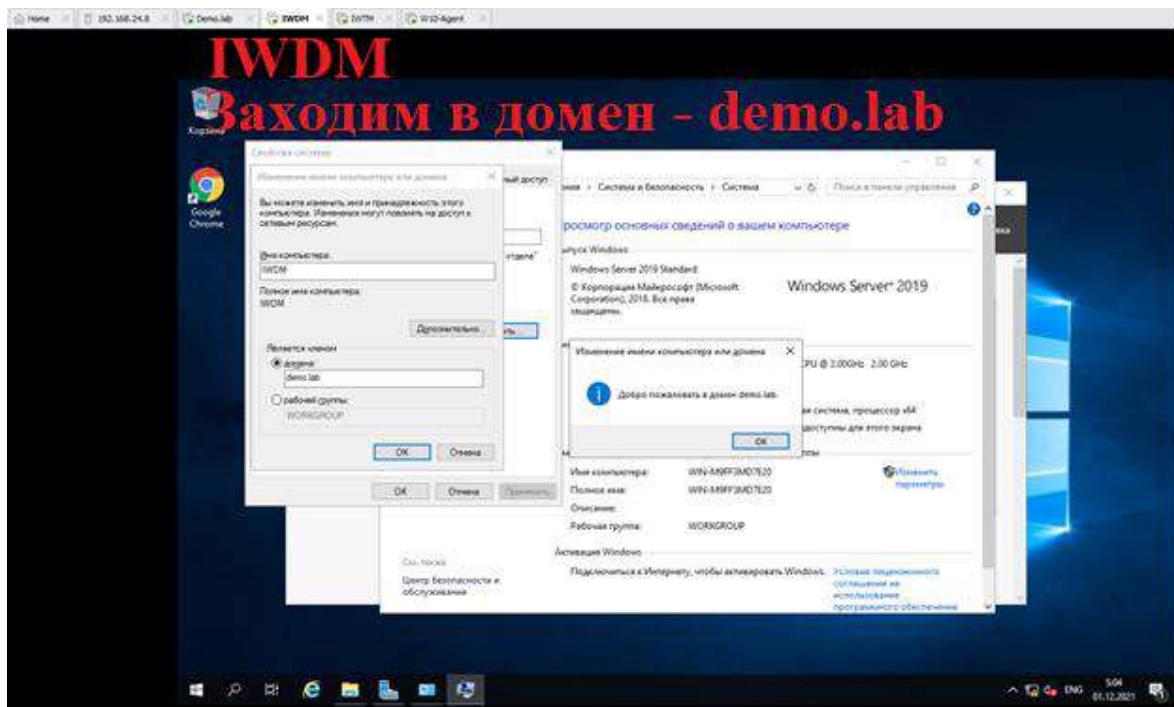
Установить сервер агентского мониторинга с параметрами по умолчанию, подключившись к ранее созданной БД.

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`

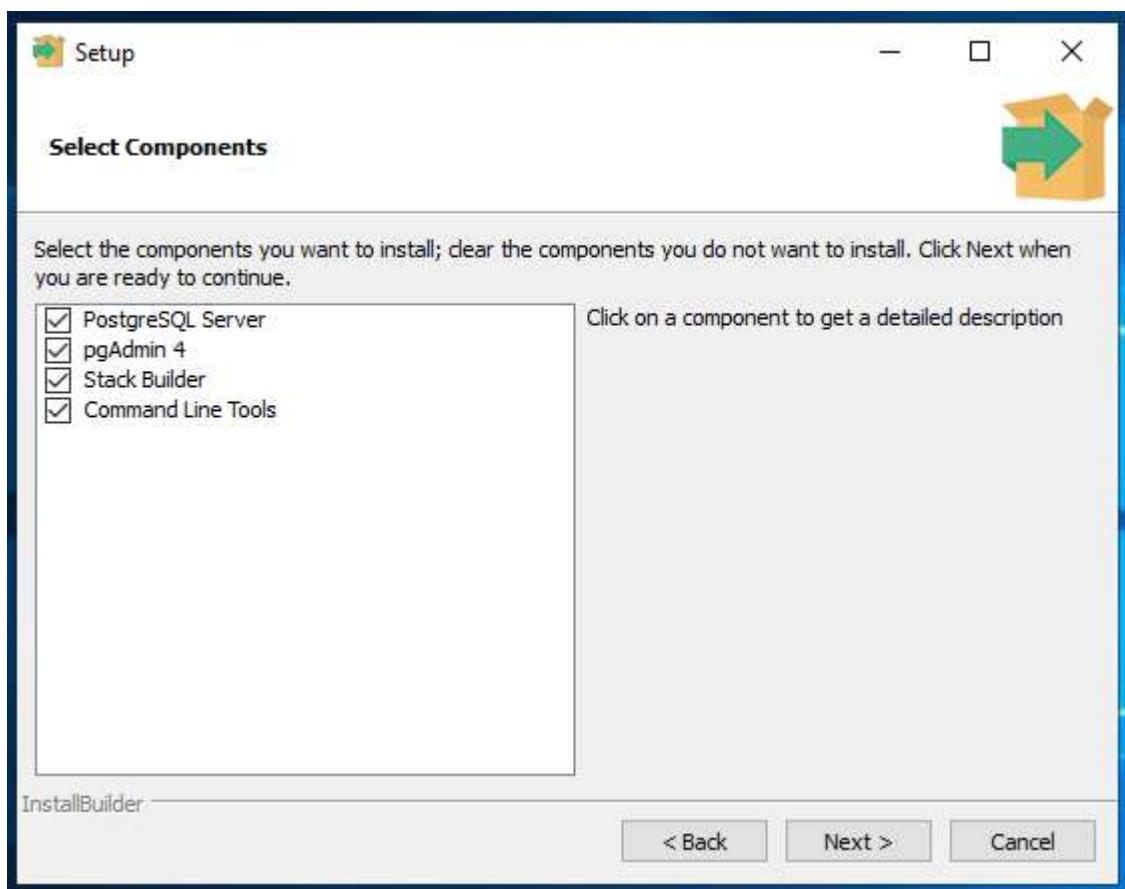
Синхронизировать каталог пользователей и компьютеров с Active Directory.

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

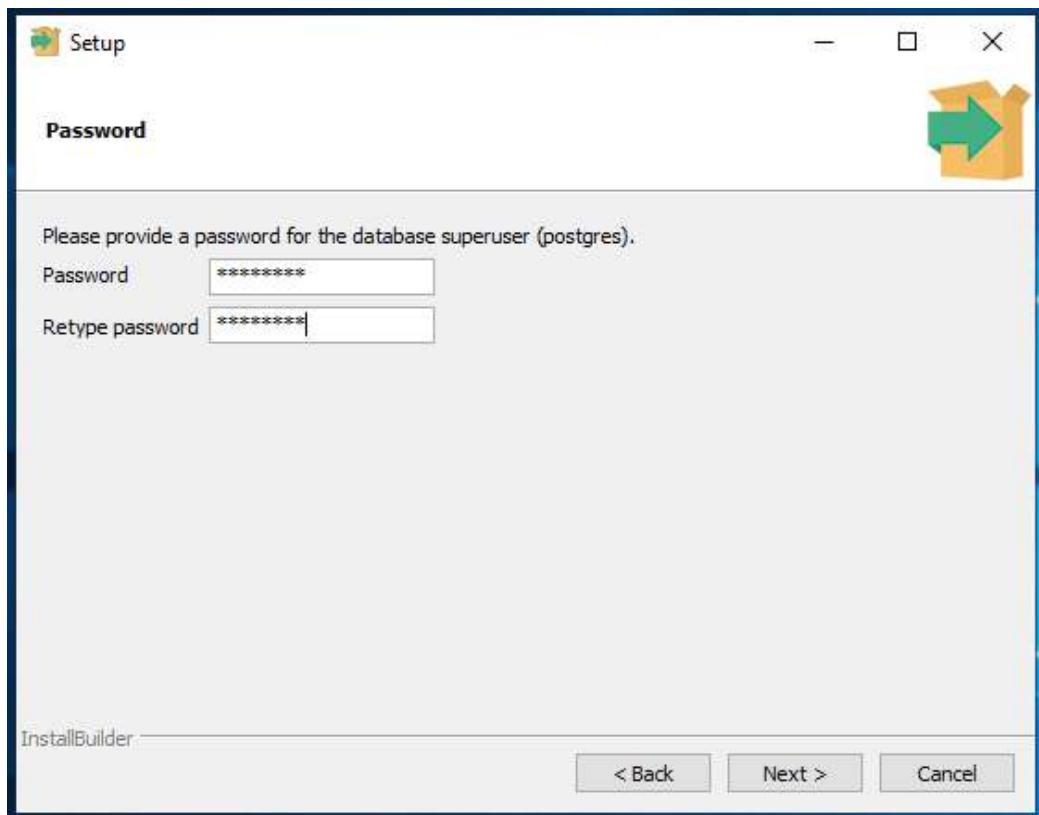
Проверить работоспособность входа в консоль управления без ввода пароля. Если сервер не введен в домен или работает от другого пользователя, данная опция работать не будет.



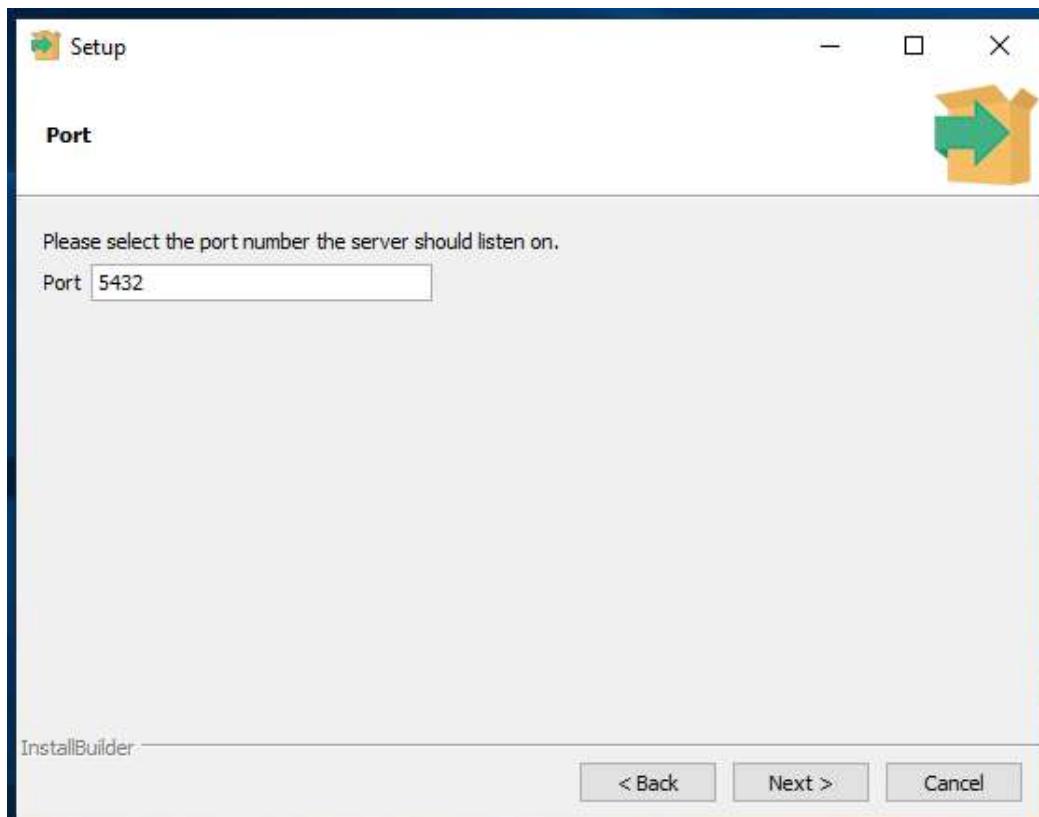
После перезагрузки заходим под iw-admin



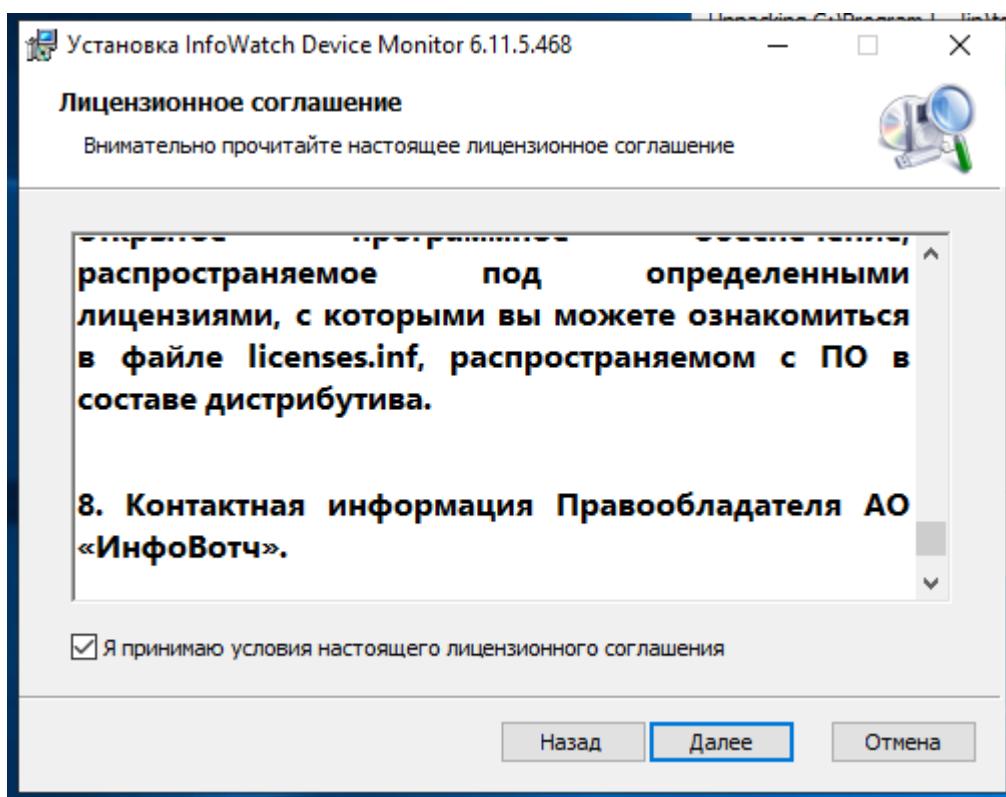
Вводим стандартный пароль



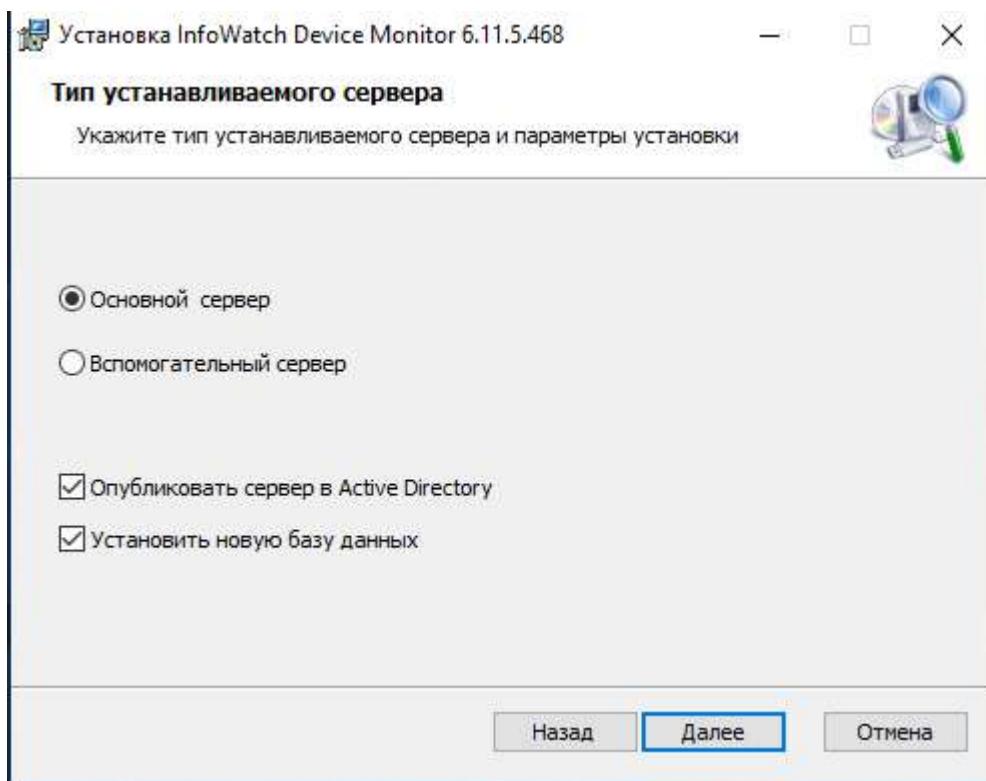
Порт оставляем по умолчанию

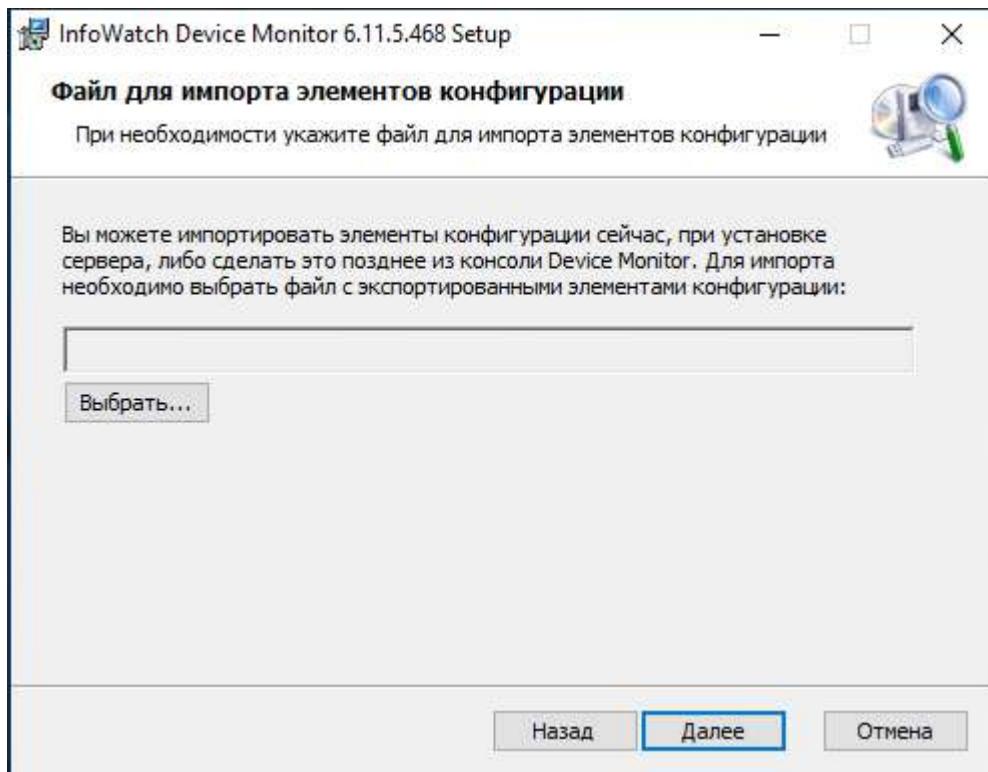


Затем, переходим к установке InfoWatch Device Monitor

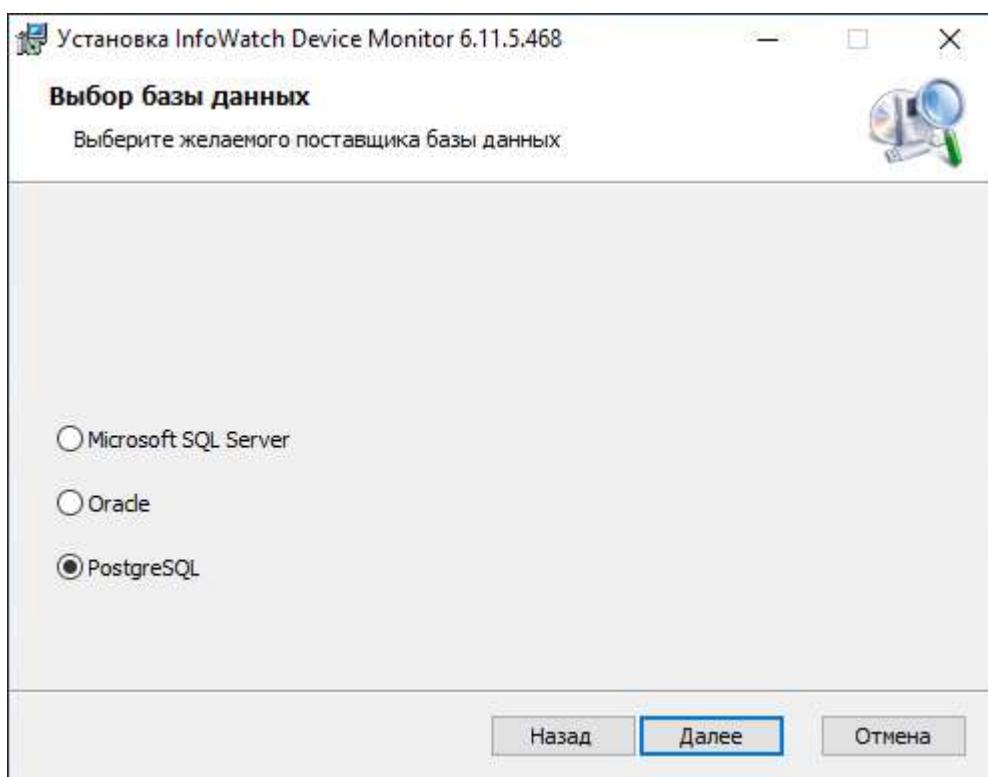


Оставляем галочку на основном сервере

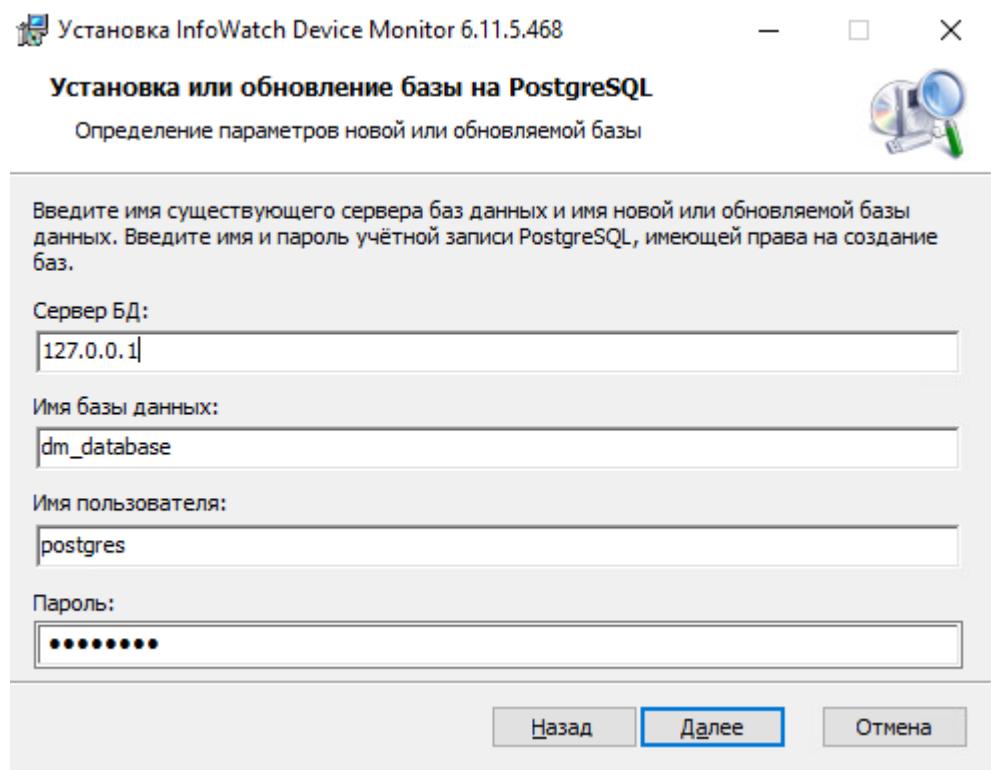




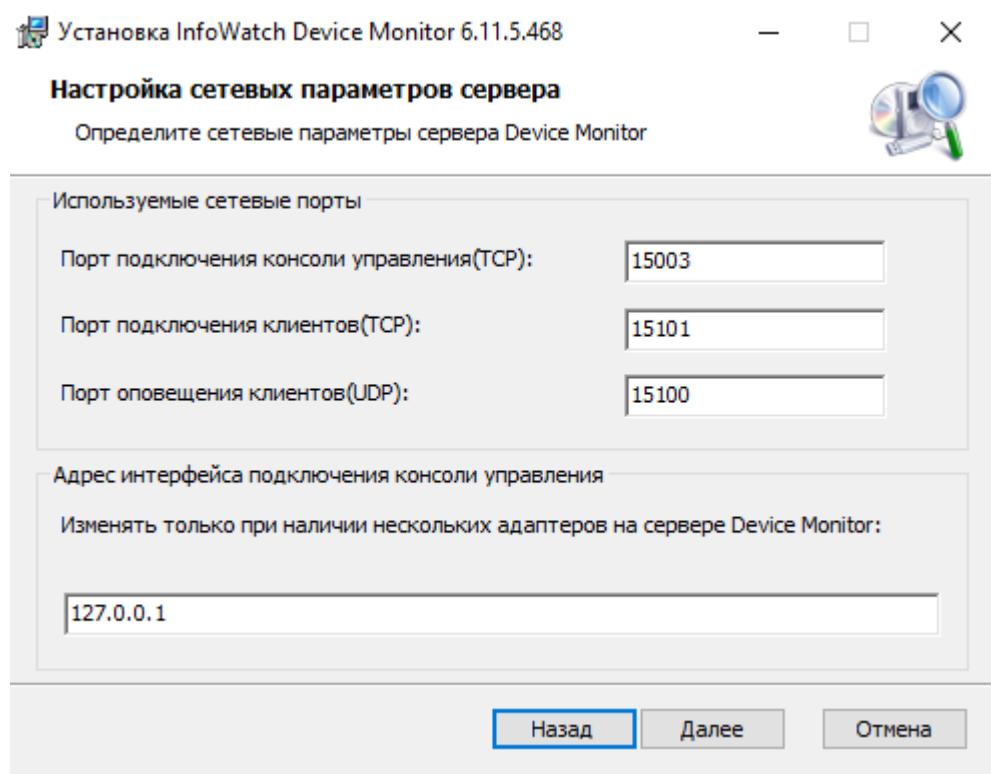
Выбираем базу данных, в нашем случае будет - PostgreSQL



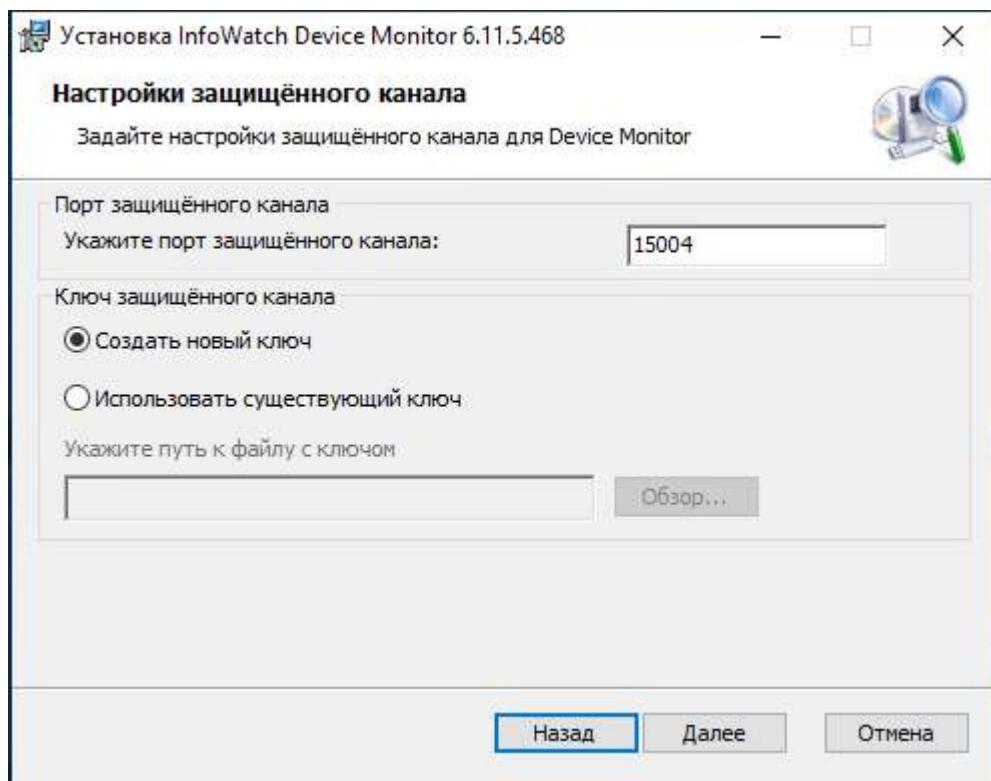
Задаем сервер БД – 127.0.0.1; Имя БД – dm_database, имя пользователя – postgres и стандартный пароль



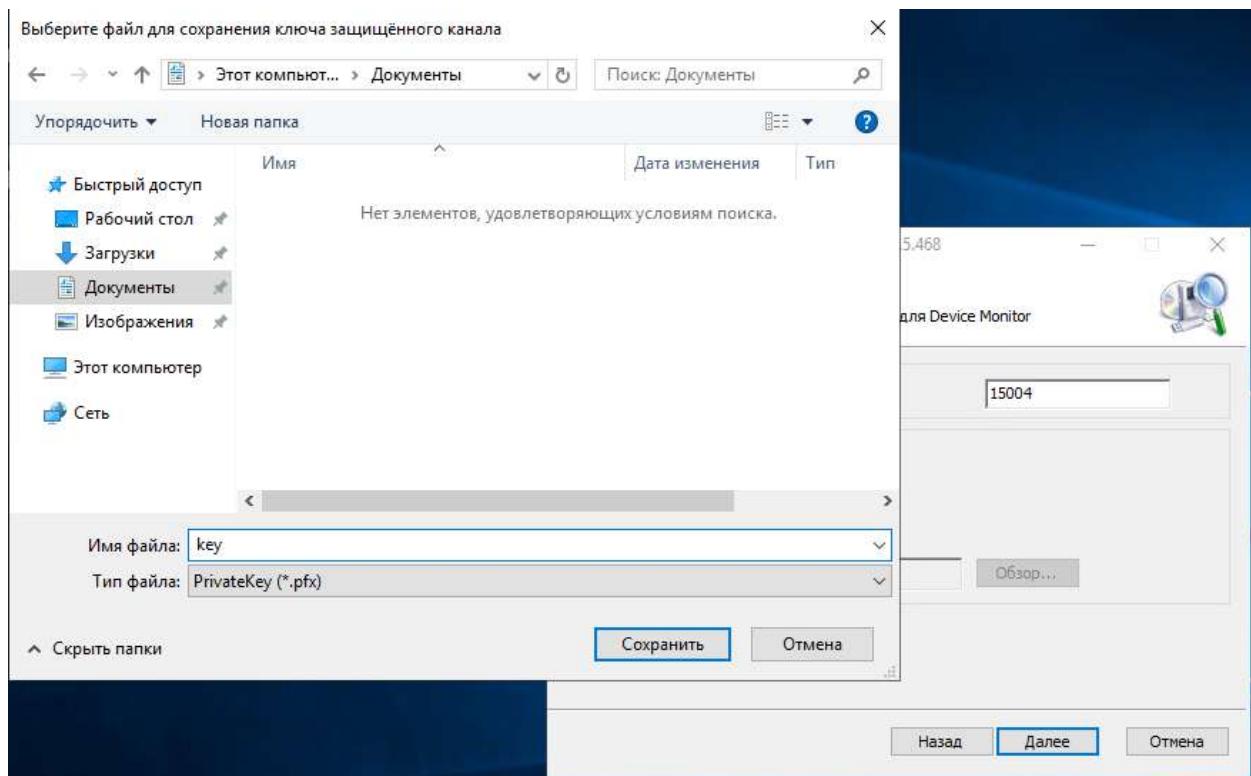
Настраиваем сетевые параметры



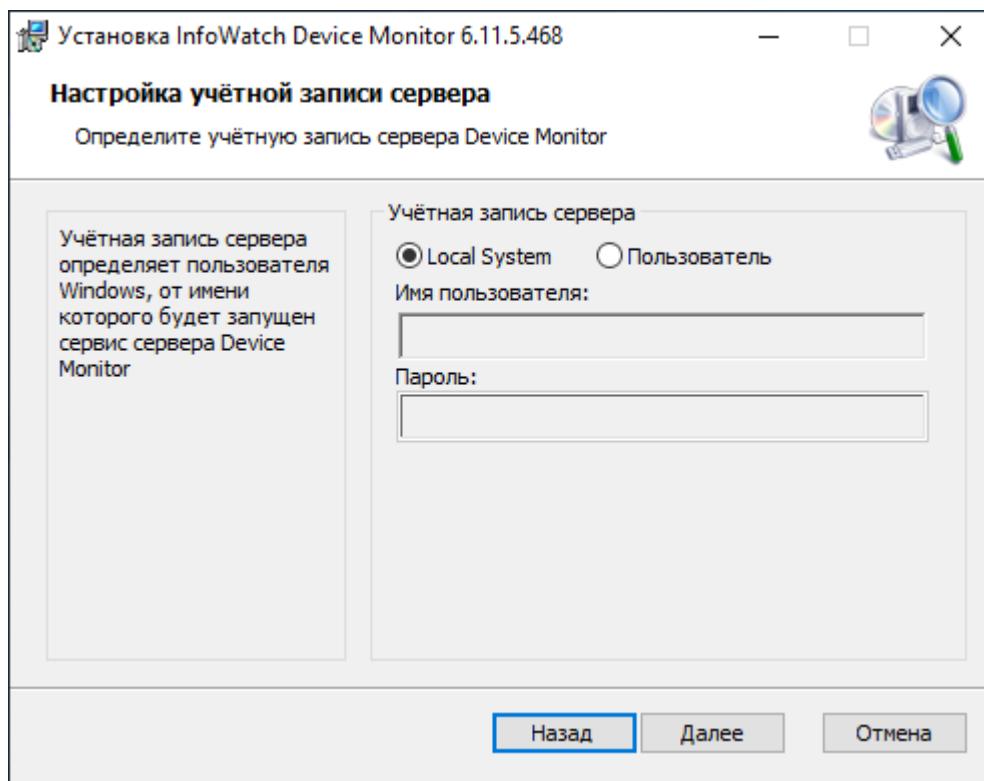
Настраиваем защищённый канал и создаём новый ключ



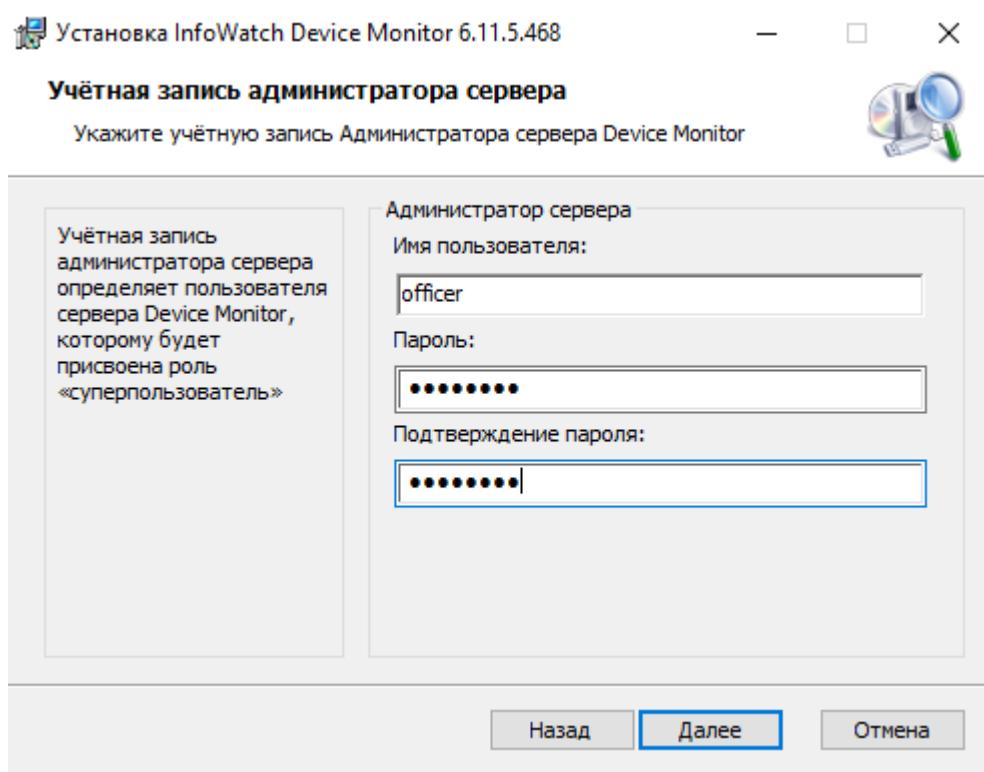
Сохраняем ключ



Оставляем локальную учётную запись



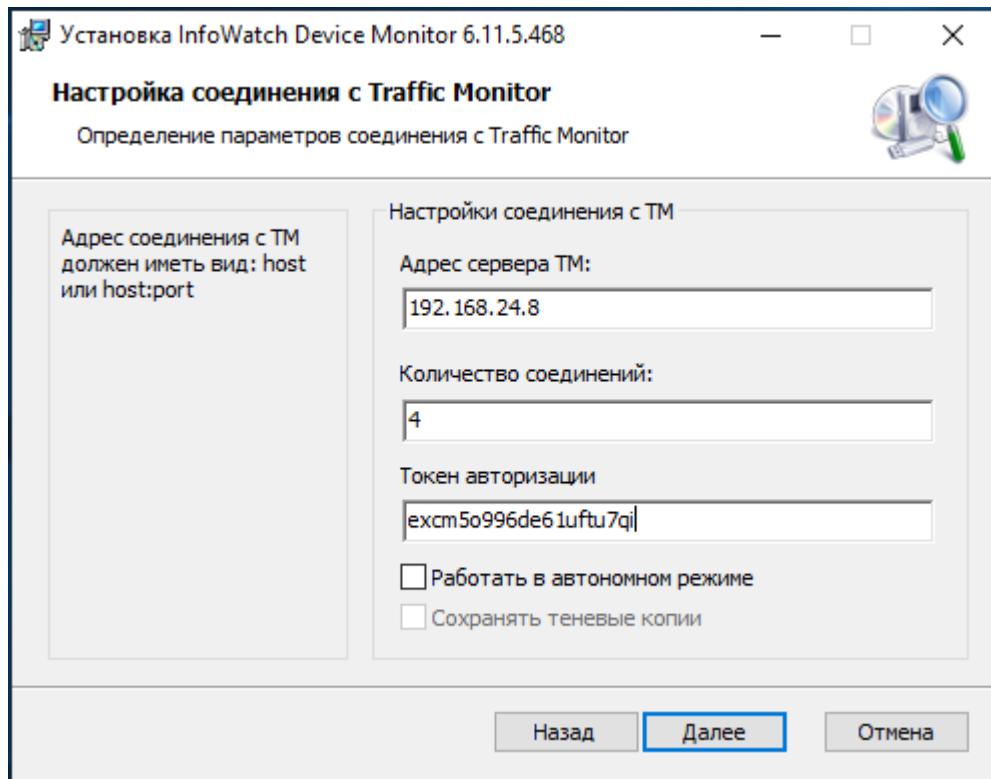
Вводим логин и пароль администратора



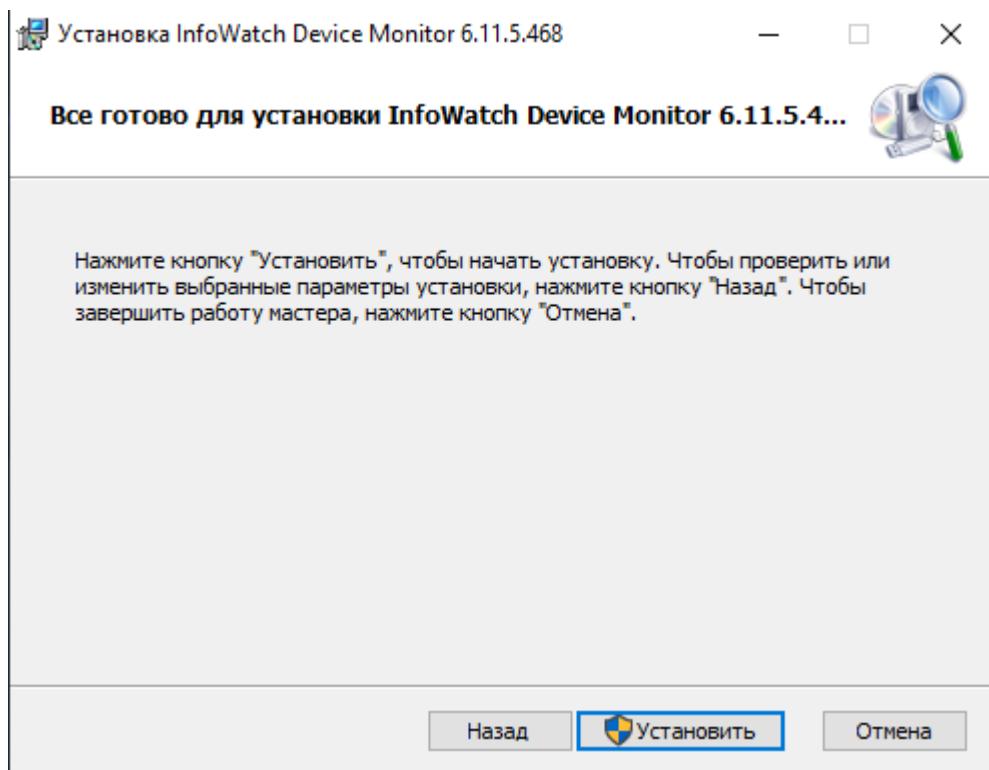
Смотрим токен

The screenshot shows the InfoWatch Traffic Monitor Enterprise application window. In the top navigation bar, there are tabs like Сводка, События, Отчеты, Технологии, Объекты защиты, Персоны, Политики, Списки, Управление, Краулер, and Офицер безопасности. Below the tabs, there's a search bar labeled 'Поиск событий' and a button labeled 'Офицер безопасности'. The main area is titled 'Плагины' (Plugins). It lists several items: InfoWatch Crawler, InfoWatch Device Monitor (selected), and InfoWatch Sample documents Autoupdate. On the right side, there's a detailed view of the selected 'InfoWatch Device Monitor' plugin, showing its name, provider (InfoWatch Device Monitor), version (6.11.5), status (Активный - Active), name (Token-3), content (excm5o996de61uftu7qj), and description.

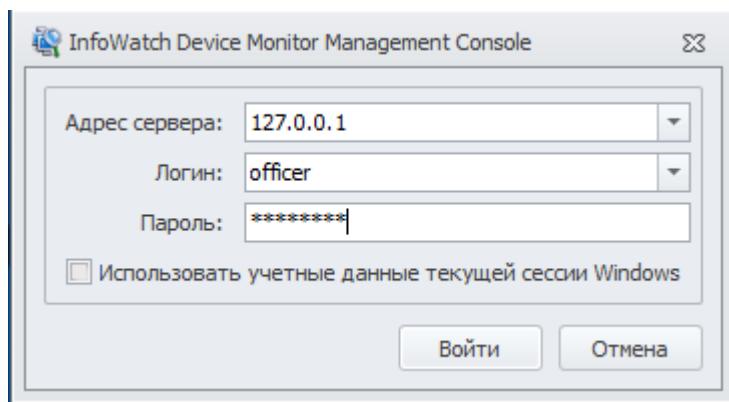
Указываем Ip-адрес IWTM и токен (который только что посмотрели в трафик мониторе)



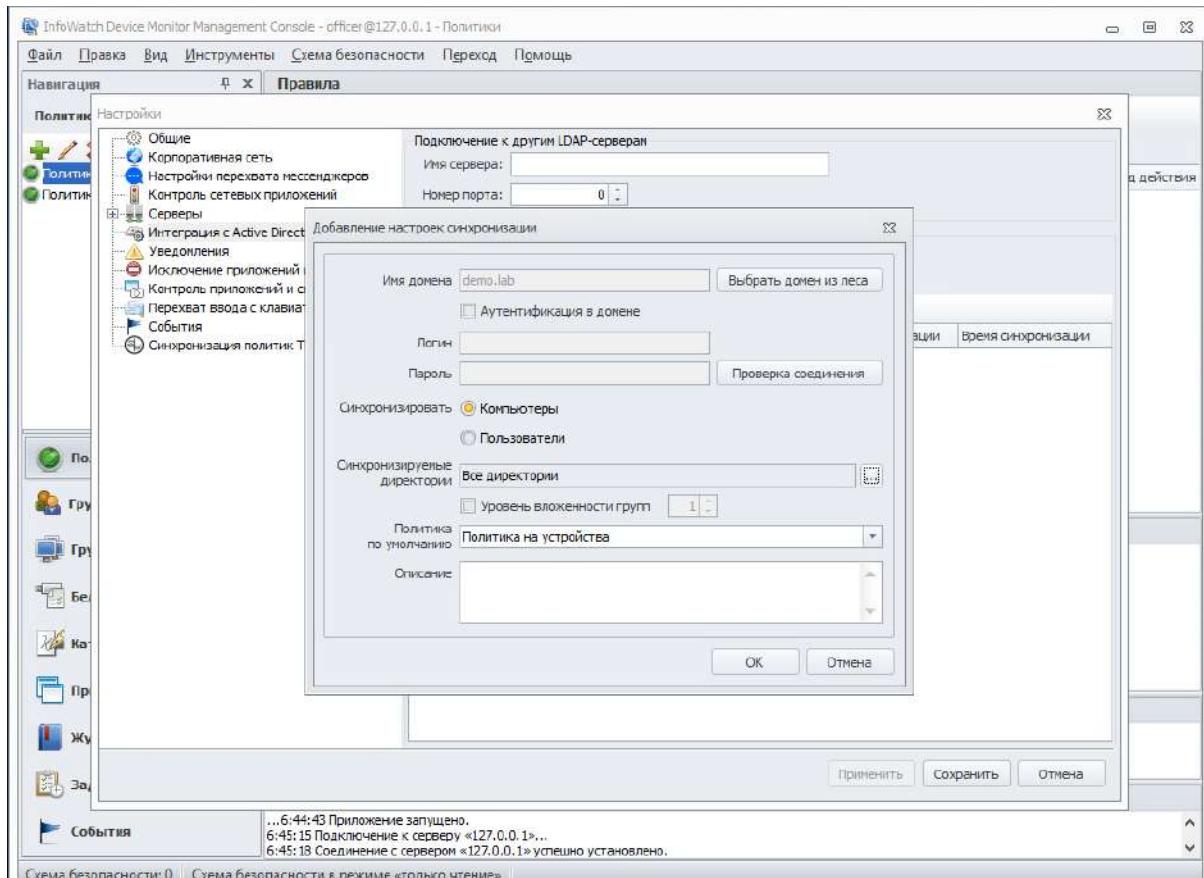
Устанавливаем



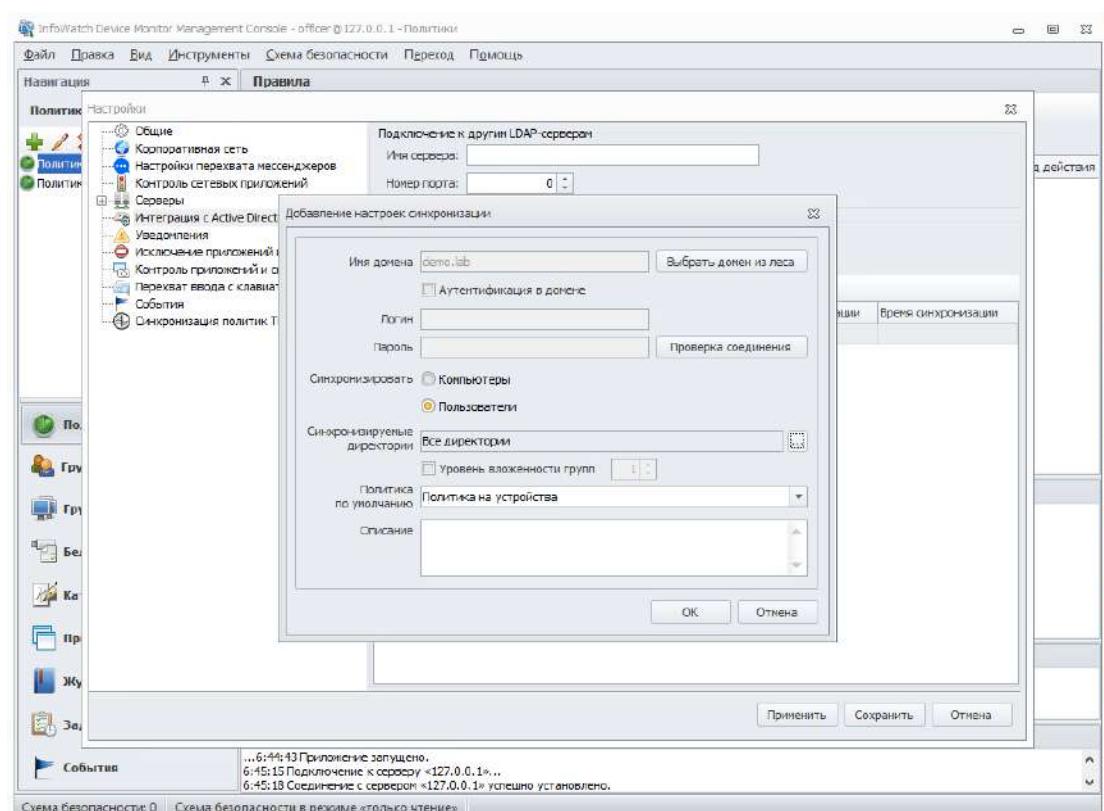
Подключаемся к InfoWatch Device Monitor Management Console



Синхронизуем компьютеры

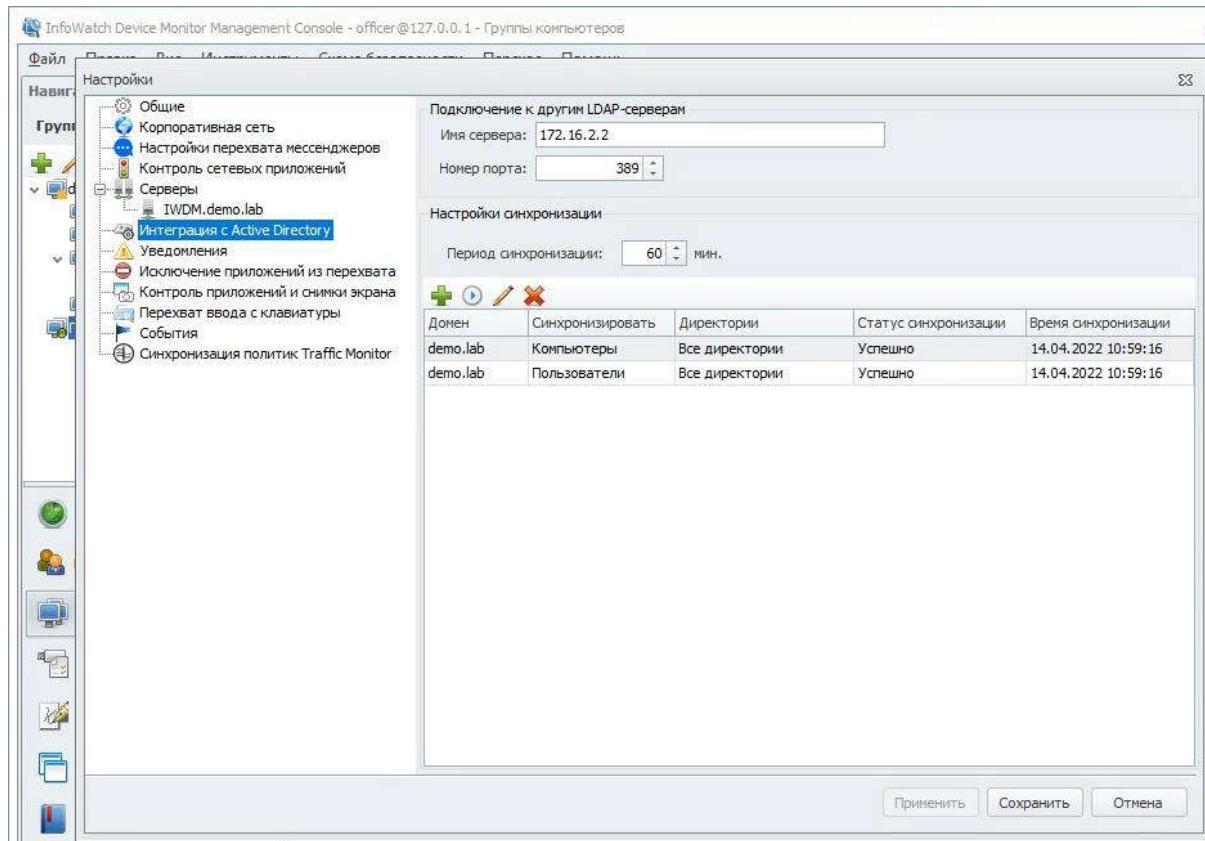


Синхронизуем пользователей



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

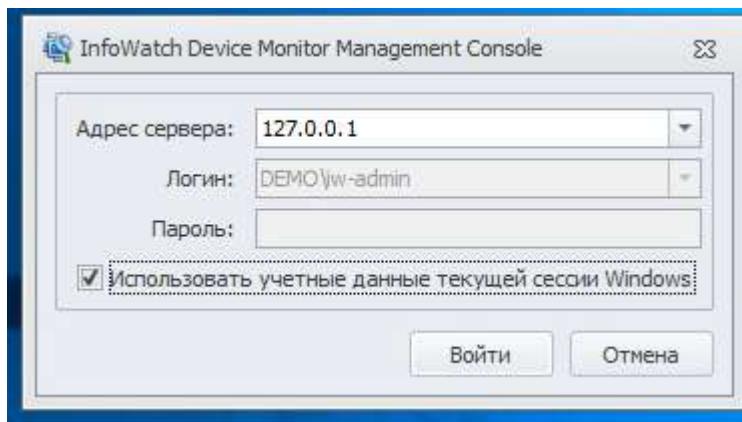
Офицер безопасности	Выбрать
Администратор	Удалить

Сохранить **Отмена**

Пользователи консоли

Пользователи консоли		Роли		
Показать записи: Все				
Пользователи:				
Статус	Логин	Группы	Полное имя	Добавить из AD Создать... Изменить... Удалить Заблокировать
●	DEMO\jw-admin	Группа сотрудников по ум...	iw-admin	
●	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

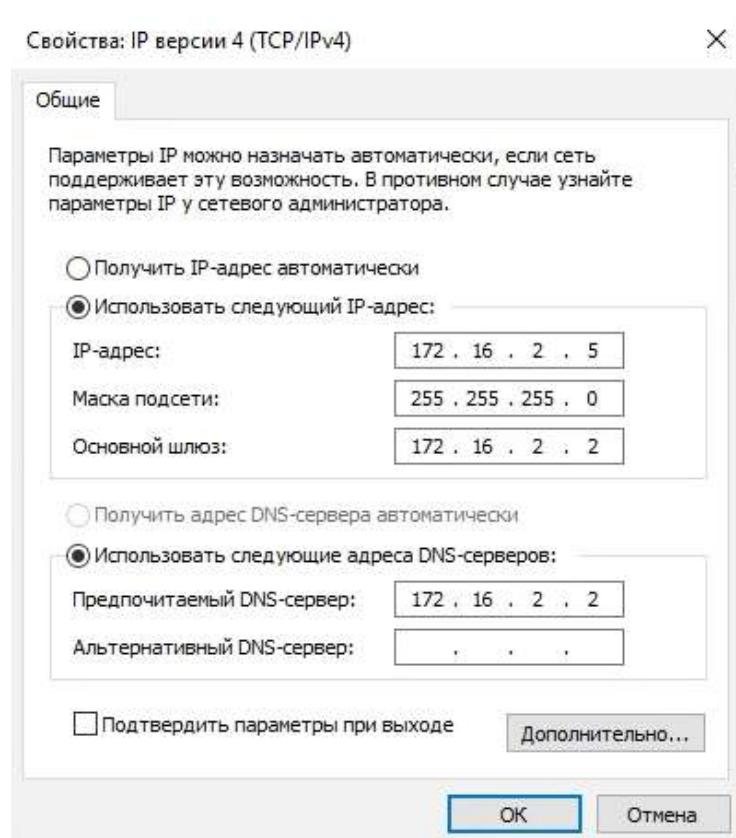
выполнения

политик.

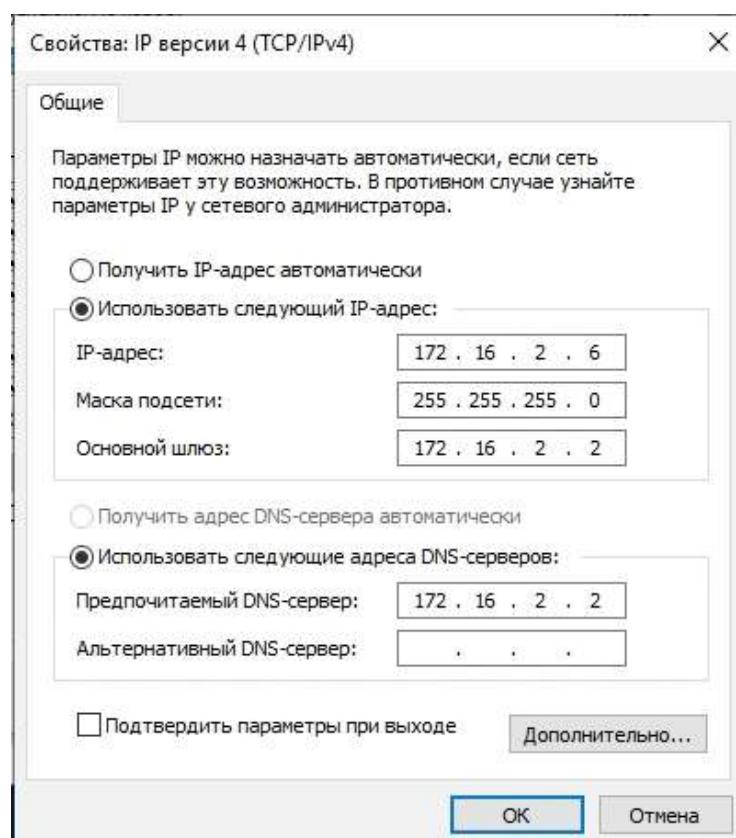
Ручная установка с помощью переноса на машину нарушителя пакета

установки является некорректным выполнением задания

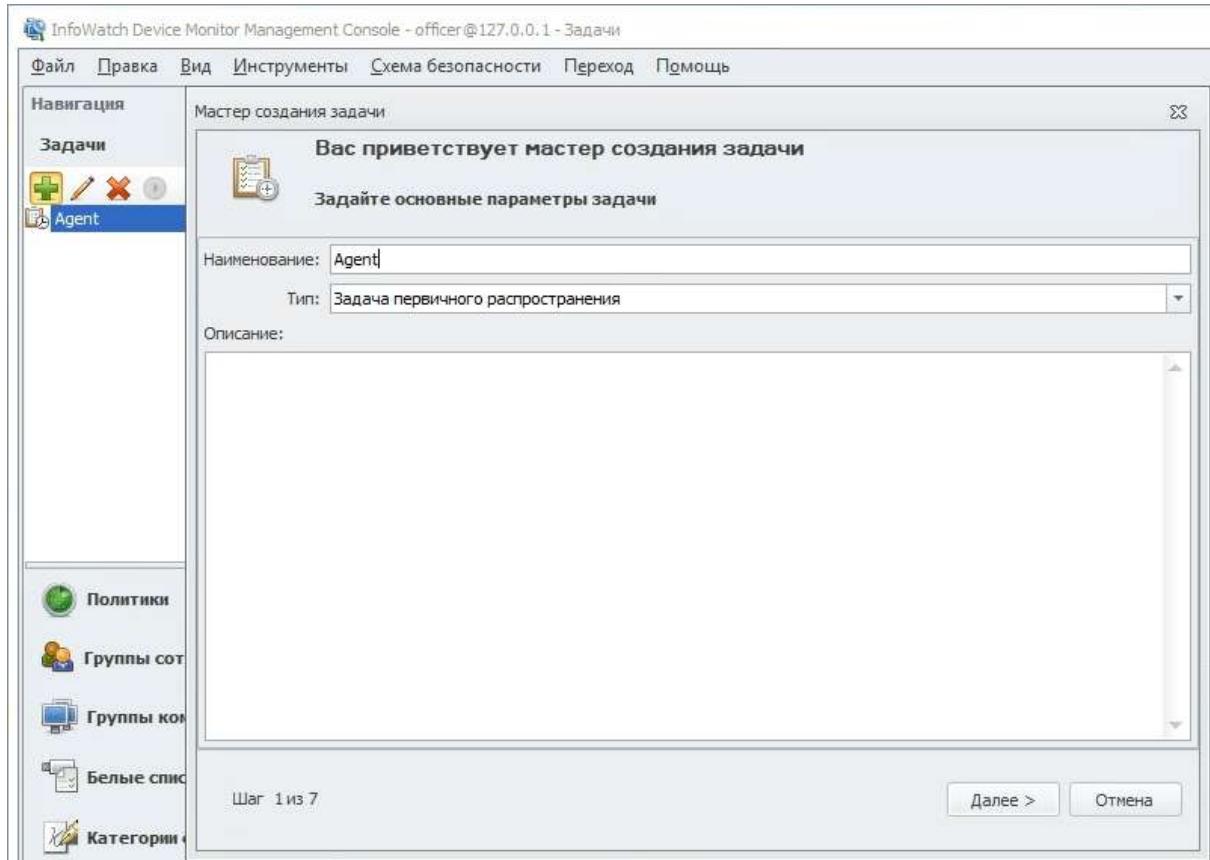
Клиент1



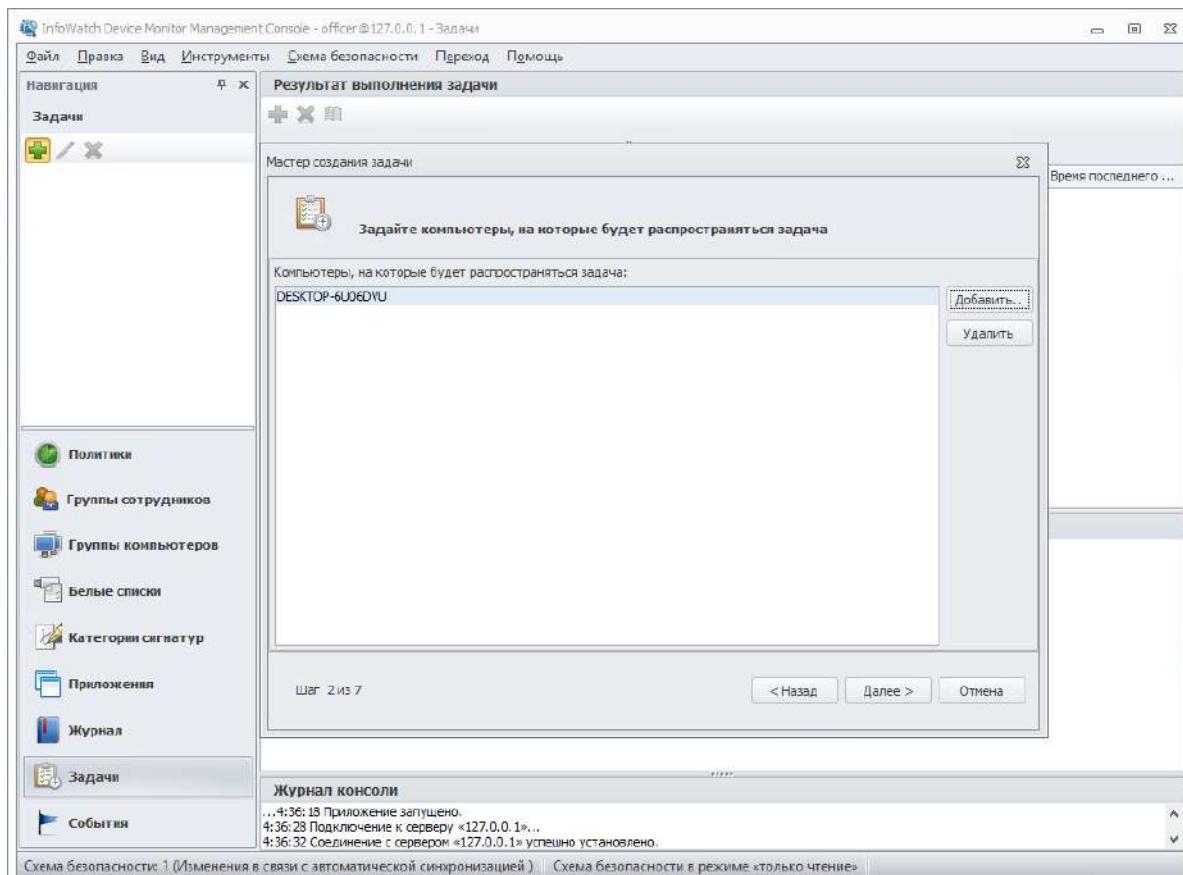
Клиент2



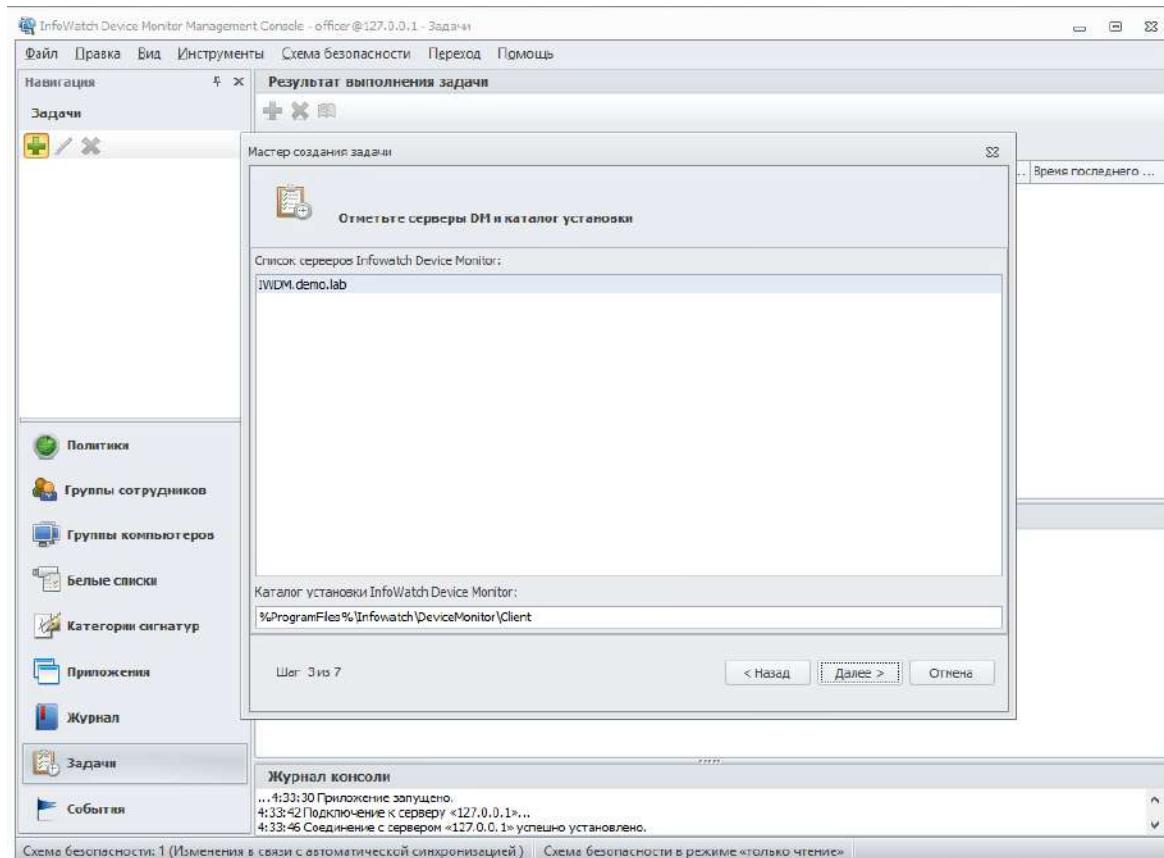
Создаем новую задачу

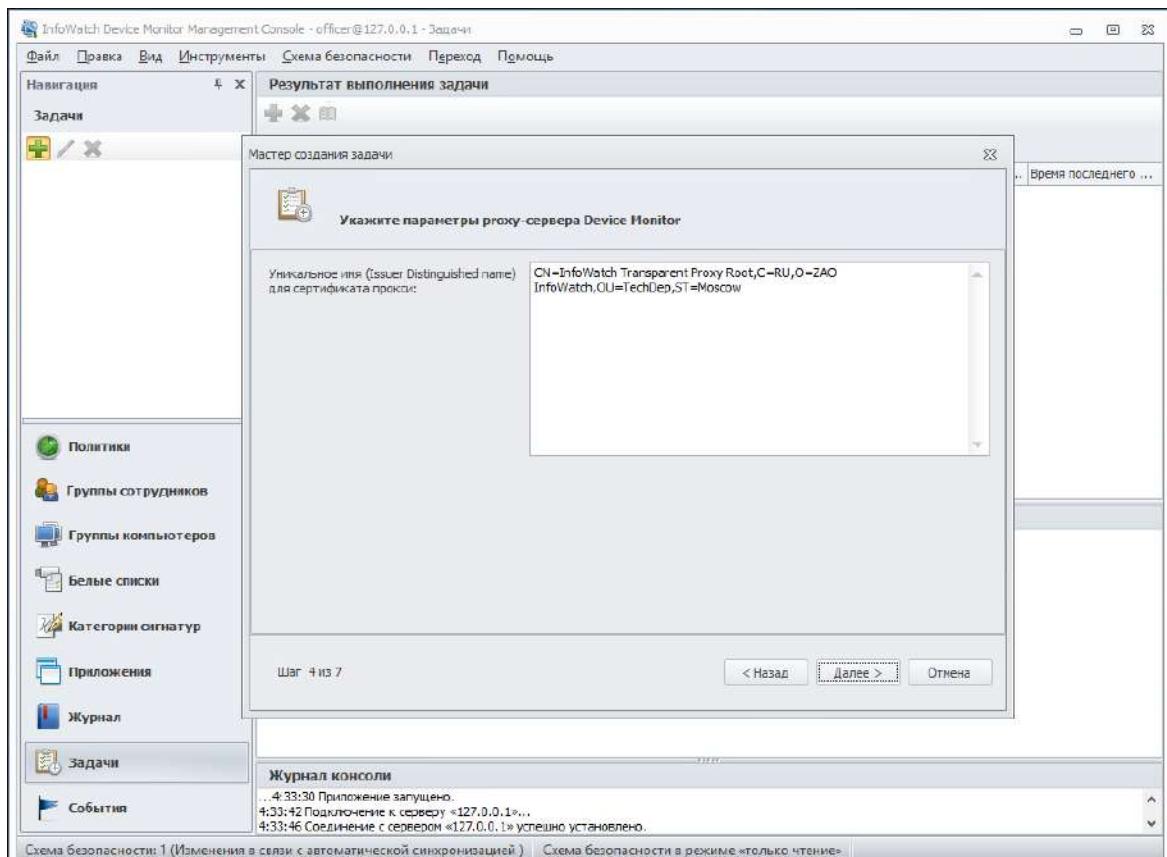


Выбираем компьютер агента

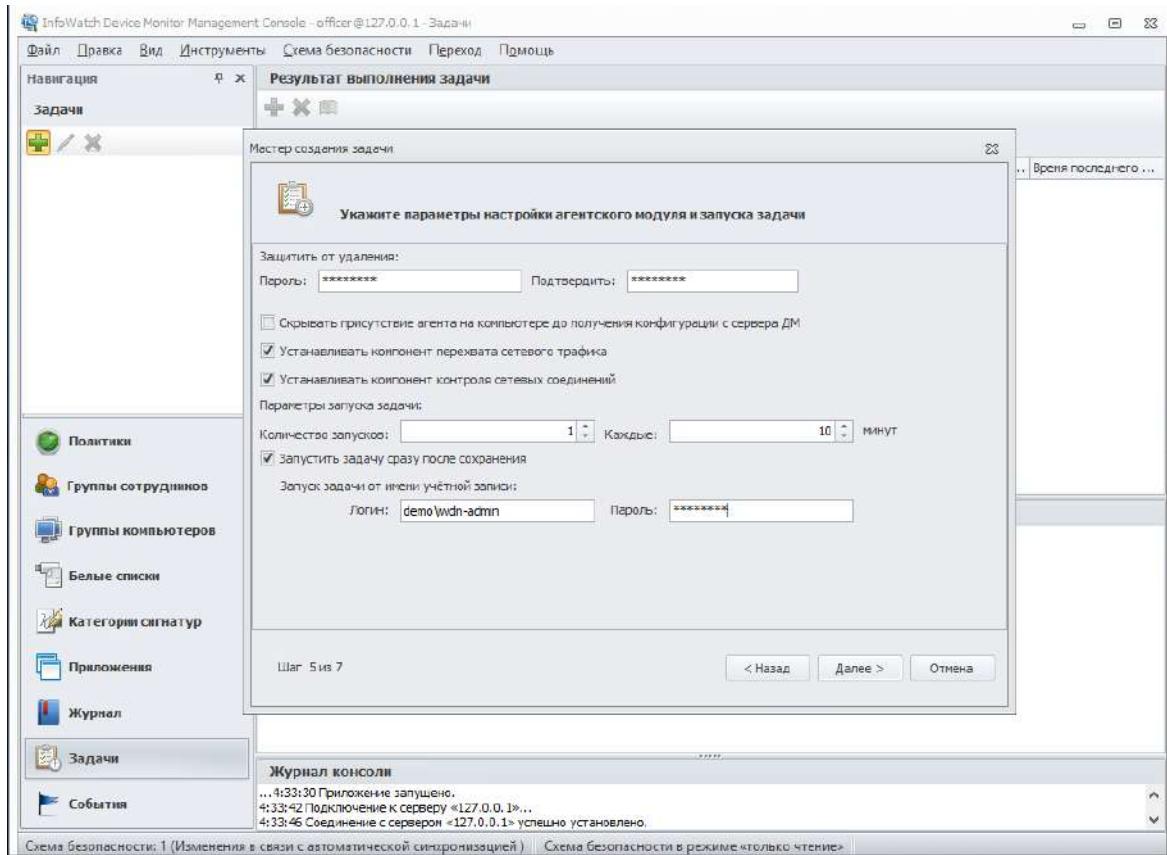


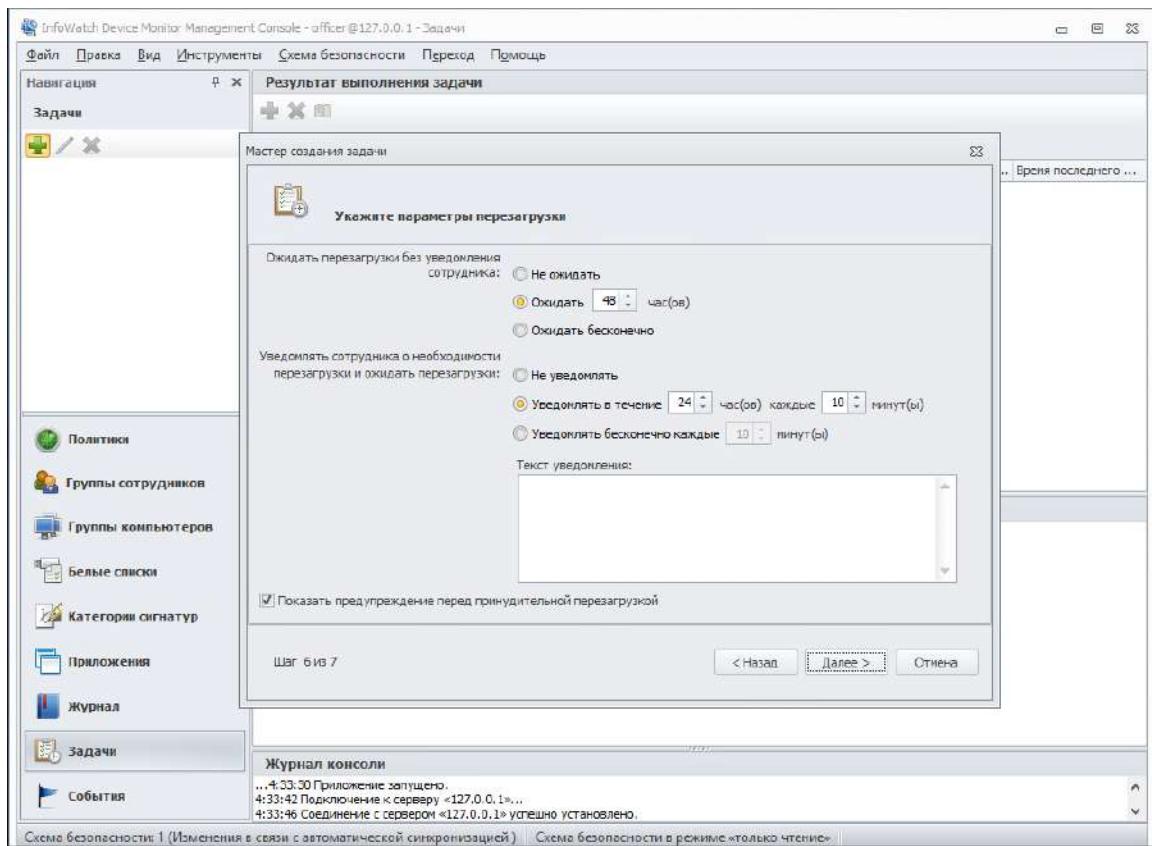
Выбираем наш сервер IWDM



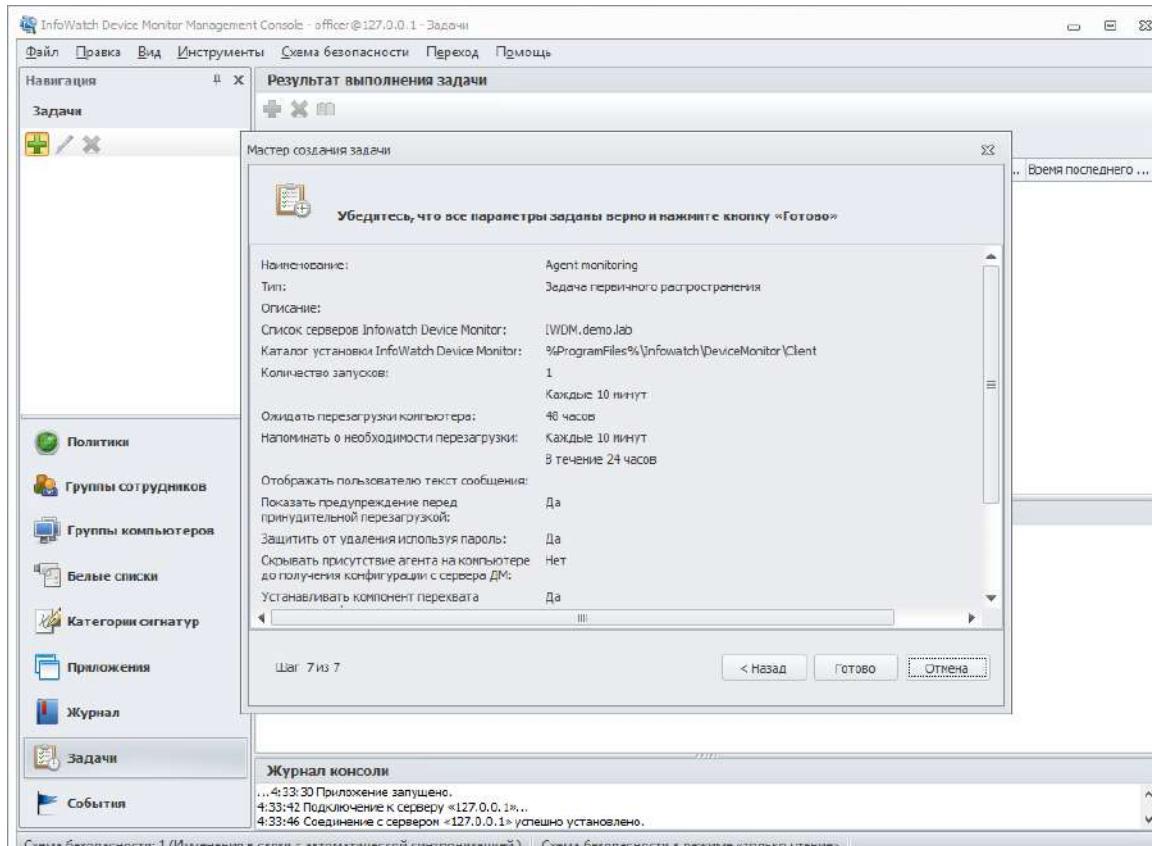


Вводим пароль, и учётную запись от которой будет запускаться задача





Готово



Ожидаем подготовку

The screenshot shows the InfoWatch Device Monitor Management Console interface. The main window displays a table titled 'Результат выполнения задачи' (Task Execution Result) with one row: 'DESKTOP-8U06DVU...' with status 'Подготовка' (Preparation) and timestamp '1 03.12.2021 7:35:08'. The left sidebar lists navigation options: Навигация, Задачи, Политики, Группы сотрудников, Группы компьютеров, Белые списки, Категории сигнатур, Приложения, Журнал, and Задачи. The 'Задачи' section is currently selected, showing a list with 'monitor' highlighted. The bottom right panel, titled 'Подробно' (Detailed), shows the configuration for the 'monitor' task, including fields like Наименование (Name), Описание (Description), Тип (Type), Статус (Status), and various settings for configuration distribution and agent behavior.

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, Дправка, Вид, Инструменты, Схема безопасности, Переход, Помощь. The left sidebar navigation menu includes: Навигация, Задачи, Политики, Группы сотрудников, Группы компьютеров, Белые списки, Категории сигнатур, Приложения, Журнал, and Задачи (selected). The central area displays a table titled "Результат выполнения задачи" (Task execution result) with one row: Имя: DESKTOP-6U06DVU..., Статус выполнен...: В процессе (In progress), Версия агента: Windows 10, Операционная сис...: x64, Разрядность опер...: 64-bit, Количество подкл...: 1, Время последнего ...: 1 03.12.2021 7:36:01. Below this is a detailed view titled "Подробно" (Detailed) for the task "monitor". The "Задача" section contains the following configuration:

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

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

Компьютер агента ожидает перезагрузки

InfoWatch Device Monitor Management Console - office@127.0.0.1 - Задачи

Файл Правка Вид Инструменты Схема безопасности Переход Помощь

Навигация

Задачи

+ X

monitor

Поместите сюда заголовок колонки для группировки по этой колонке

Имя	Статус выполнения задачи	Версия агента	Операционная с...	Разрядность оп...	Количество под...	Время последнего...
DESKTOP-6J06DVU...	Ожидание перезагрузки		Windows 10	x64		1 03.12.2021 7:39:01

Политики

Группы сотрудников

Группы компьютеров

Белые списки

Категории сигнатур

Приложения

Журнал

Задачи

Результат выполнения задачи

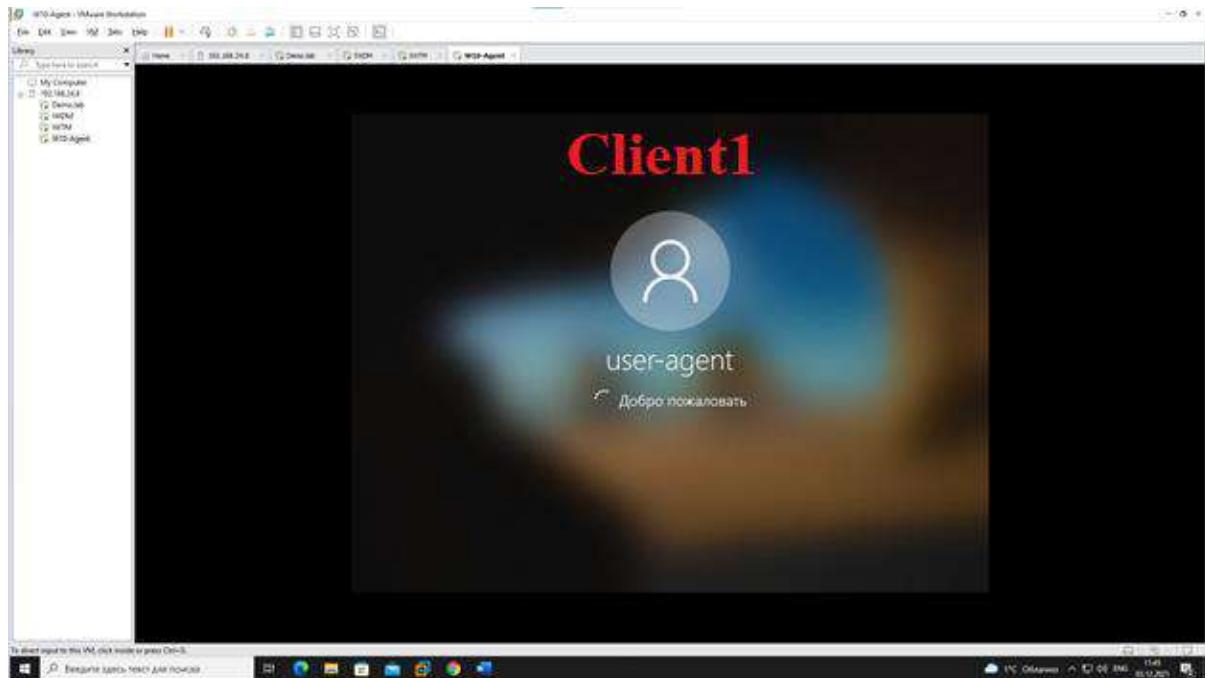
Подробно

Задача	
Назначение	monitor
Описание	
Тип	Первичное распространение
Статус	Выполняется
Период повторного запуска, мин	10
Количество попыток повторного запуска	1
Выдавать 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.

The left sidebar navigation pane contains links: Навигация, Задачи, Политики, Группы сотрудников, Группы компьютеров, Белые списки, Категории сигнатур, Приложения, Журнал, Задачи (selected), and События.

The central area displays the "Результат выполнения задачи" (Task Execution Result) table:

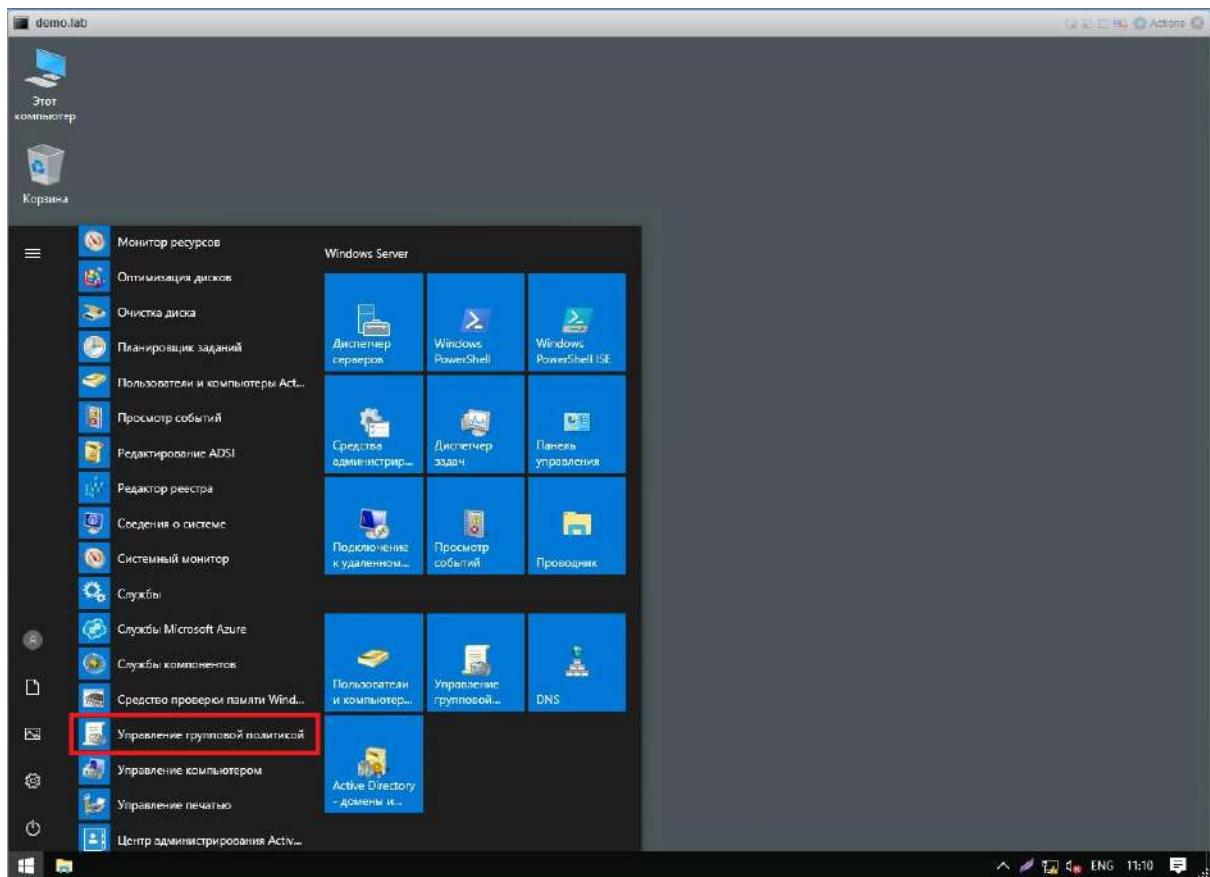
Имя	Статус выполнения задачи	Версия агента	Операционная с...	Разрядность оп...	Количество под...	Время последнего...
DESKTOP-6U06DVU...	Выполнено	6.11.5.468	Windows 10	x64	1	03.12.2021 7:47:05

Below the table, there is a "Подробно" (Detailed) section showing task configuration details:

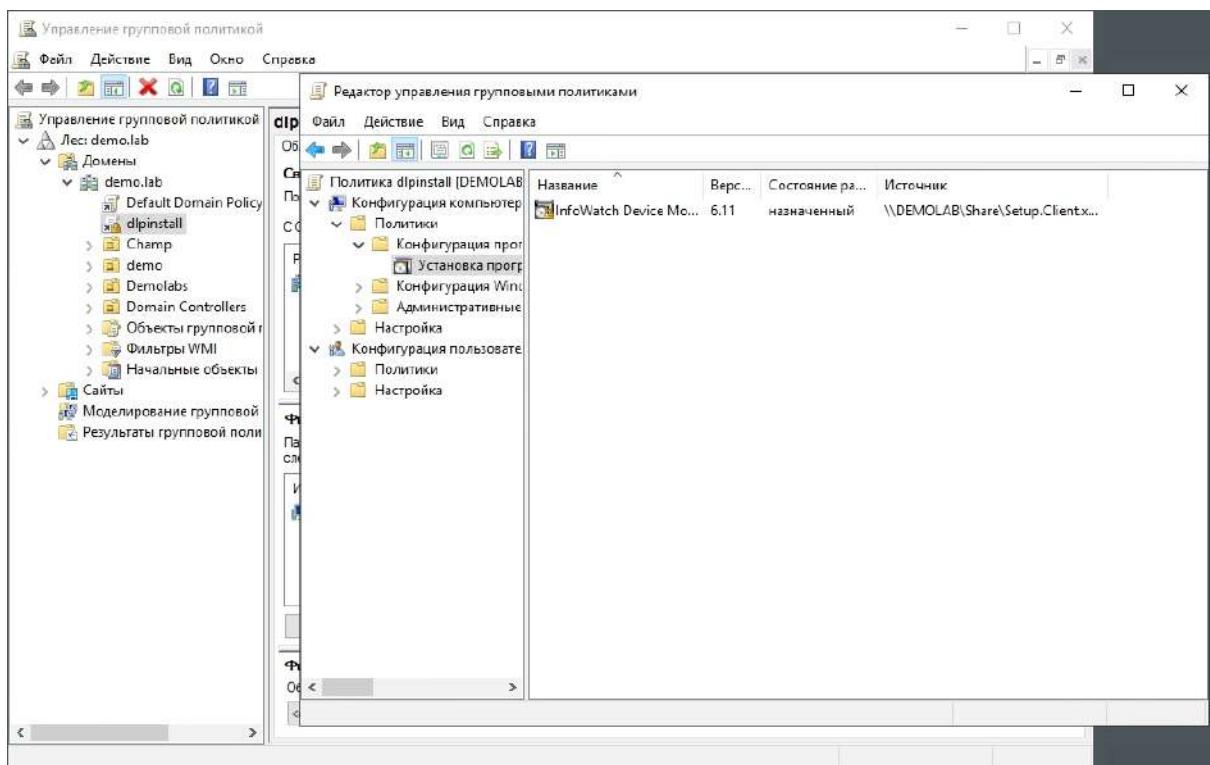
Задача	monitor
Название задачи	monitor
Описание	
Тип	Первичное распространение
Статус	Выполнена. Для каждого компьютера проверьте статус в поле "Статус..."
Период повторного запуска, мин	10
Количество попыток повторного запуска	1
Выдавать сотруднику уведомления о работе Device Monitor Client	Да
Скрывать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

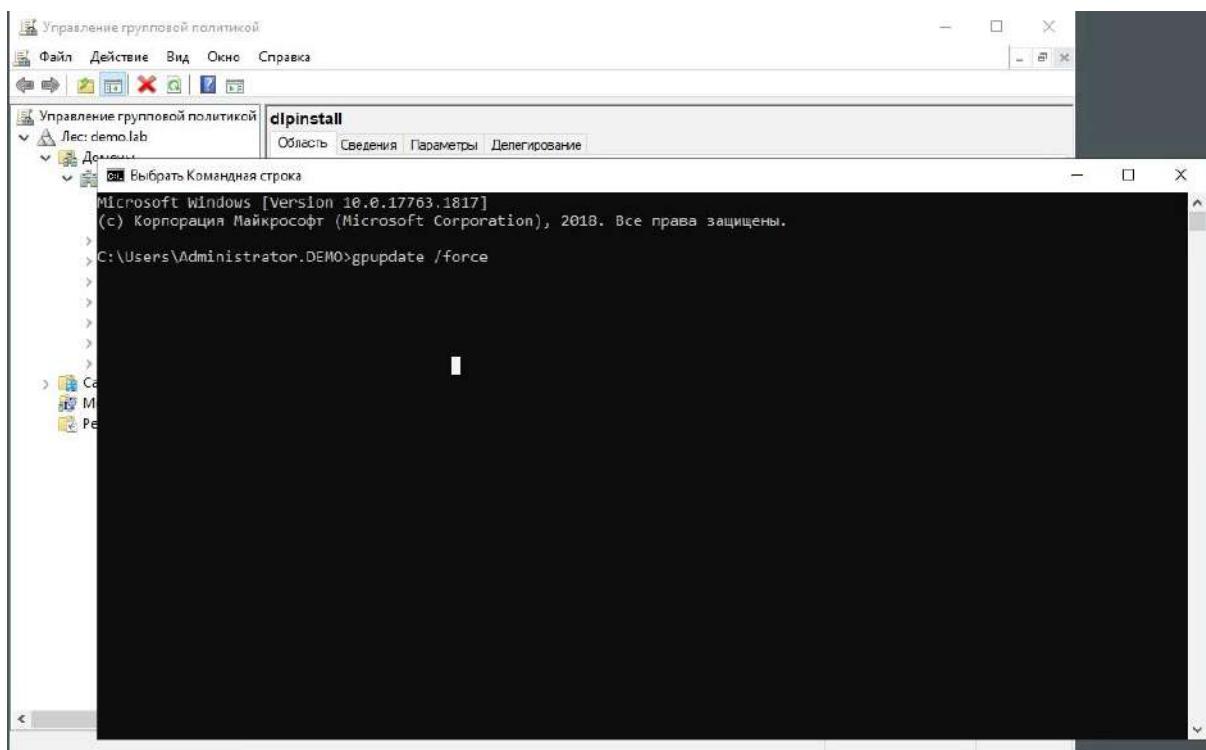
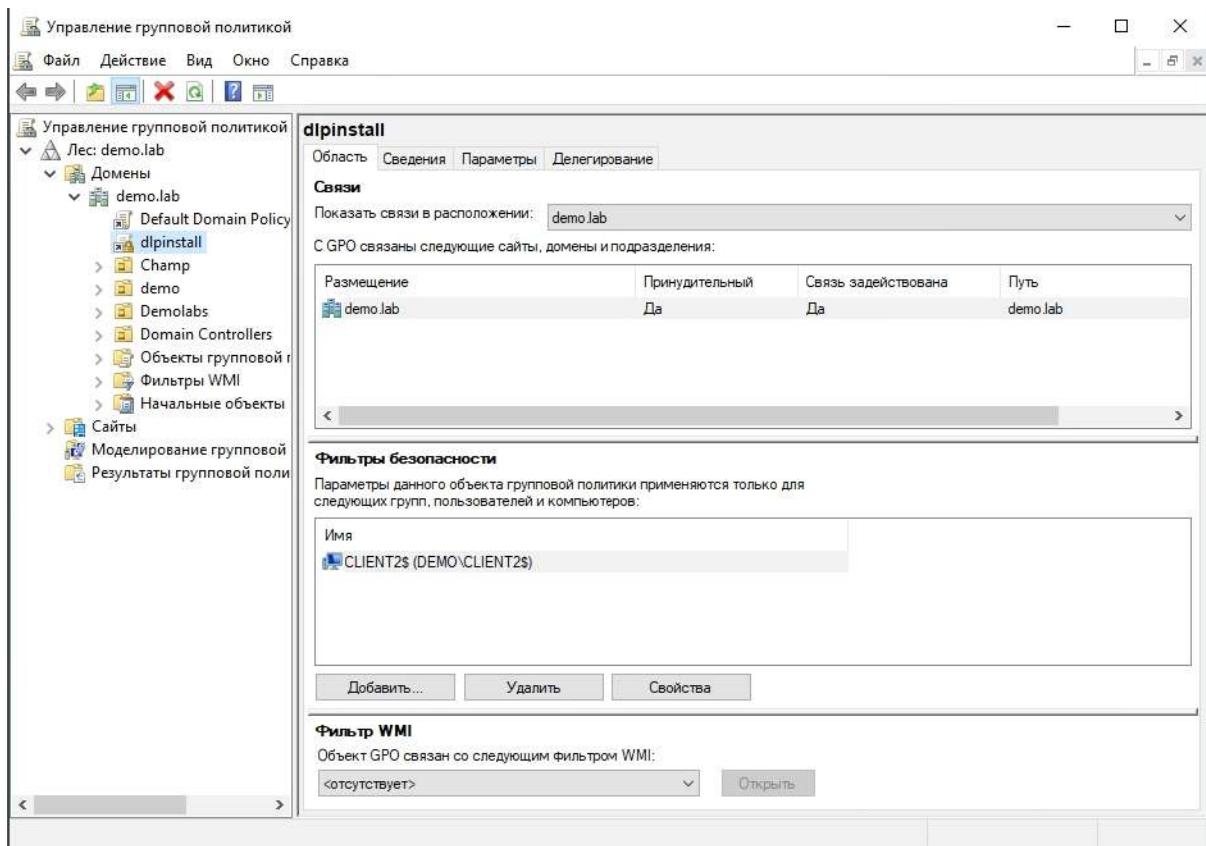
At the bottom, the "Журнал консоли" (Console Log) shows the following log entries:

```
...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





После этого перезапускаем компьютер – Клиент2

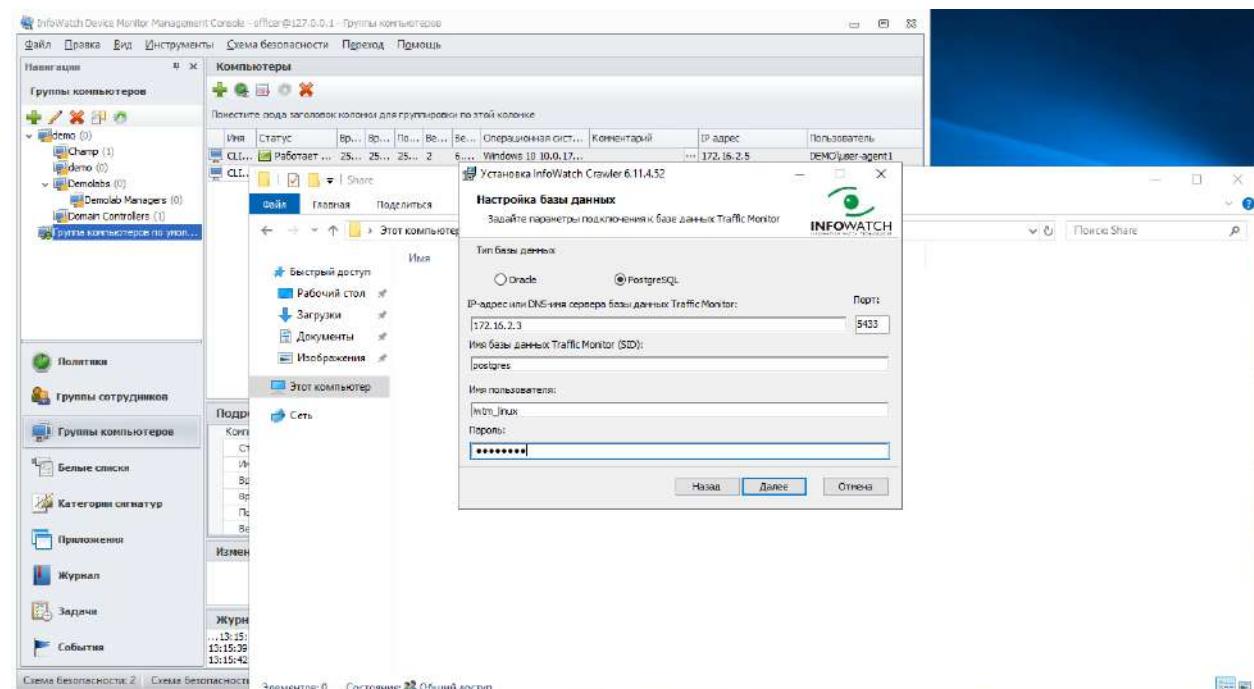
Задание 5: Установка и настройка подсистемы сканирования сетевых ресурсов.

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).

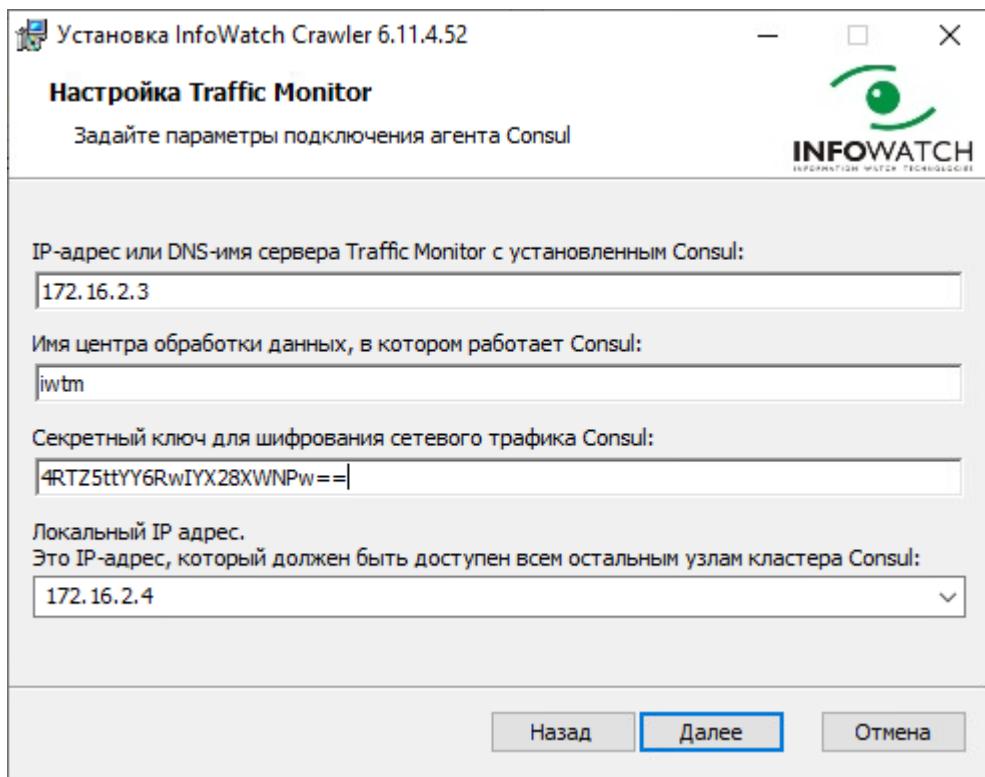
Скринов создание общей папки – нет!



```
}[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]#
```

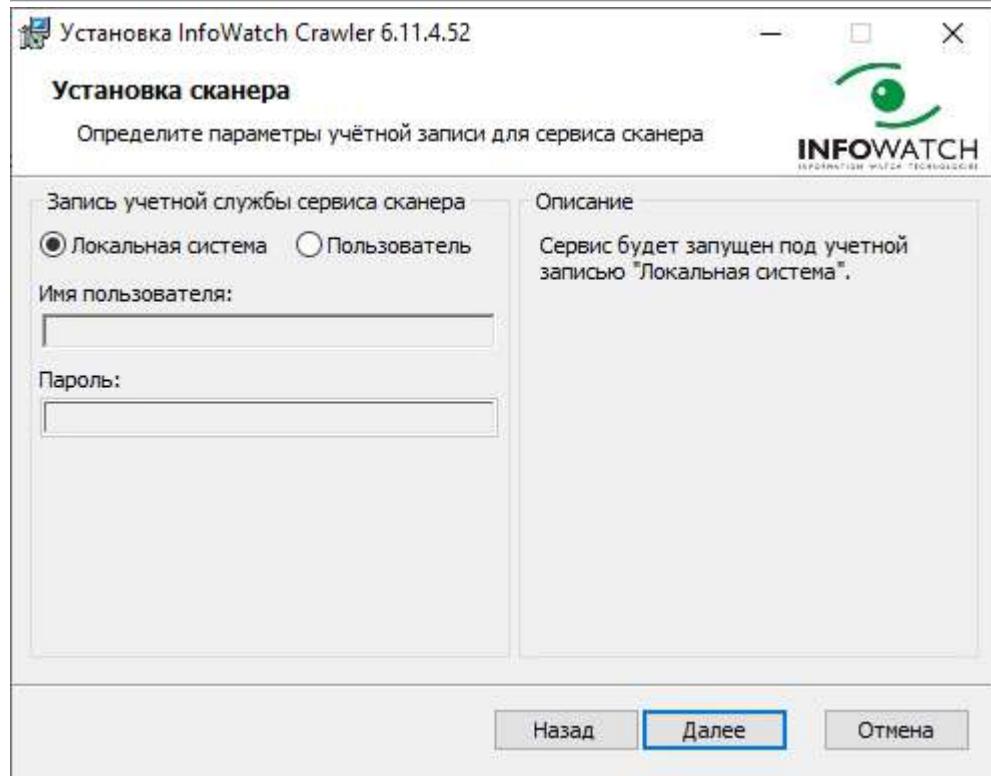
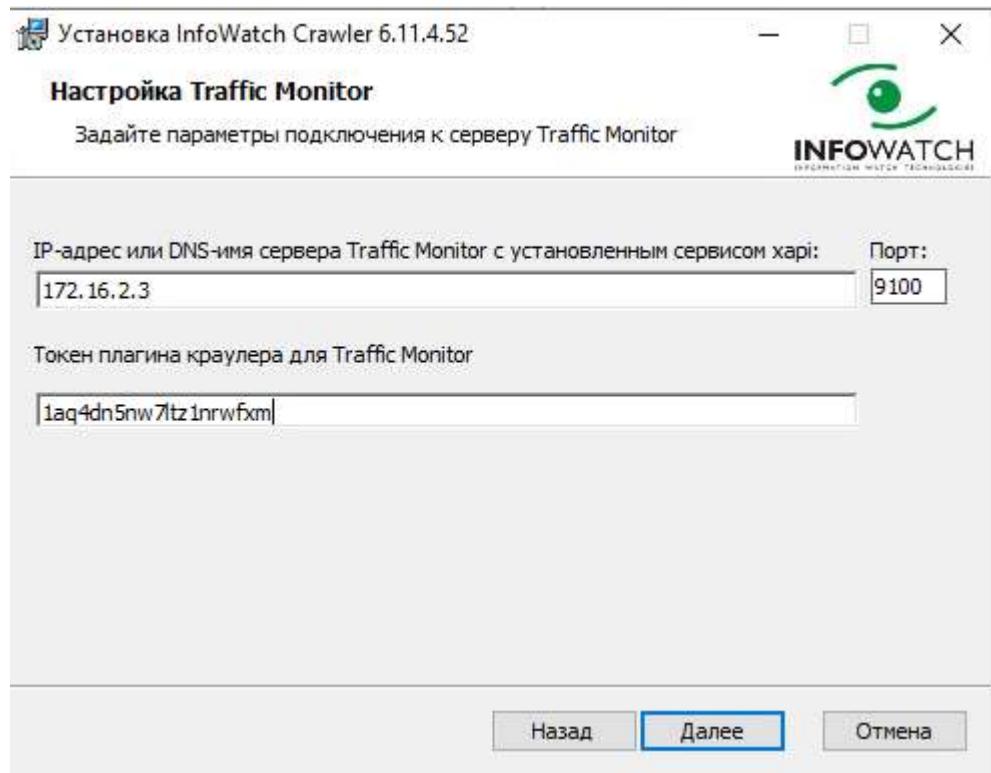


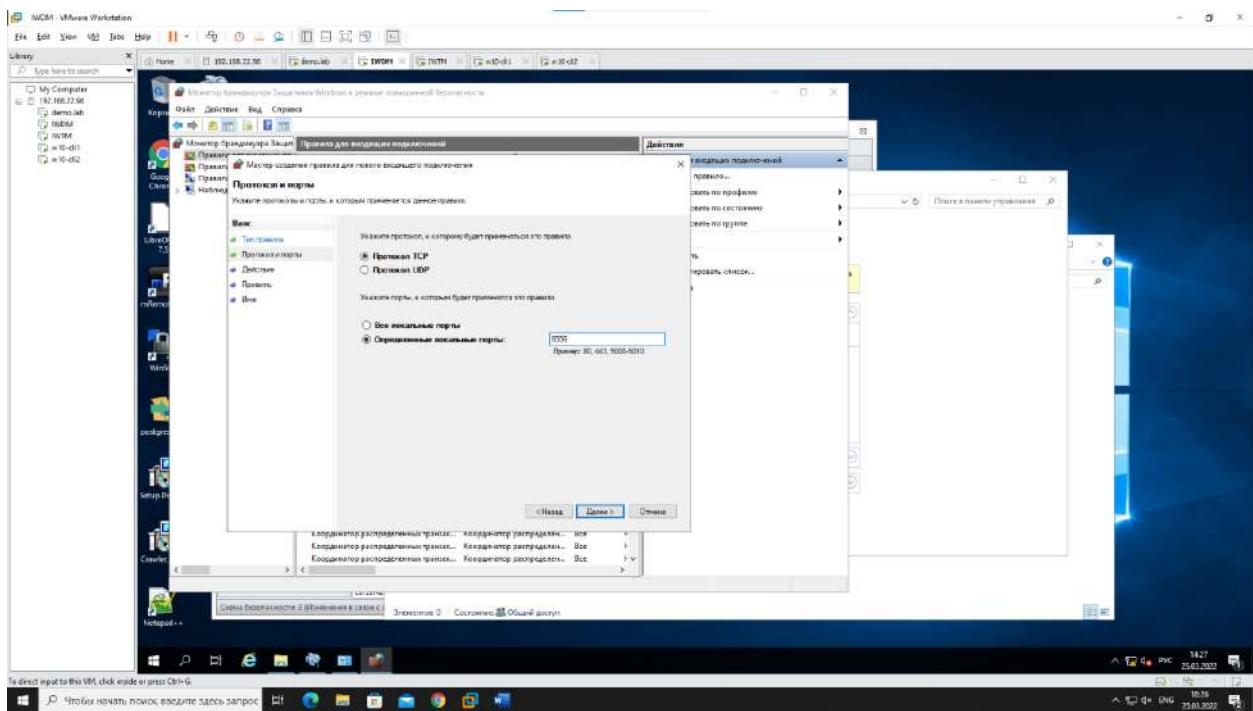
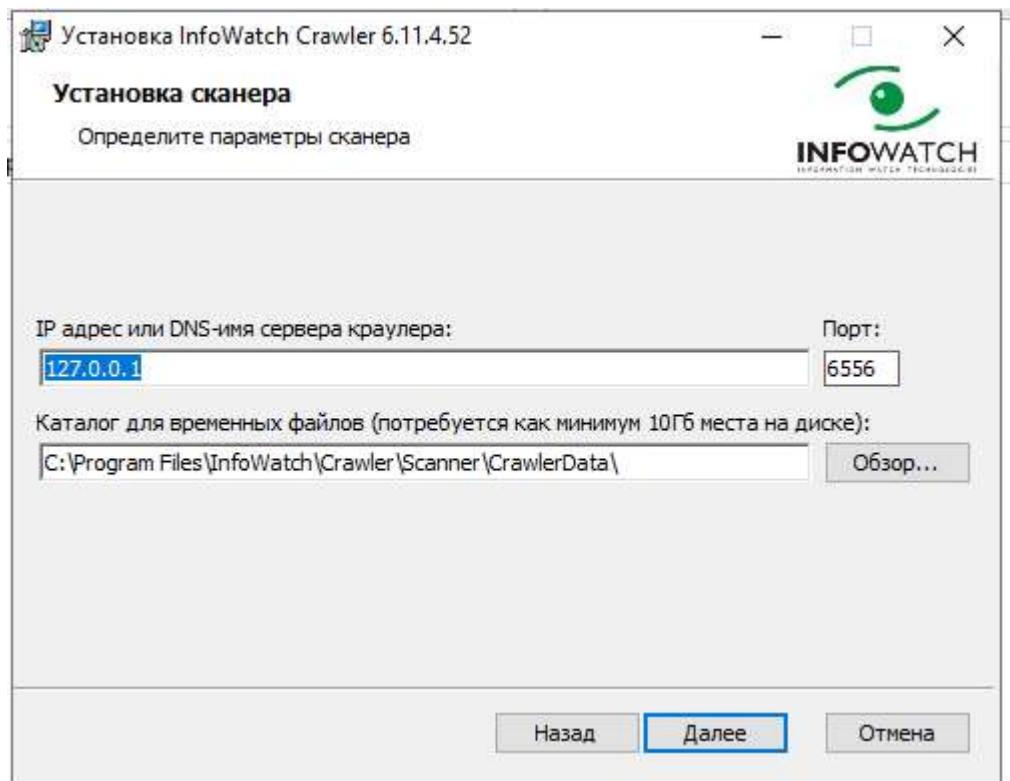
Плагины	InfoWatch Crawler	
+ ×	Прием событий Краулер Производитель: IW Версия 6.11.5	
InfoWatch Crawler		
InfoWatch Device Monitor		
InfoWatch Sample documents Autoupda...		
	Плагины Лицензии Токены	
	+ × × ×	
	Статус Имя Содержание Описание	
	Активный Token-2 Tag4dn5nw7ltz1nrwfxm	
Статус	Имя	Содержание
Активный	Token-2	Tag4dn5nw7ltz1nrwfxm

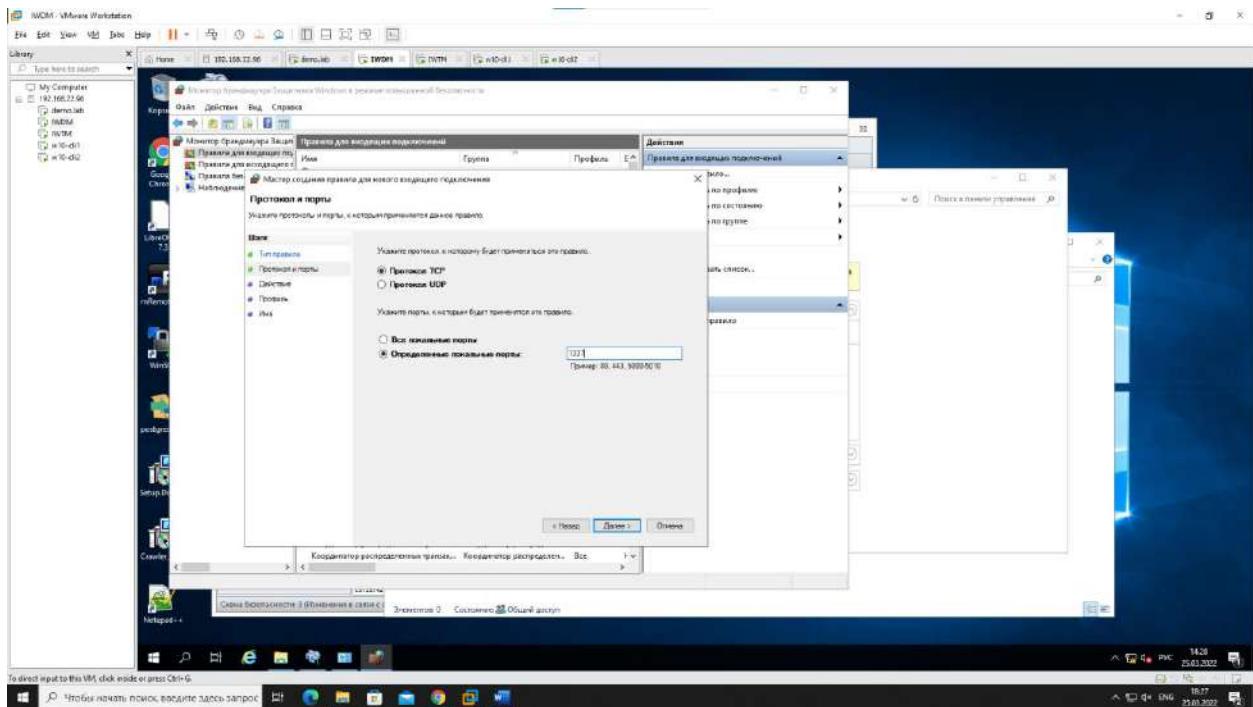
```
[root@iwtm etc]# cd /opt/iw/tm5/etc
```

```
[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.

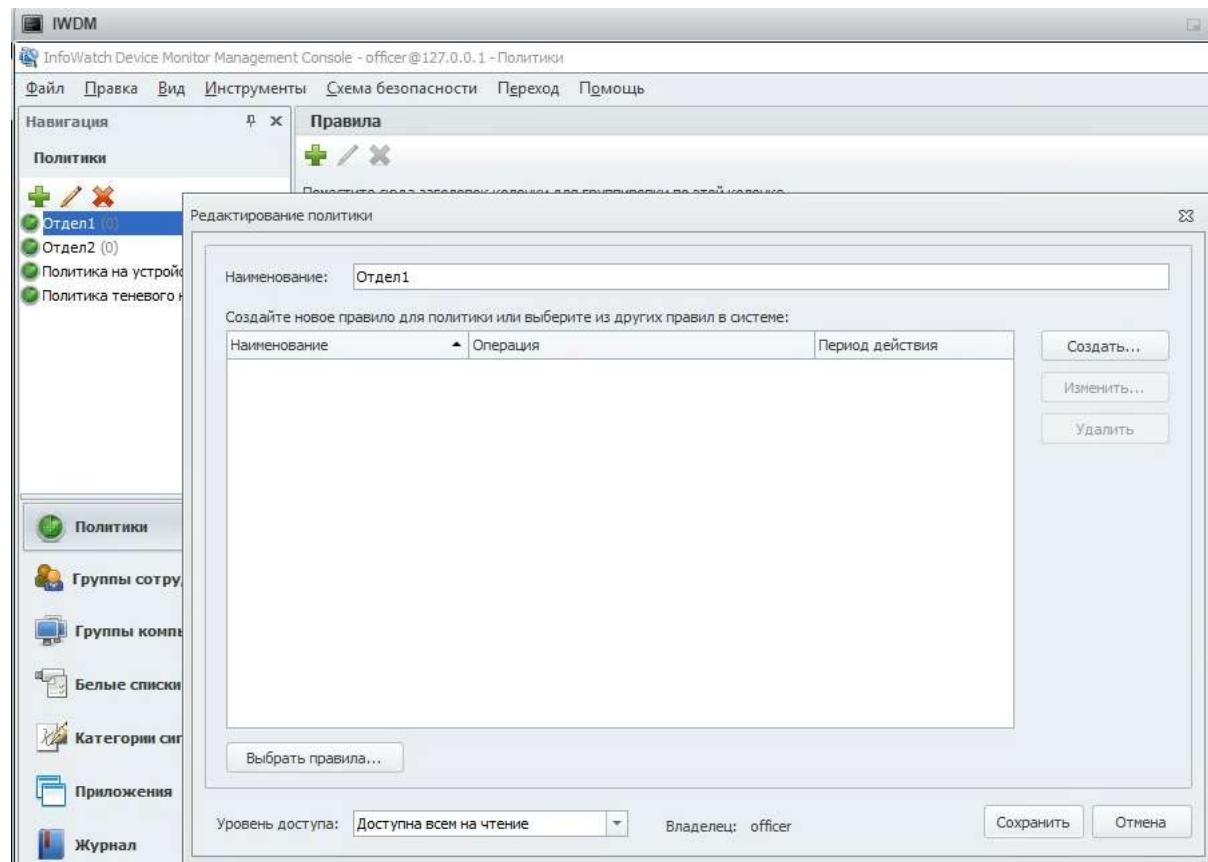
Не делал!

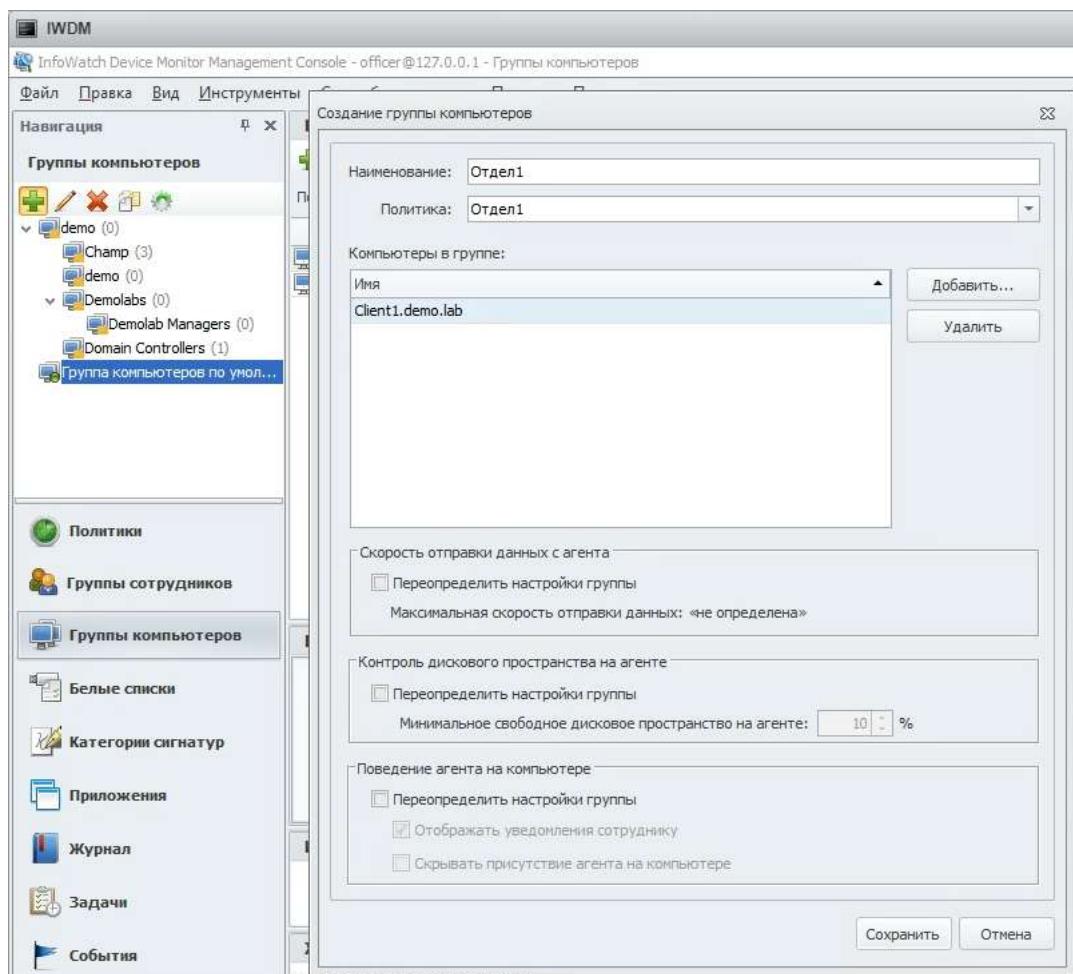
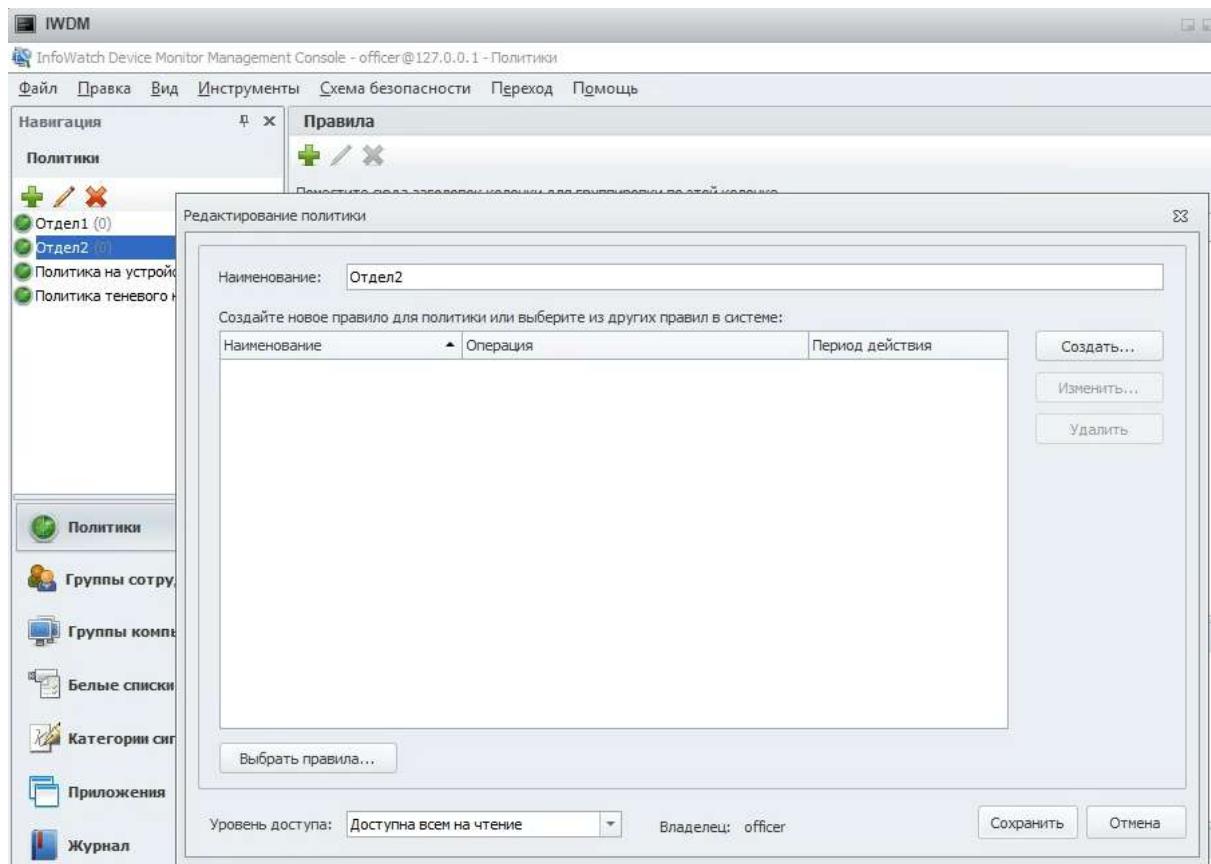
Модуль 2.

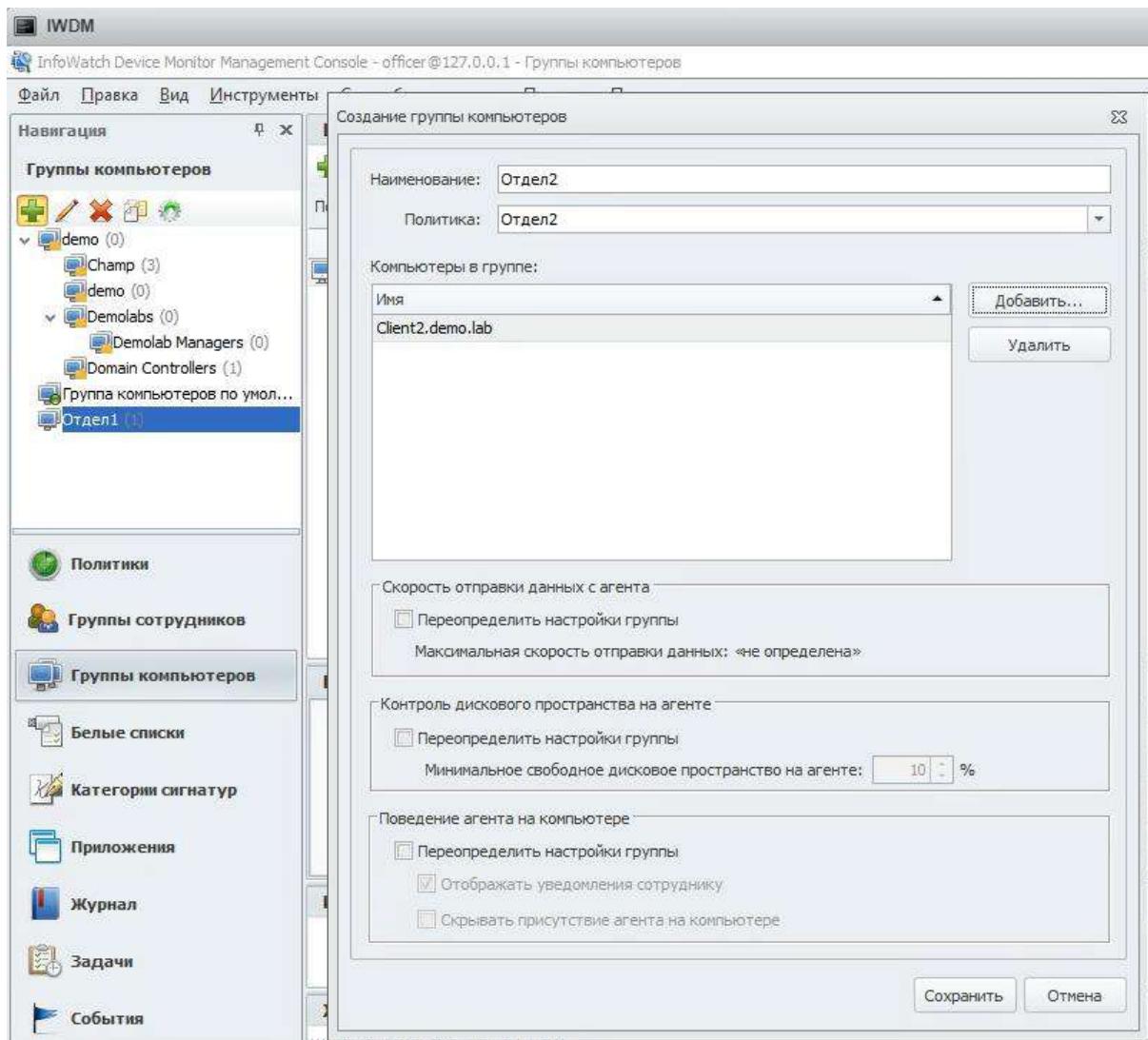
Задание 1

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.



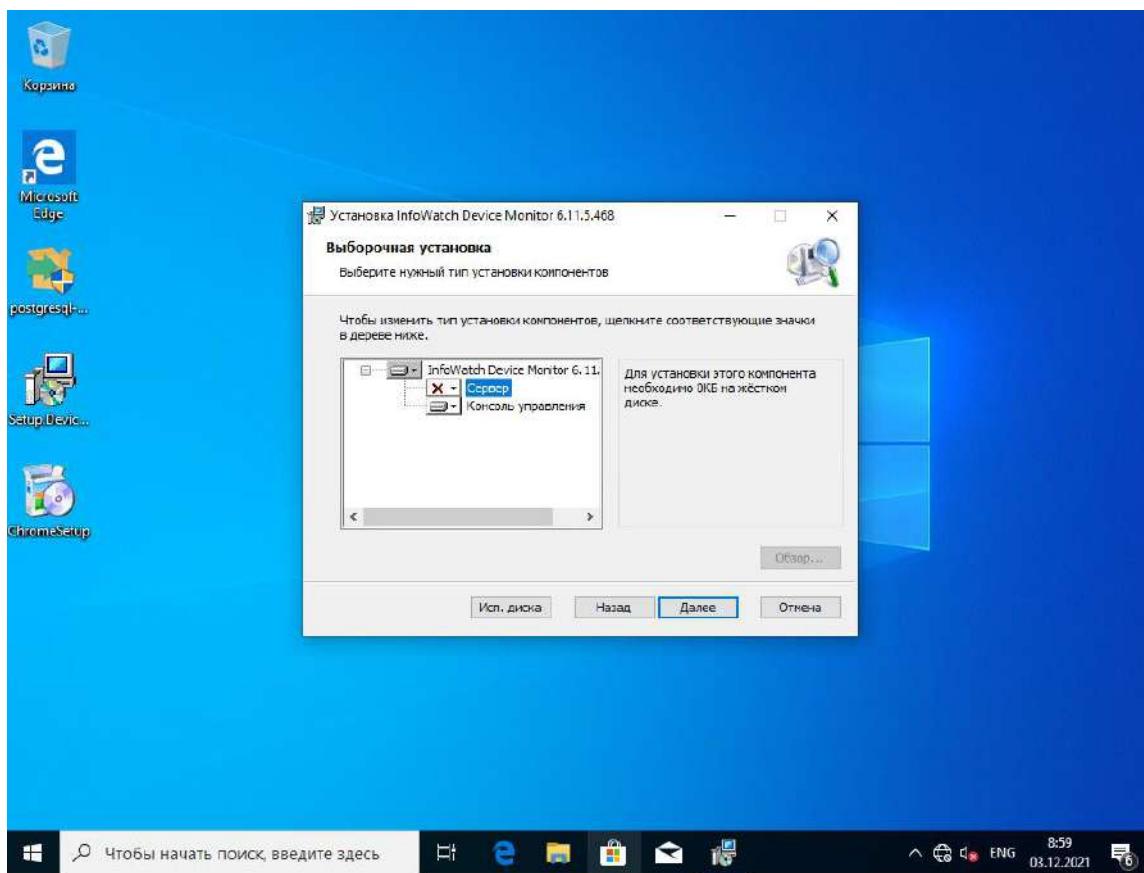




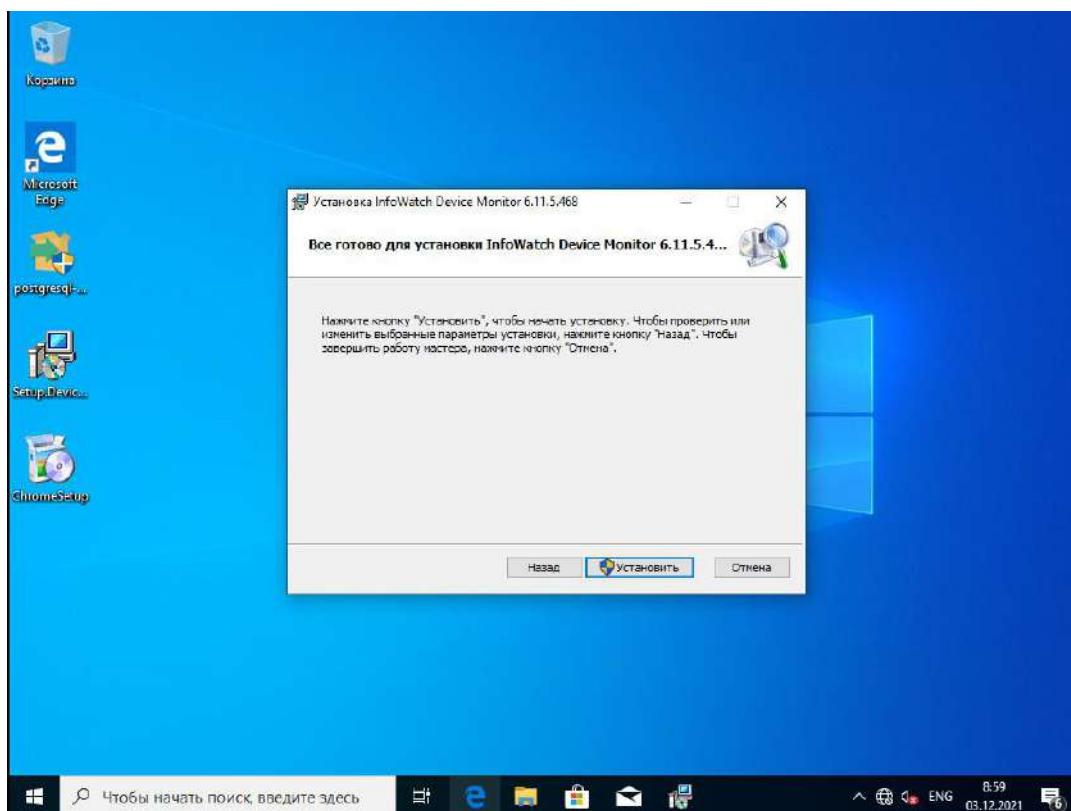
Задание 2

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».

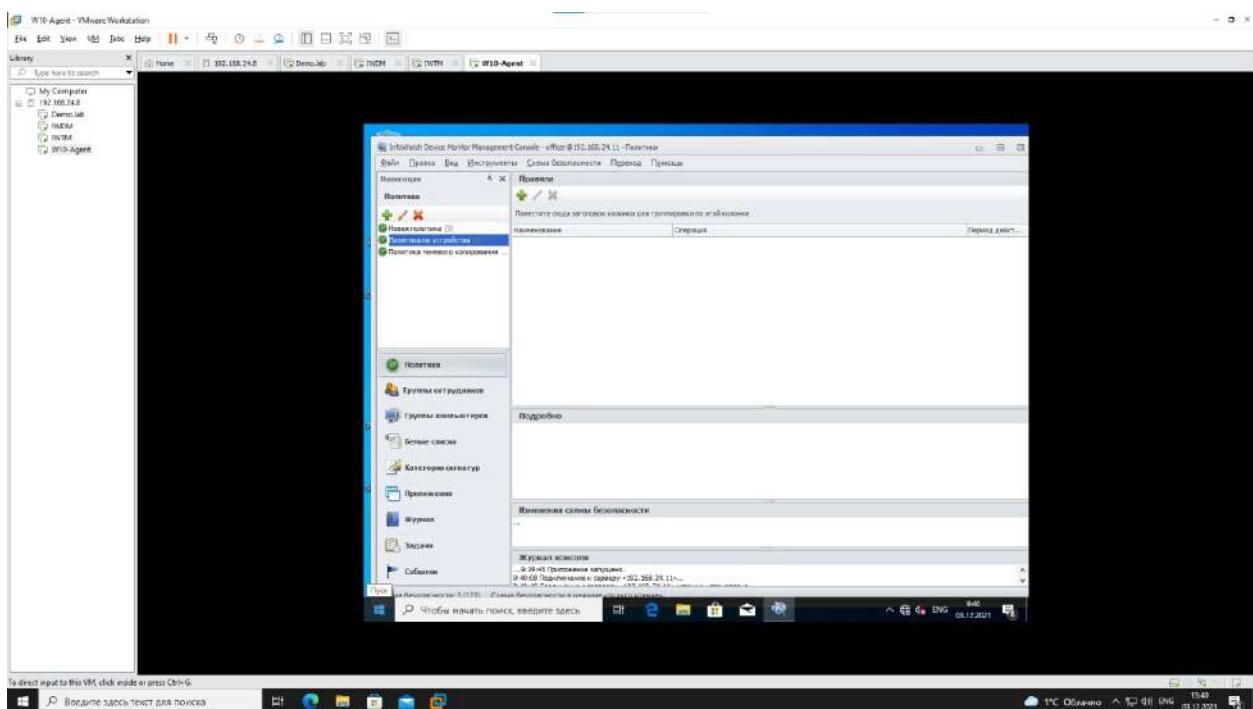
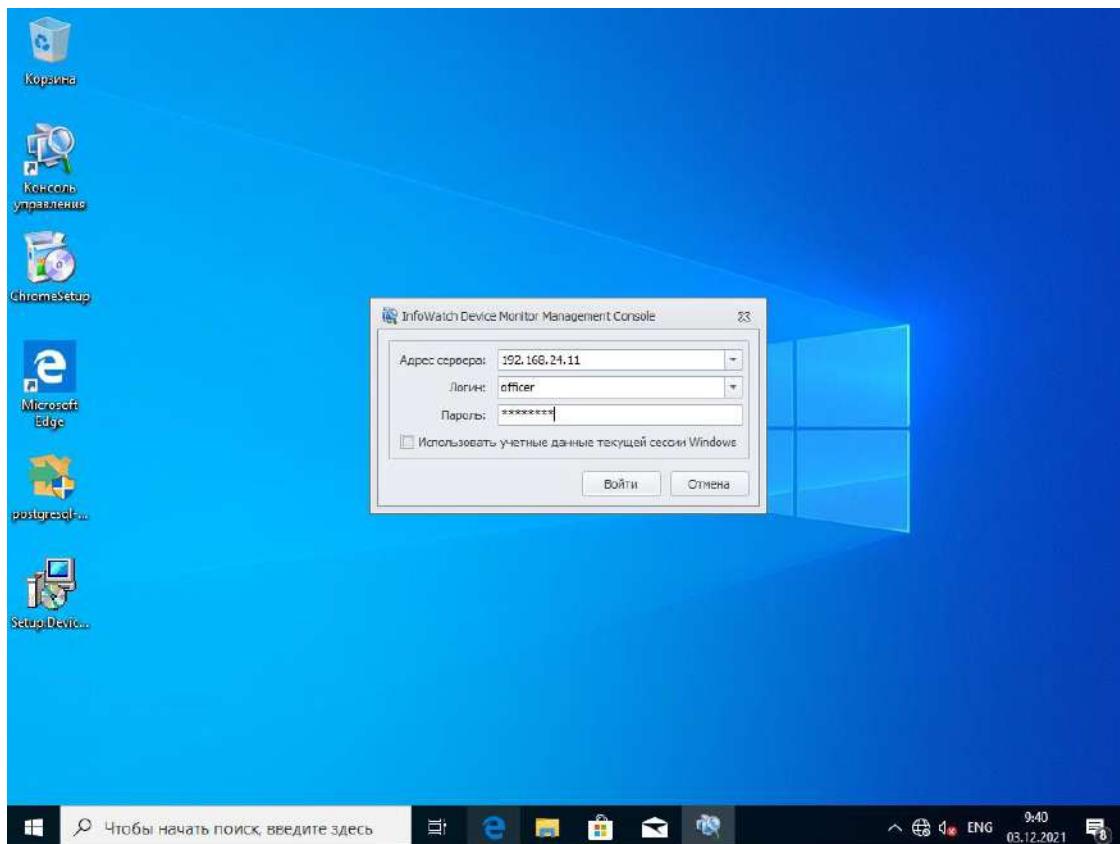
Убираем сервер, оставляем только консоль управления



Установили InfoWatch Device Monitor



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



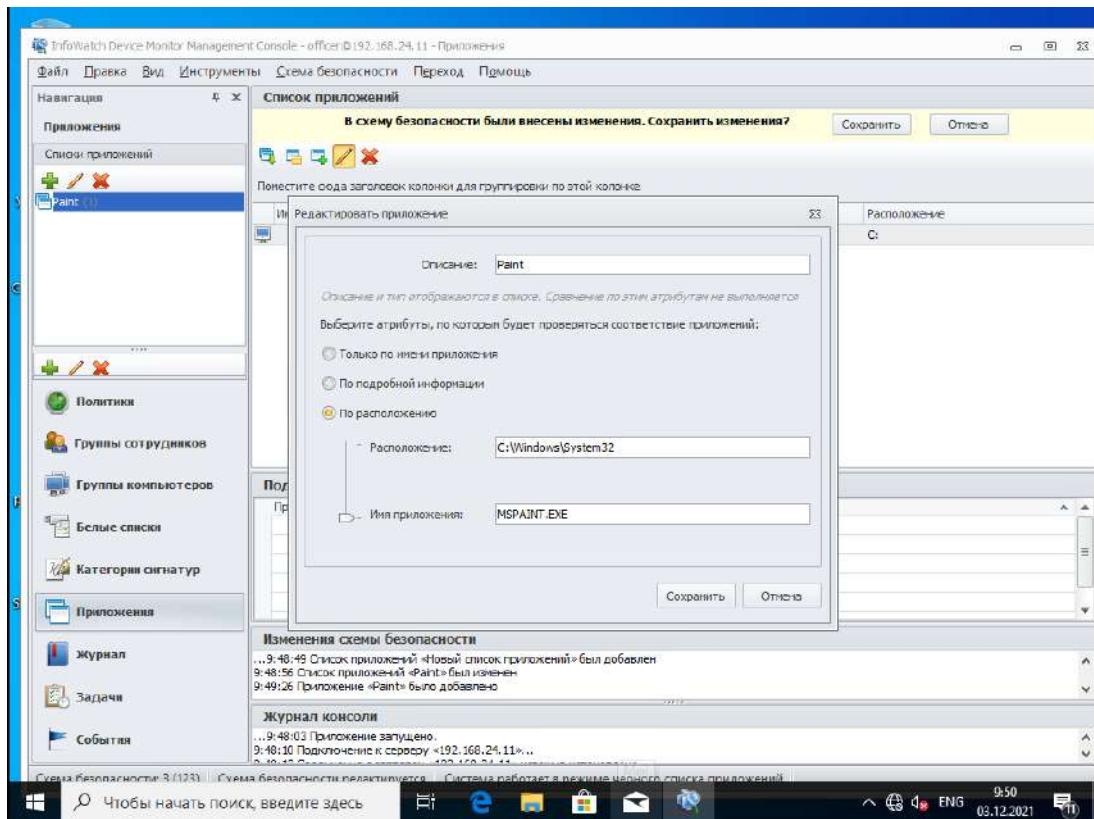
Следующие правила создаются в политике «Отдел1»

Правило 1

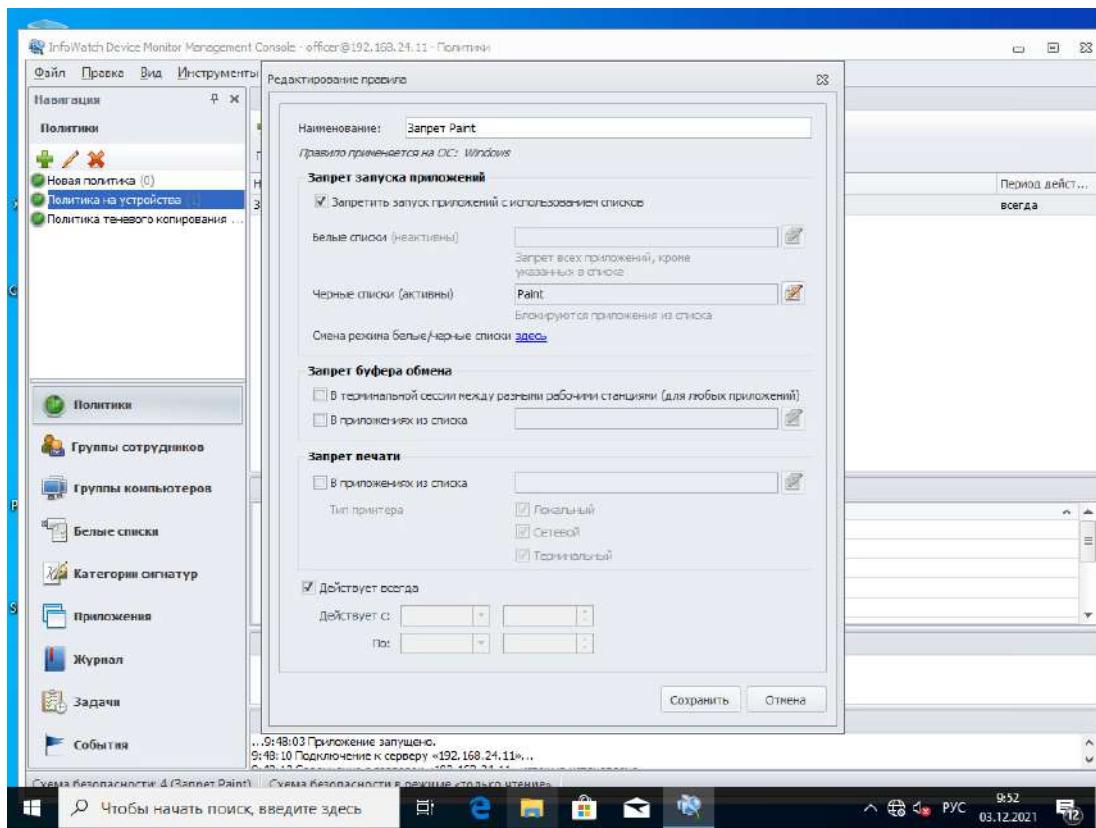
Необходимо запретить пользоваться Microsoft Paint, так как участились случаи подделки печатей компании.

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.

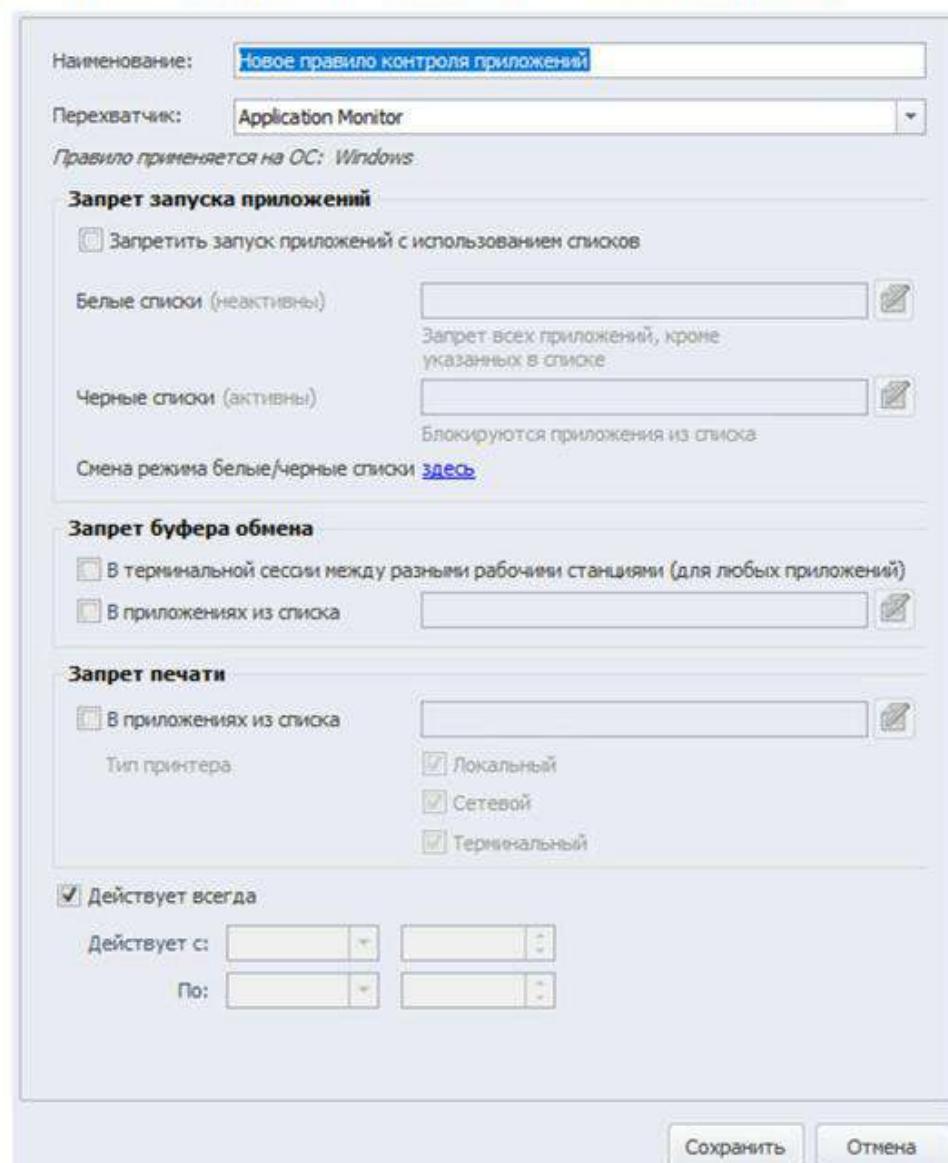


Рисунок 57 – «Создание правила»

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...	ShellFvmeria	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.

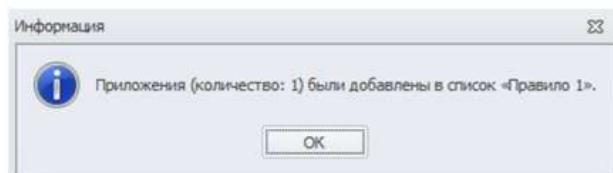


Рисунок 59 – «Успешное добавление приложения»

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: [] []

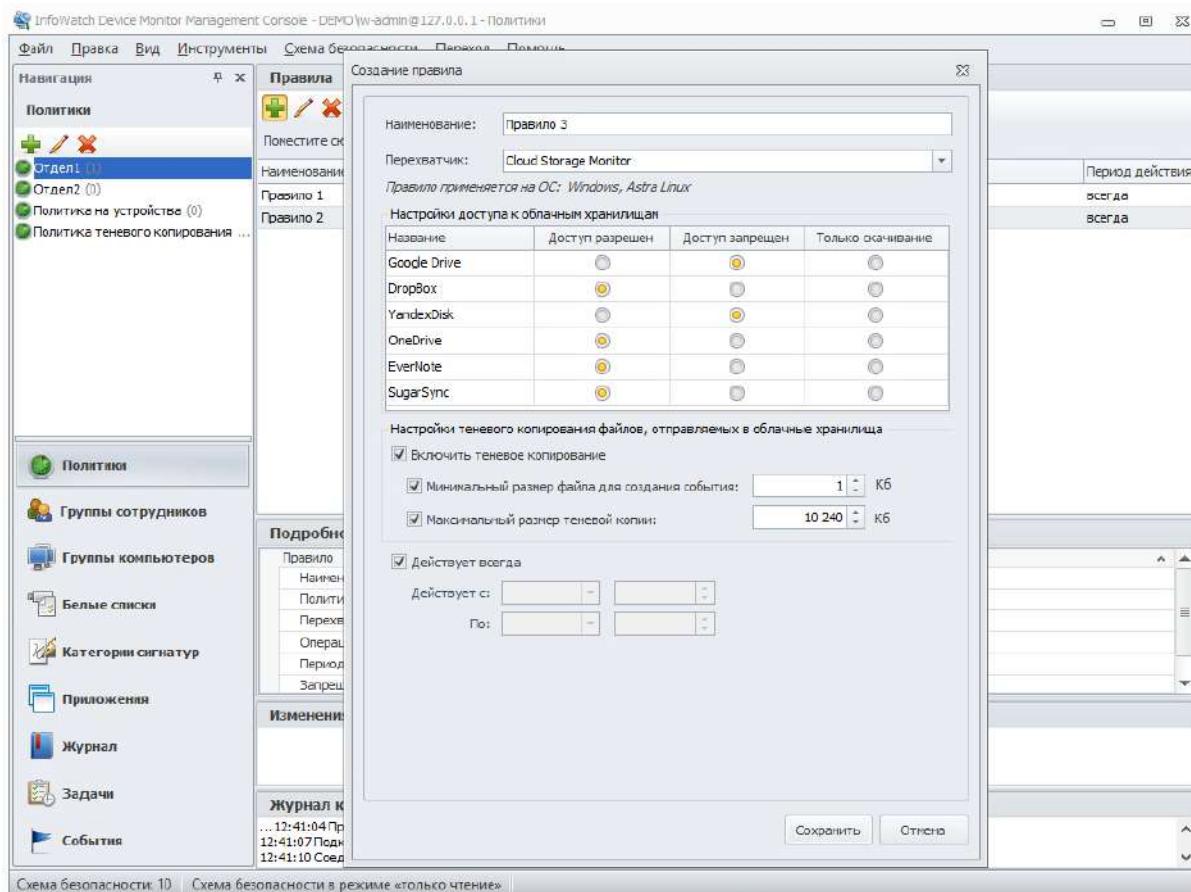
Рисунок 60 – «Правило 1»

Зафиксировать скриншотами необходимо!

Правило 3

Ограничить доступ к облачным хранилищам GoogleDrive и YandexDisk.

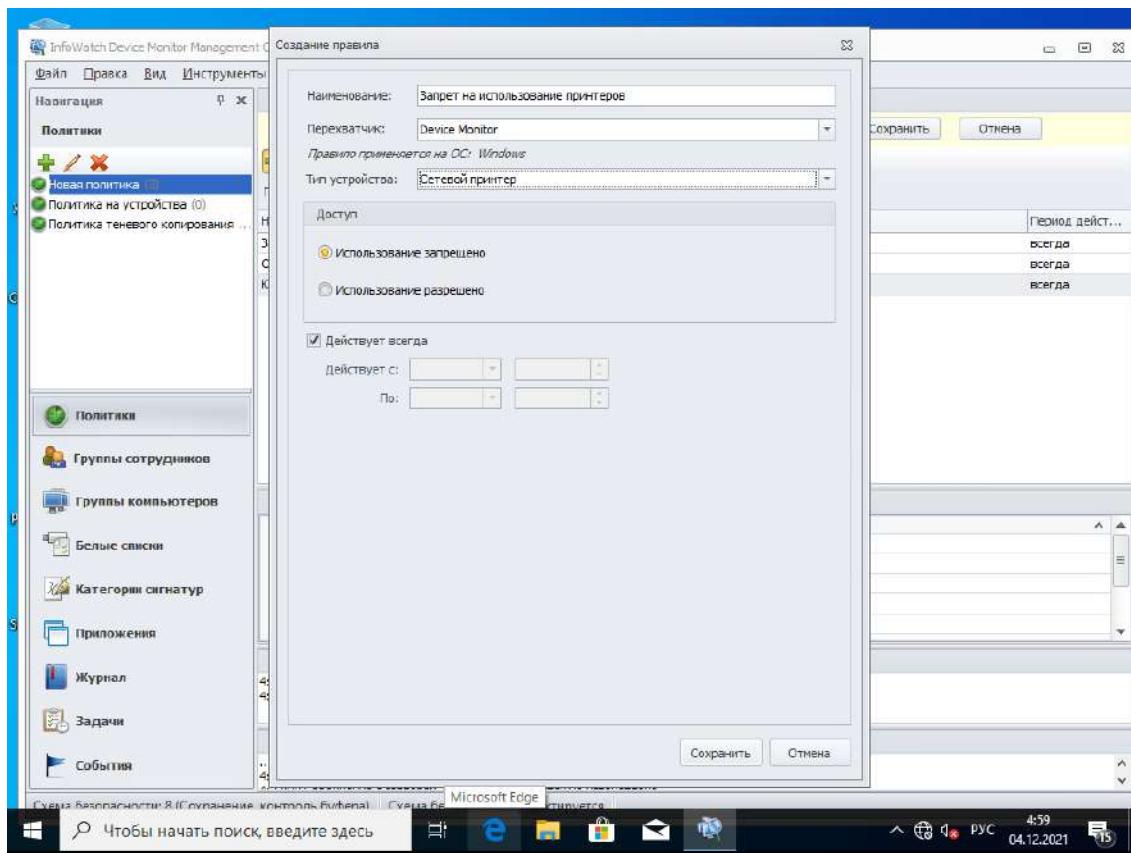
Проверить работоспособность и зафиксировать выполнение



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

A screenshot of the 'Правило 5' configuration dialog. The 'Наименование:' field contains 'Правило 5'. The 'Перехватчик:' dropdown is set to 'Device Monitor'. The 'Правило применяется на ОС:' dropdown is set to 'Windows'. The 'Тип устройства:' dropdown is set to 'Съемное устройство хранения' (Removable storage device). The 'Доступ' (Access) section contains four radio buttons: 'Нет доступа' (No access), 'Только чтение' (Read-only) which is selected, 'Полный доступ на зашифрованные носители' (Full access to encrypted media), and 'Использование разрешено' (Usage allowed).

Проверить работоспособность и зафиксировать выполнение

Правило 6

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

Проверить работоспособность и зафиксировать выполнение

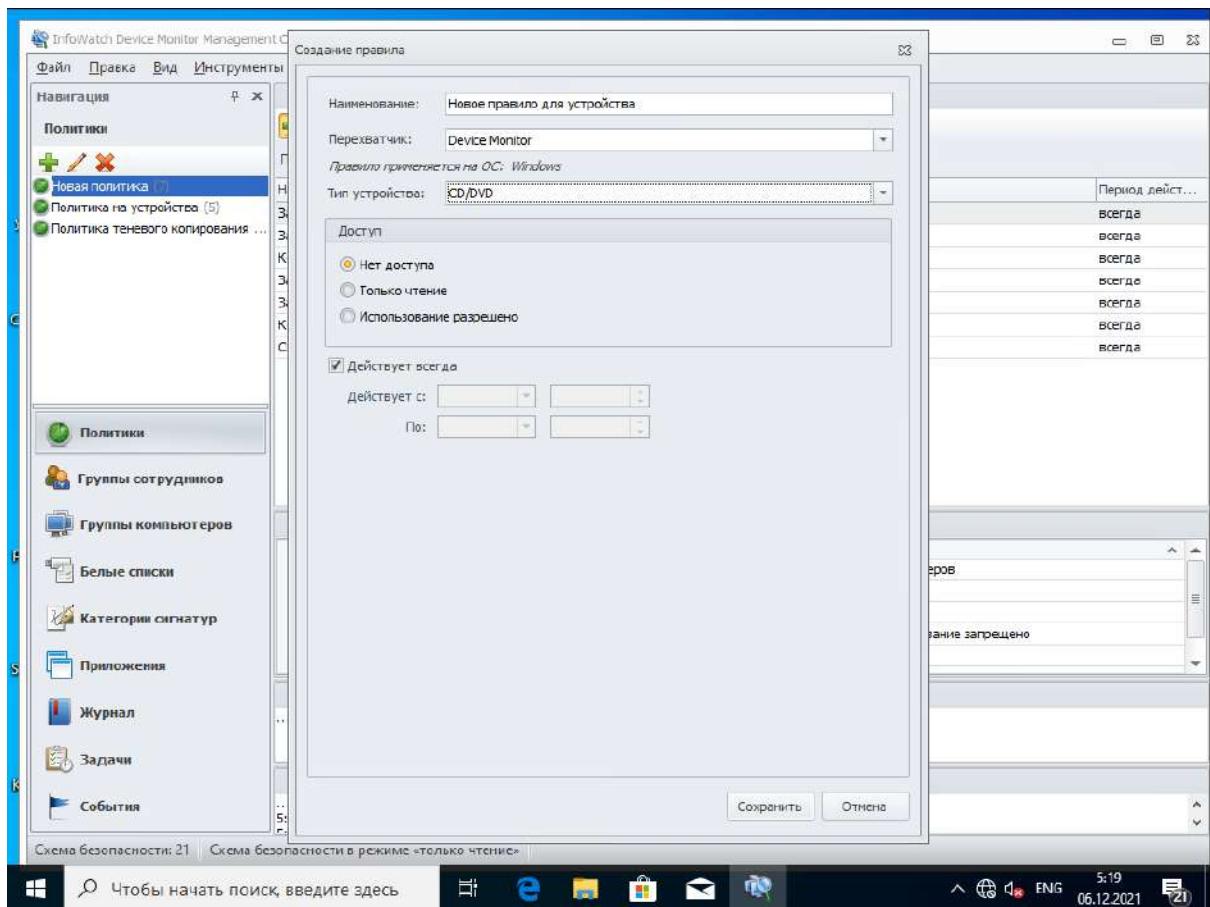
Наименование:	Правило 6
Перехватчик:	Device Monitor
Правило применяется на ОС: Windows	
Тип устройства:	Съемное устройство хранения
Доступ	
<input type="radio"/> Нет доступа	
<input type="radio"/> Только чтение	
<input checked="" type="radio"/> Полный доступ на зашифрованные носители	
<input type="radio"/> Использование разрешено	

Проверить работоспособность и зафиксировать выполнение!

Правило 7

Полностью запретить использование CD/DVD-дисковода.

Проверить работоспособность и зафиксировать выполнение



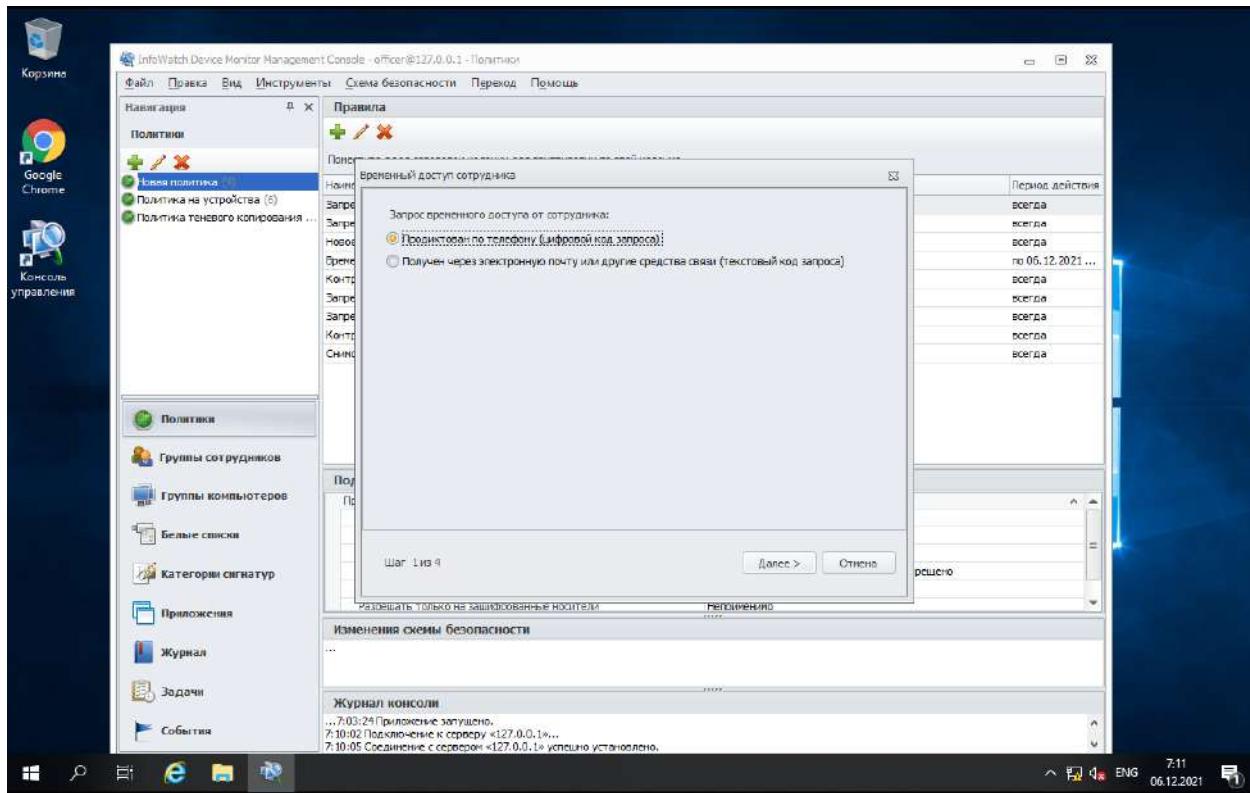
Проверить работоспособность и зафиксировать выполнение!

Правило 8

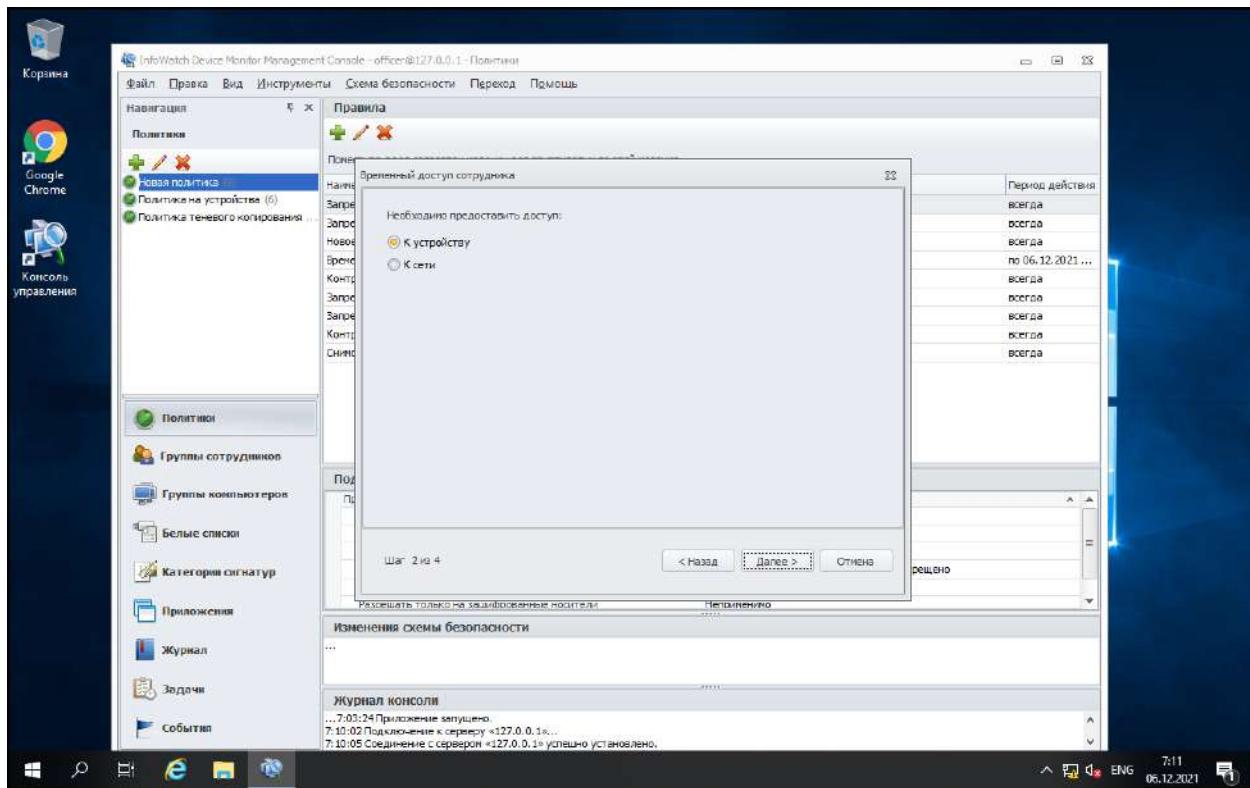
С учетом ранее выполненного запрета необходимо предоставить временный доступ для устройства на 7 минут для пользователя.

Зафиксировать этапы выдачи доступа и работоспособность скриншотами.

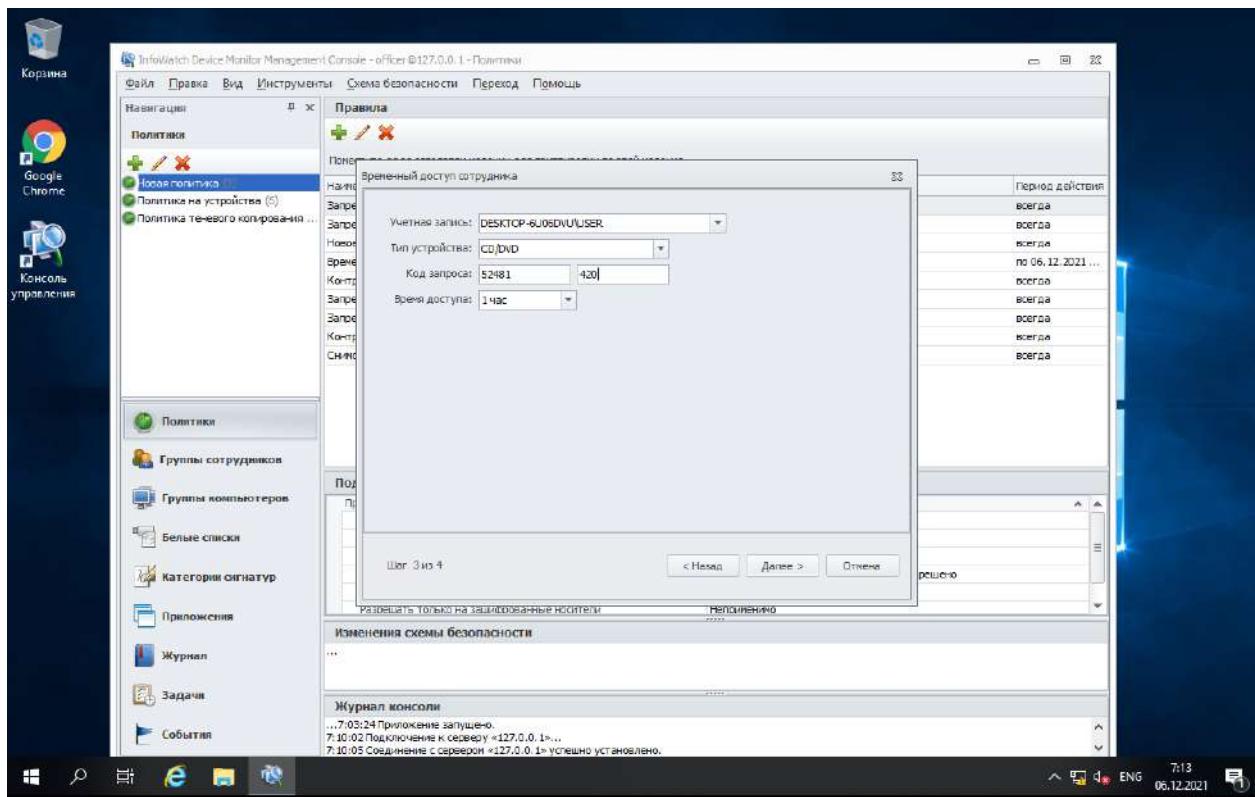
Выдаем временный доступ сотруднику



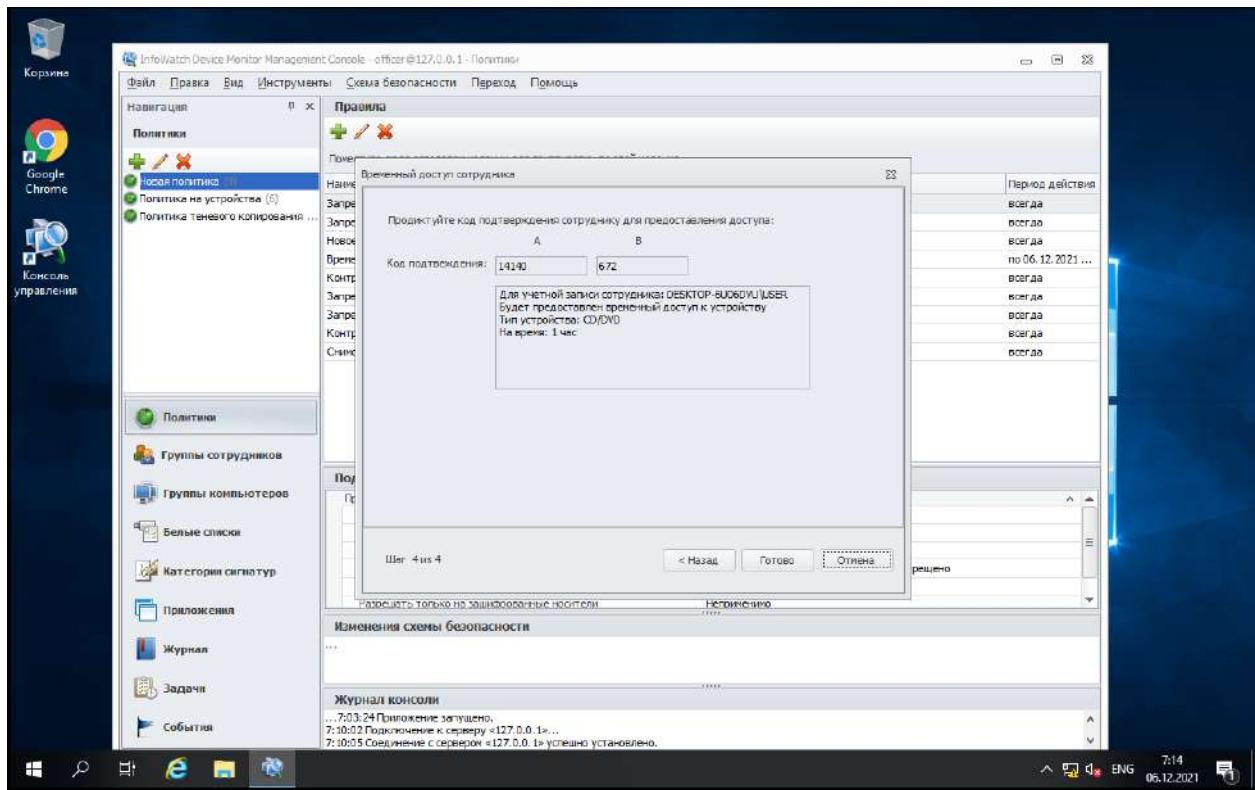
Предоставляем доступ к устройству



Выбираем компьютер, время доступа



Временный доступ



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 зафиксировать 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.

The screenshot shows the Windows Device Monitor Console interface. A new rule is being created with the following settings:

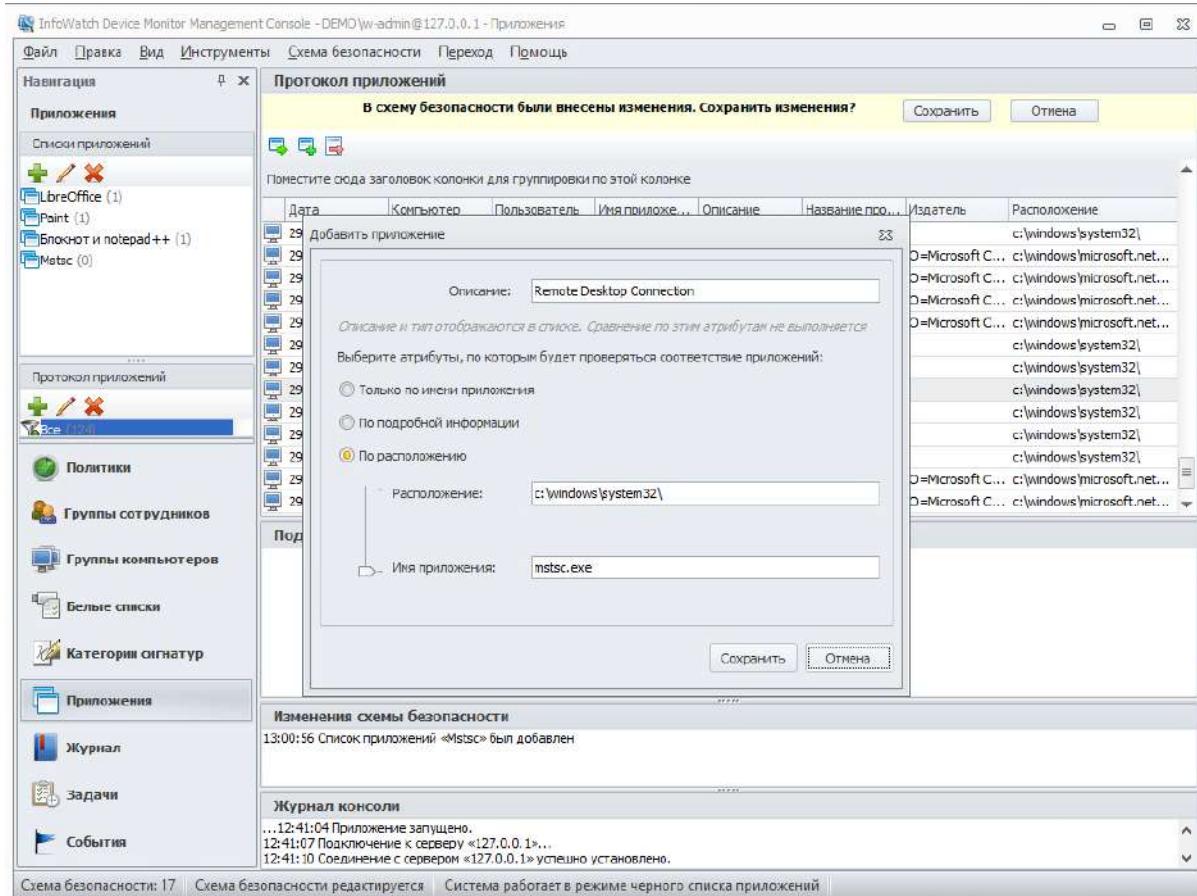
- Наименование:** Правило 8
- Перехватчик:** Clipboard Monitor
- Правило применяется на ОС:** Windows
- Перехватывать вставку из буфера обмена:**
 - В приложения терминальной сессии
 - В приложения кроме терминальных сессий Правило 8
 - В пределах одного и того же приложения
- Создавать снимки экрана при копировании в буфер обмена и вставке из него:** (unchecked)

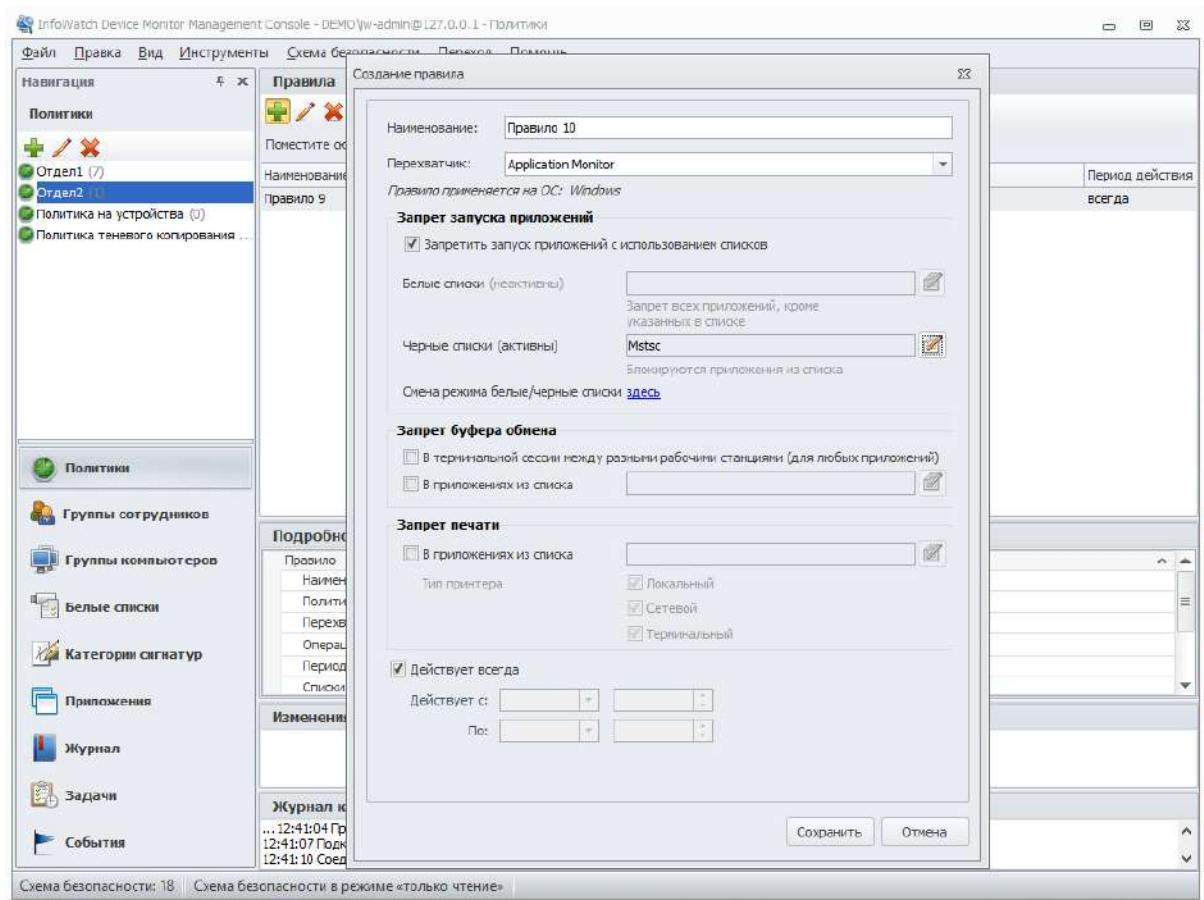
Проверить работоспособность и зафиксировать выполнение скриншотом.

Правило 10

Необходимо запретить использовать терминальные сессии для пользователя.

Проверить работоспособность и зафиксировать выполнение



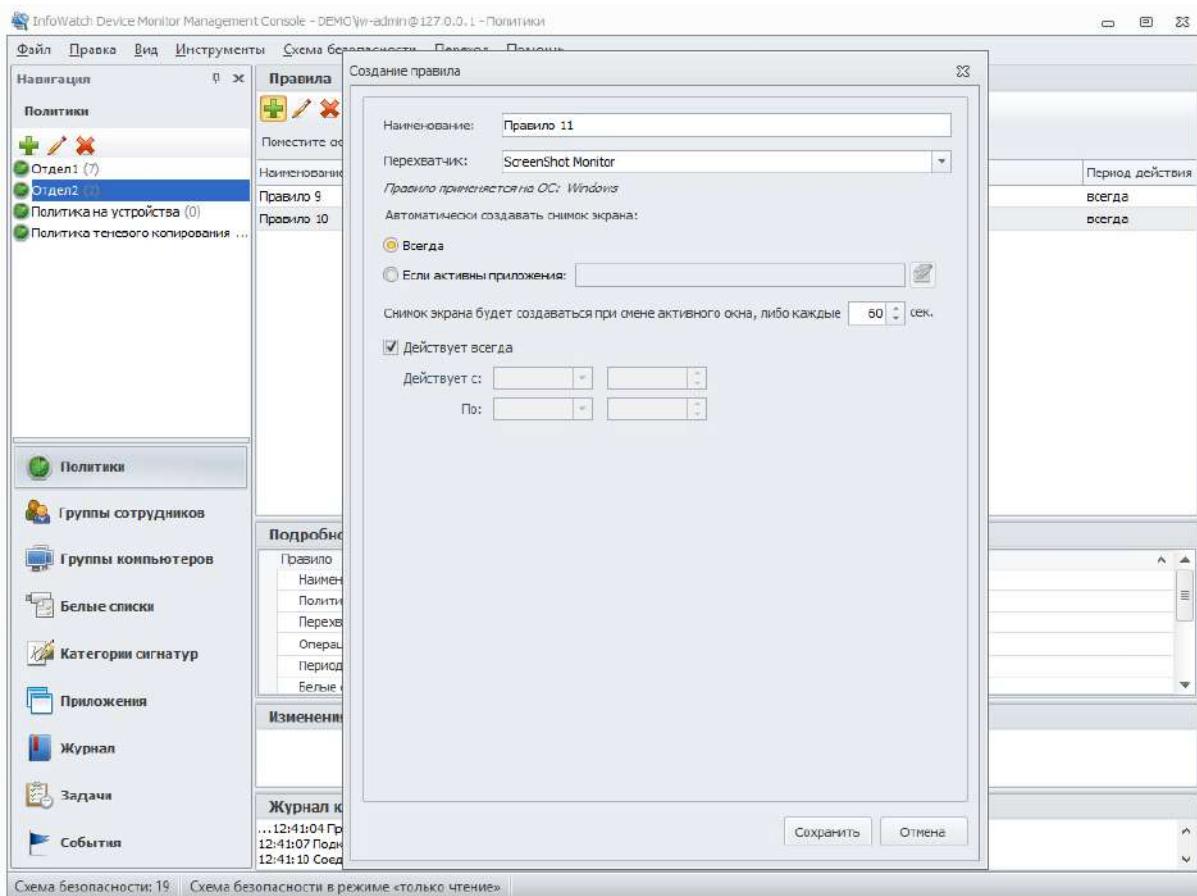


Проверить работоспособность и зафиксировать выполнение!

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

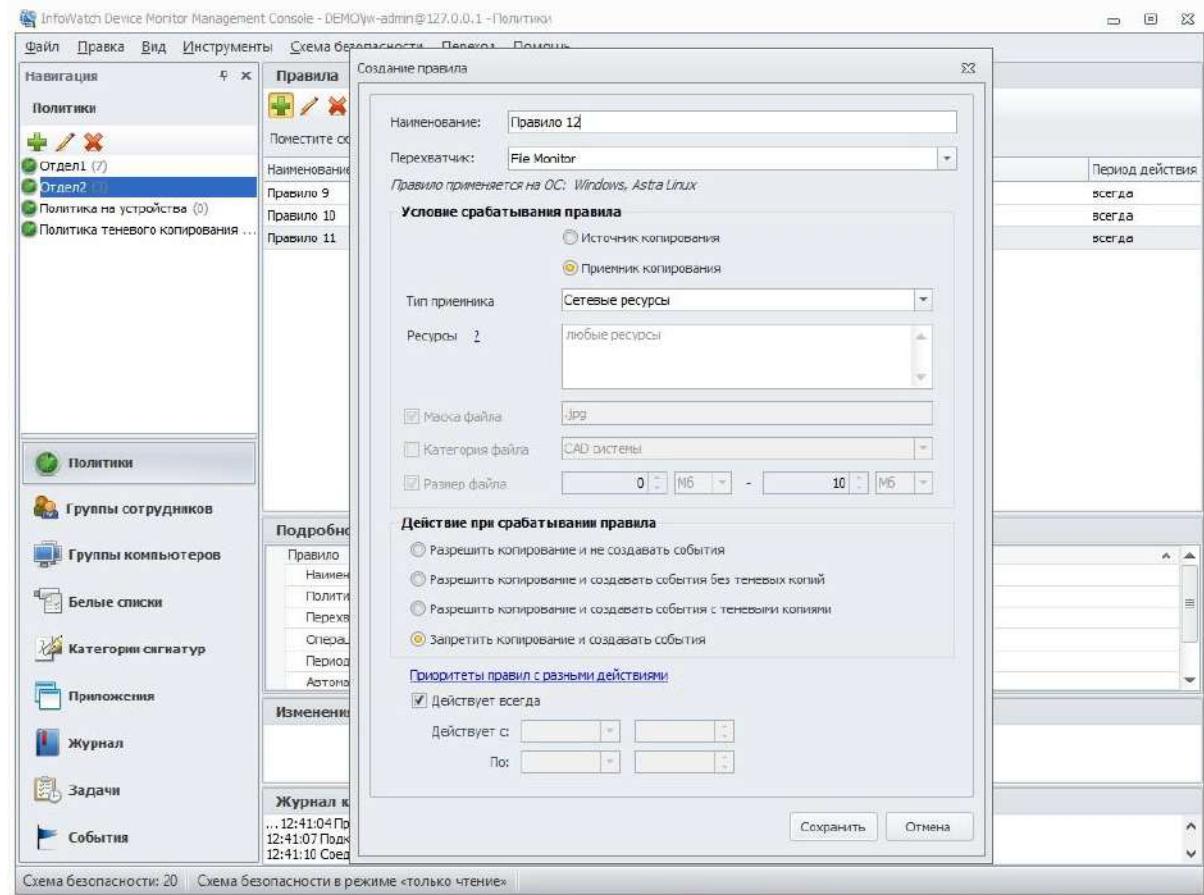


Проверить работоспособность и зафиксировать выполнение

Правило 12

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

Проверить работоспособность и зафиксировать выполнение



Проверить работоспособность и зафиксировать выполнение!

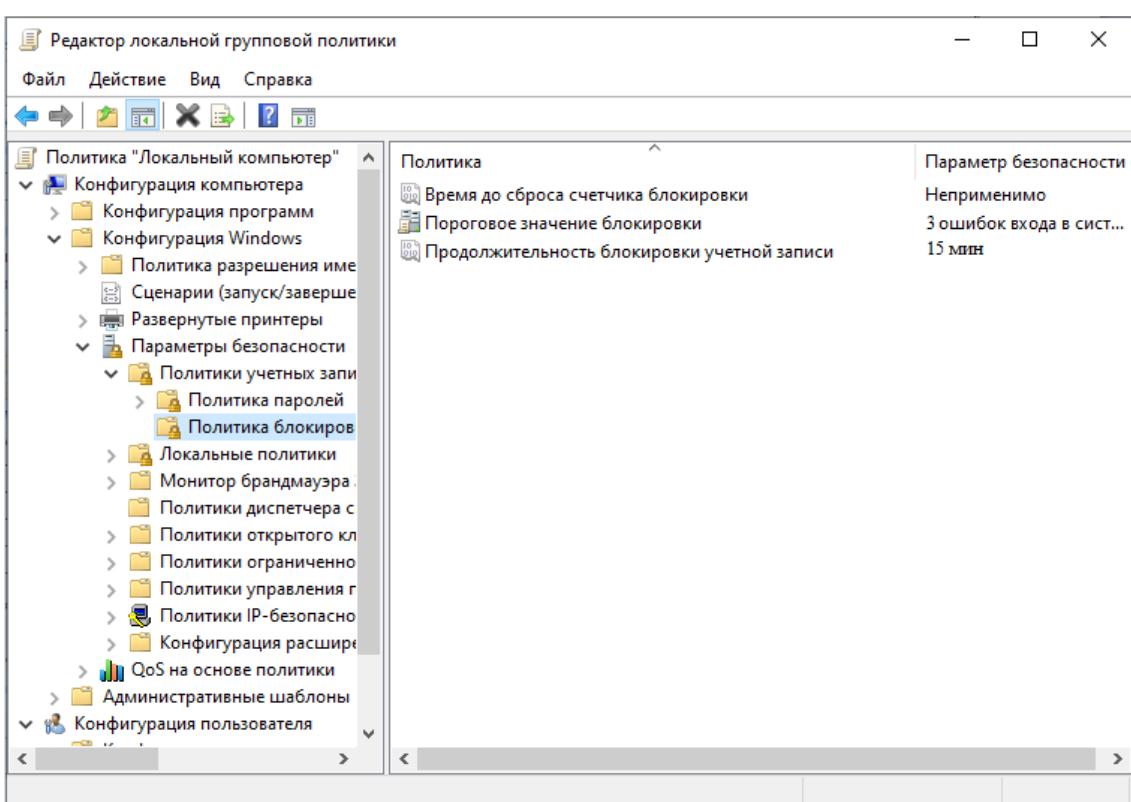
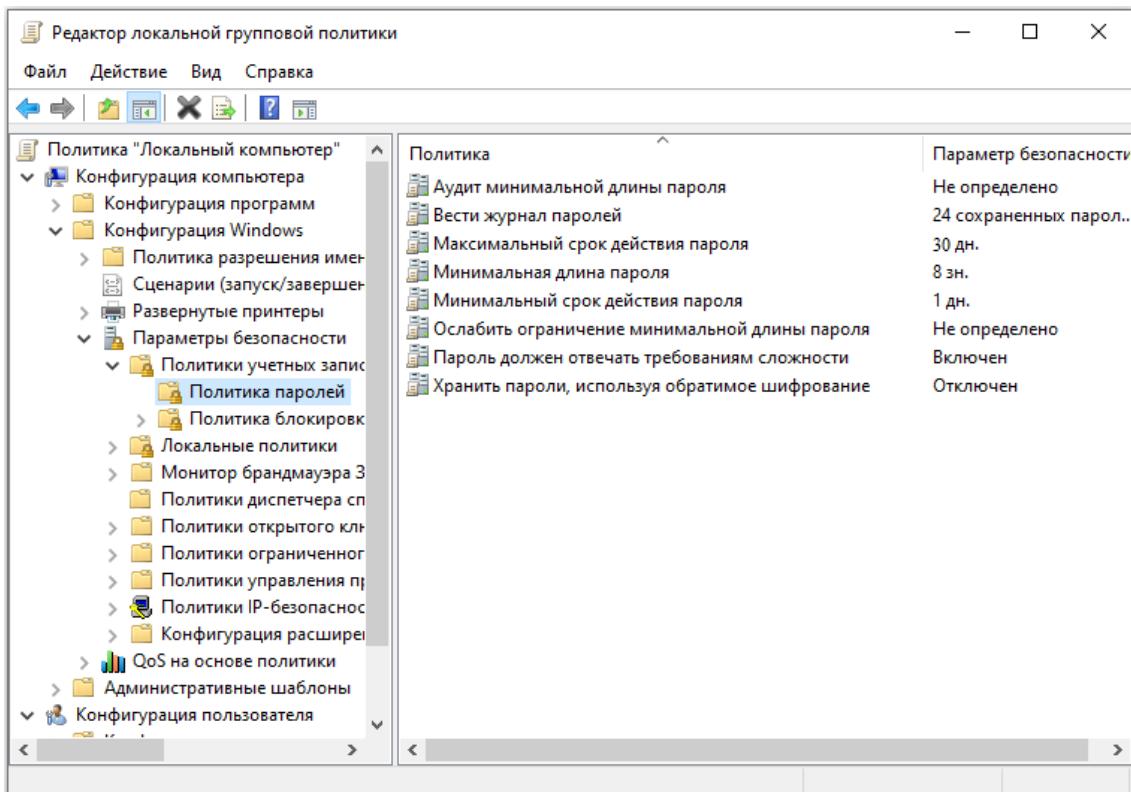
Групповые политики домена

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.



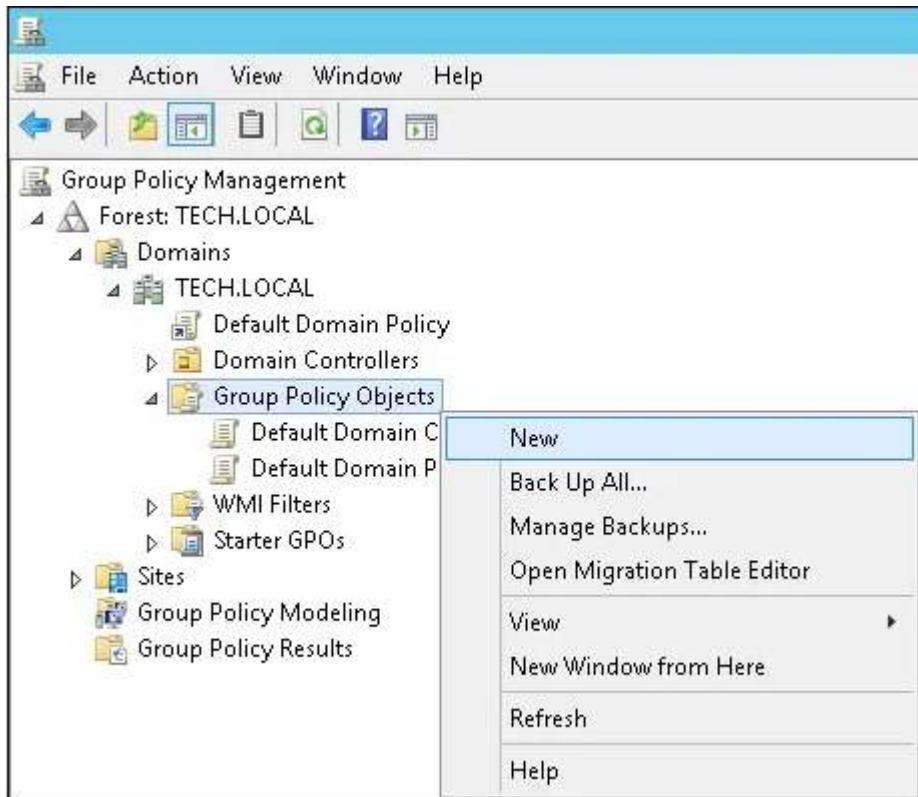
Задокументировать настройки политики скриншотами.

Групповая политика 2

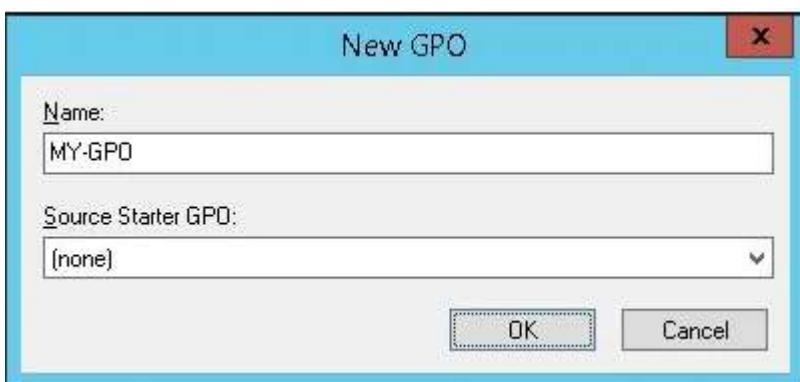
Запретить запуск приложений по списку: PowerShell, ножницы, сведения о системе.

Зафиксировать настройки политики и выполнение скриншотами.

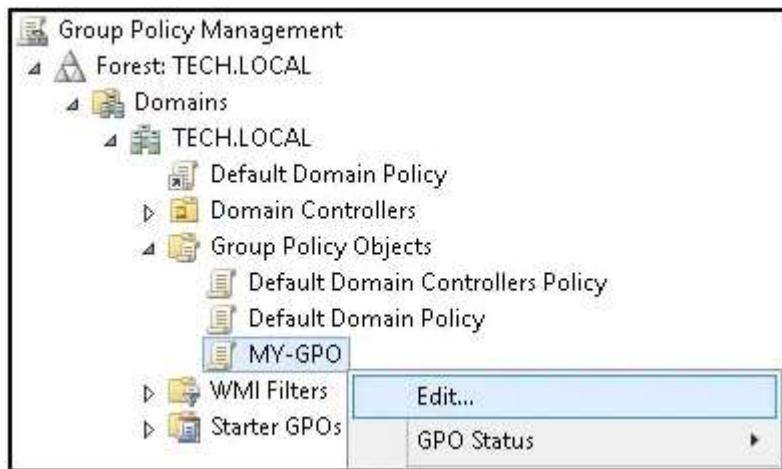
Создаем новую групповую политику



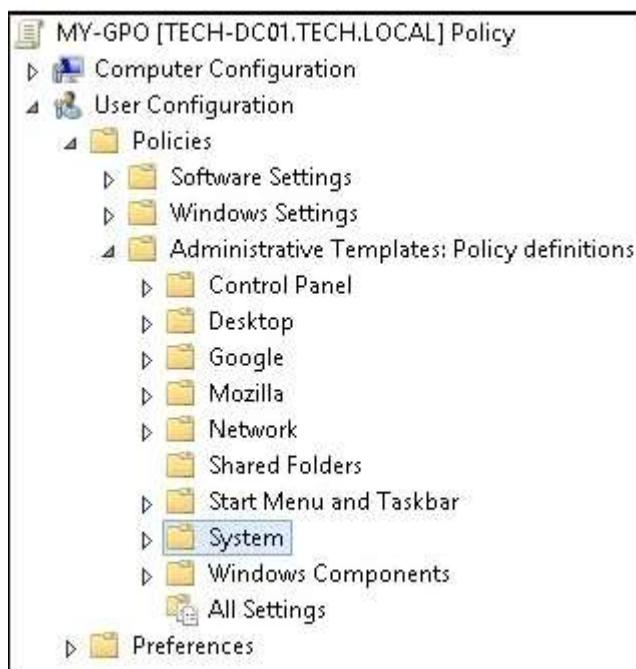
Вводим имя для новой групповой политики



Правой кнопкой по созданной политики → Редактировать



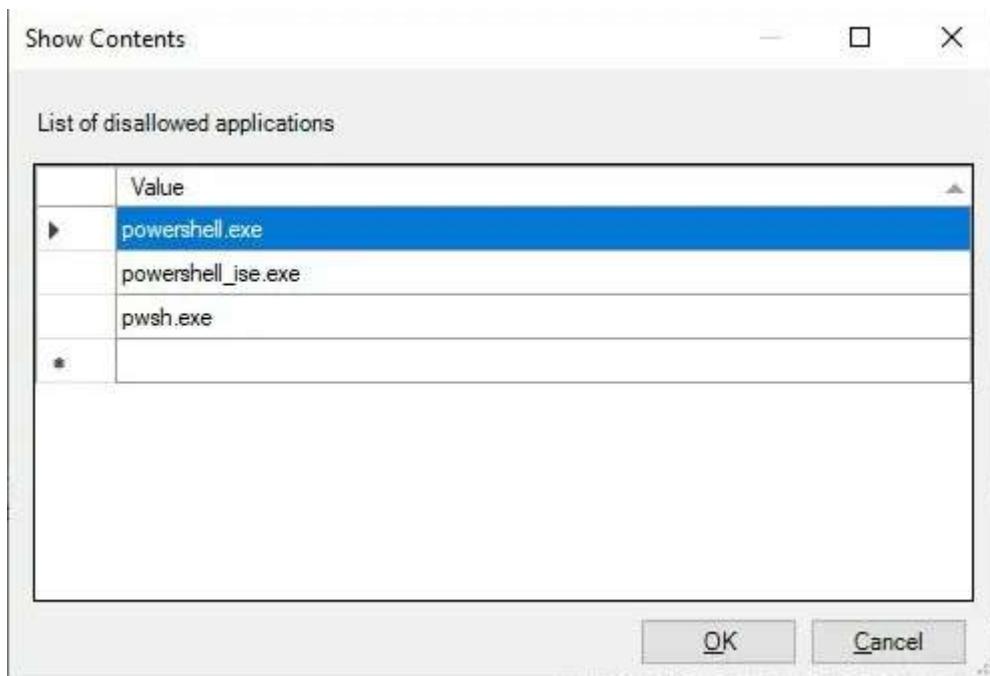
Переходим по пути в папку → Система



Включаем политики → “Не запускать указанные приложения Windows”



Нажимаем кнопку → Показать и вводим список команд, запускающих PowerShell



Также вводим ножницы

SnippingTool.exe

И сведения о системе

msinfo32.exe

Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 3

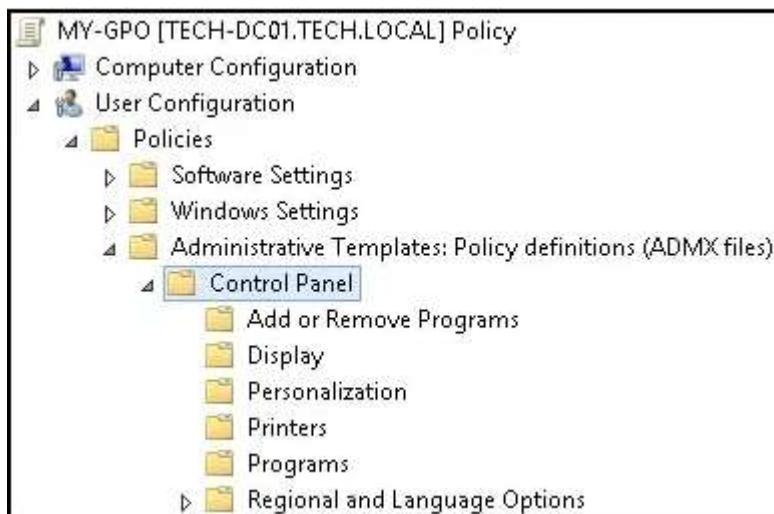
Запретить использование панели управления стандартными политиками.

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.

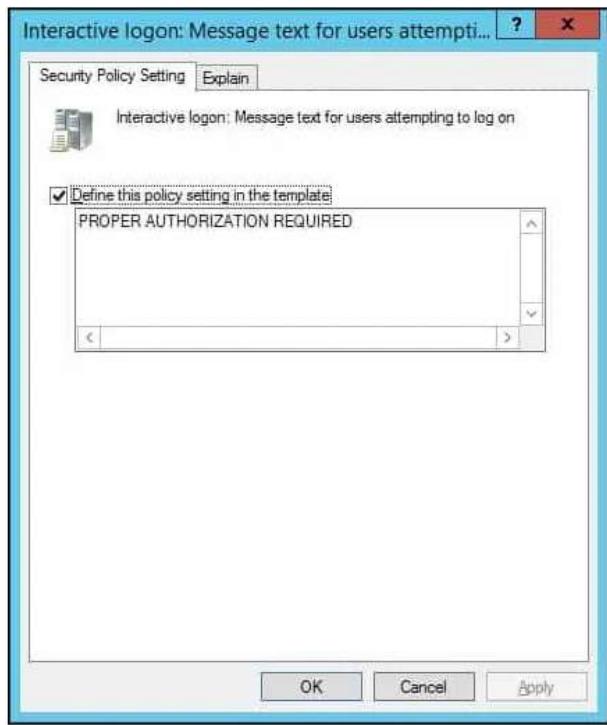
Зафиксировать настройки политики и выполнение скриншотами.

Создаем новую политику безопасности переходим к её редактированию

Переходим по пути в → Параметры безопасности



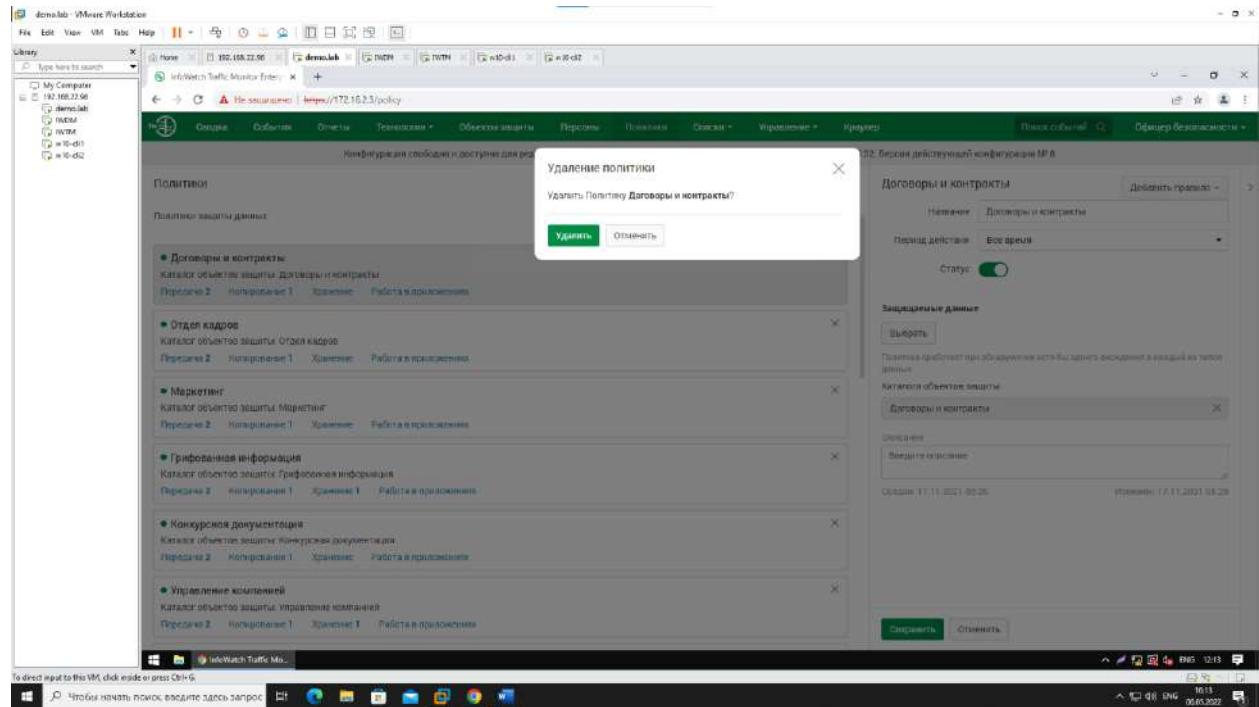
Включаем следующий элемент настройки и вводим нужный текст → “сообщение с именем сервера авторизации”



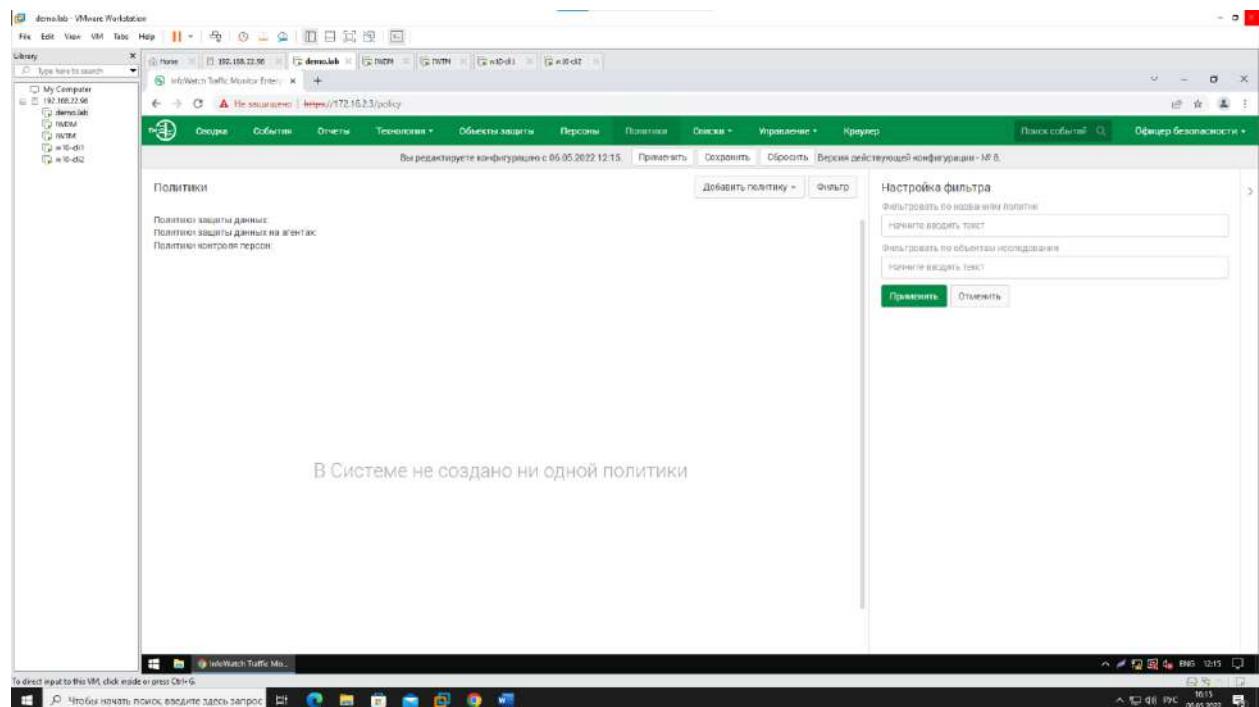
Задокументировать настройки политики и выполнение скриншотами.

Модуль 3

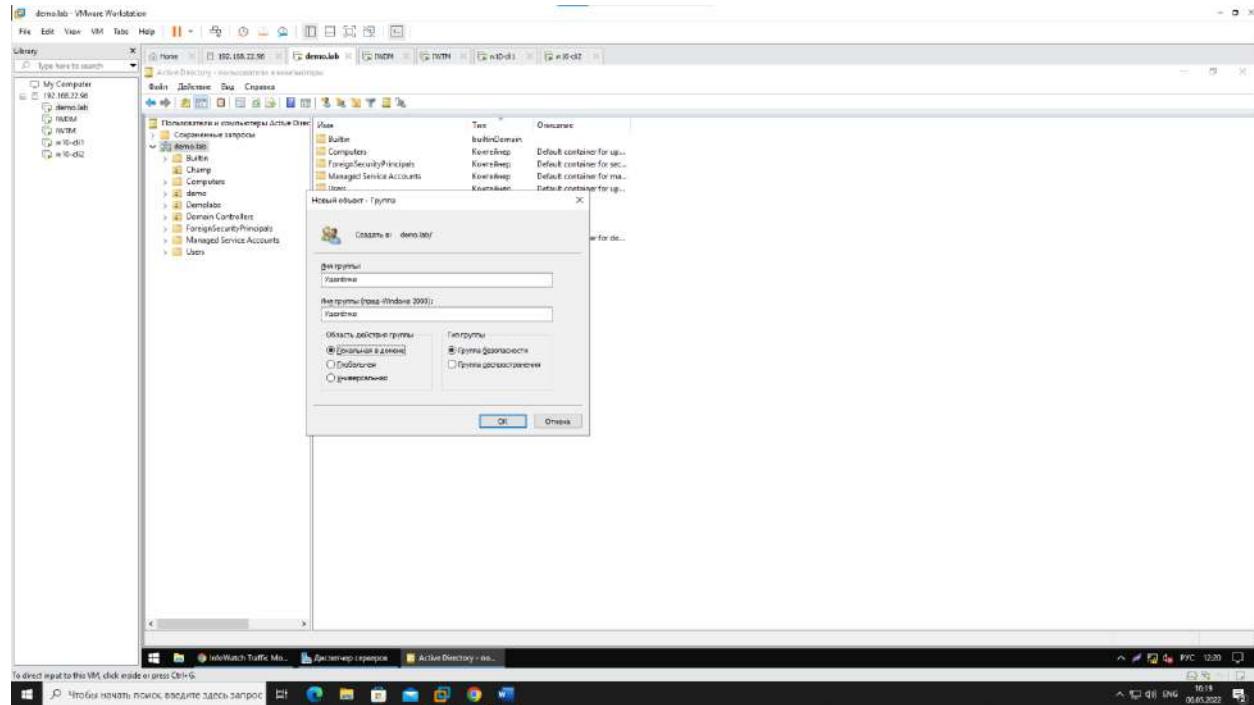
Удаляем все стандартные политики



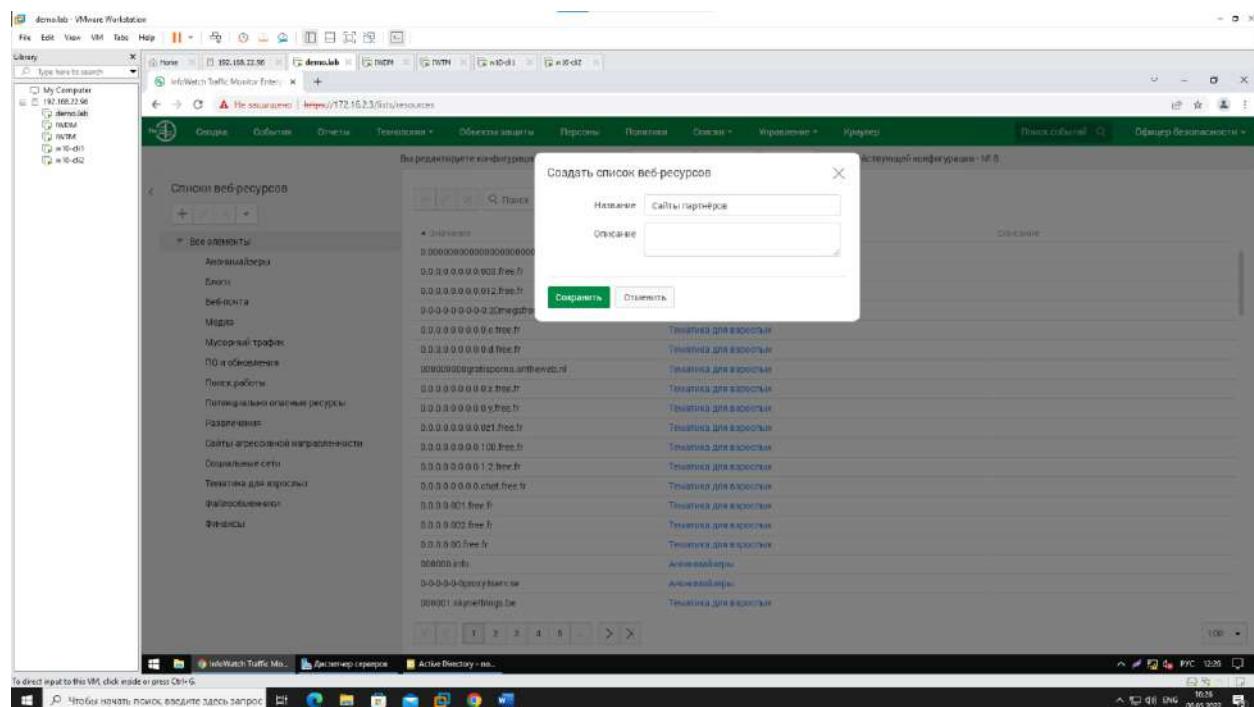
После удаления выглядит вот так



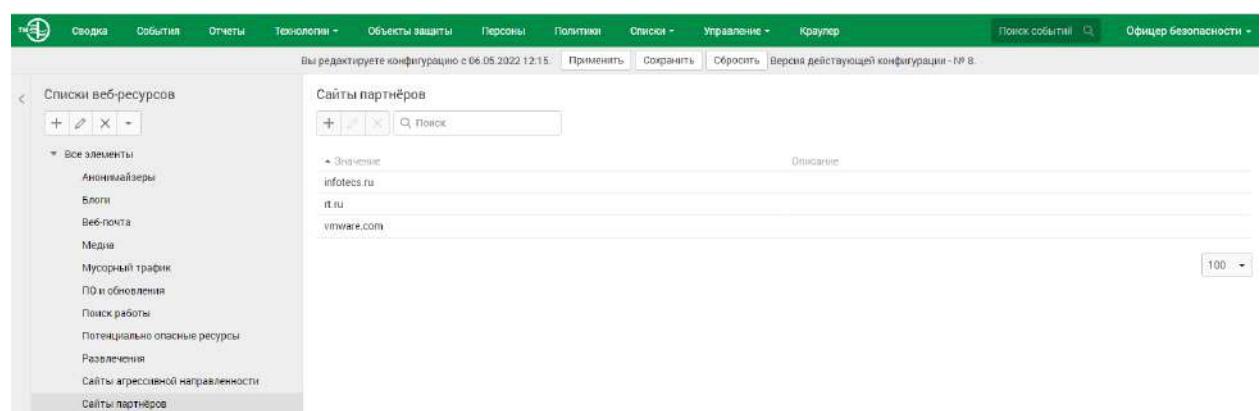
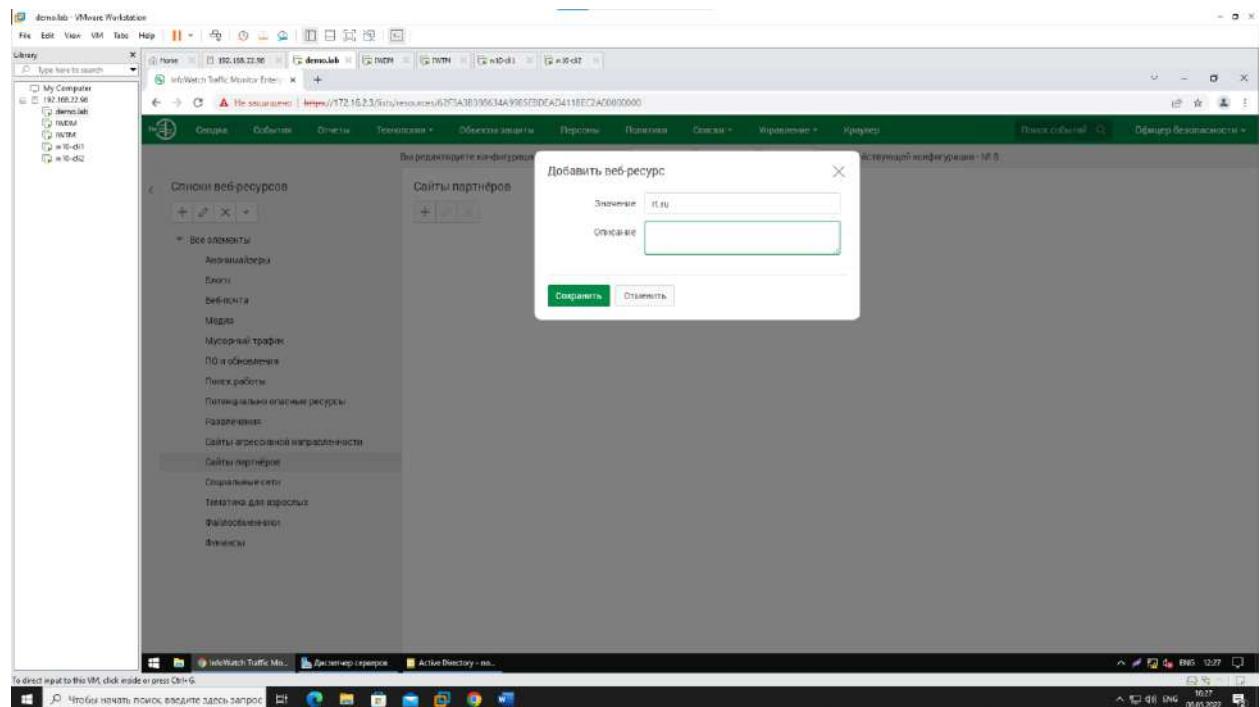
Создаем локальную группу с название – удалёнка



Создаем список веб ресурсов (Списки – Веб-ресурсы)



Добавляем веб-ресурсы



Задание 4

Периметр компании

The screenshot shows the 'Редактирование' (Editing) screen for a perimeter configuration. The left sidebar lists 'Периметры' (Perimeters) with 'Исключить из перехвата' (Exclude from capture) selected. The main panel displays the following fields:

- Название:** Компания
- Почтовый домен:** @ demo.lab
- Список веб-ресурсов:** Сайты партнёров
- Группа персон:** Удаленка
- 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'. Below these are 'Сохранить' (Save) and 'Отменить' (Cancel) buttons.

Исключение из перехвата

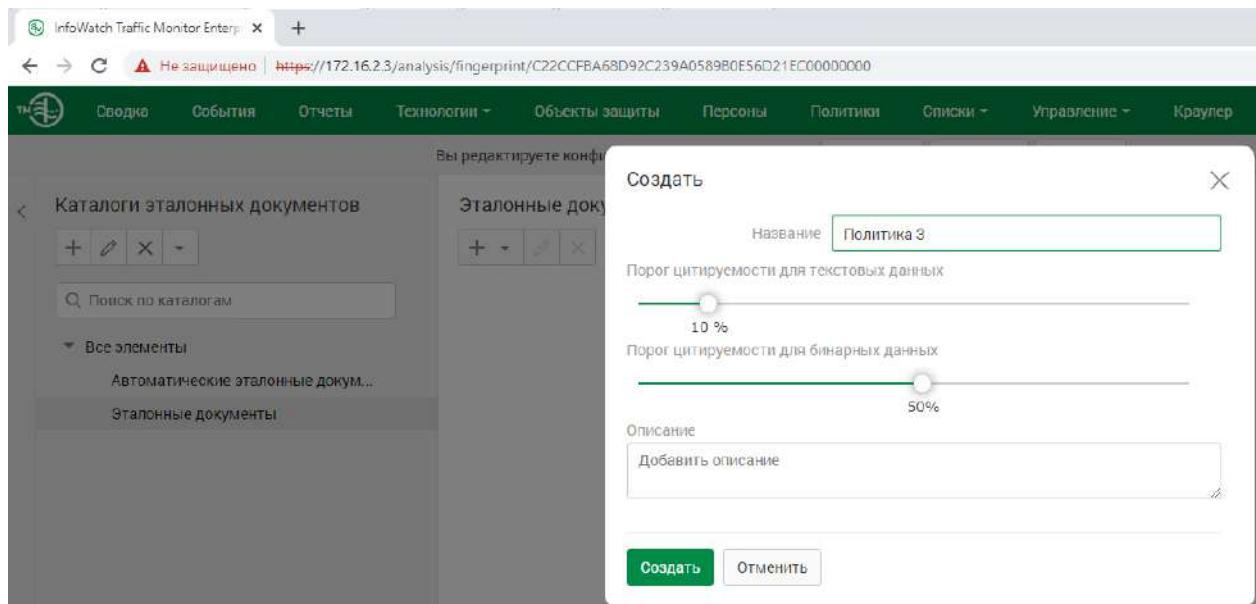
The screenshot shows the 'Редактирование' (Editing) screen for an exclude-from-capture policy. The left sidebar lists 'Периметры' (Perimeters) with 'Исключить из перехвата' (Exclude from capture) selected. The main panel displays the following fields:

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

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

Политика 3

Технологии – Эталонные документы, создаем политику в эталонных документах



На основе всех типов данных

InfoWatch Traffic Monitor Enterprise

Не защищено | <https://172.16.2.3/analysis/fingerprint/C5AE72383BB242BEA47AE8>

Сводка События Отчеты Технологии Объекты защиты П

Вы редактируете конфигурацию с 06.0

Каталоги эталонных документов

+ ⚪ X ▾

Поиск по каталогам

Все элементы

Автоматические эталонные докум...

Эталонные документы

Политика 3

Политика 3

+ ⚪ X ▾

На основе текстовых данных

На основе всех типов данных

The screenshot shows the 'Baseline Document Catalogs' configuration screen. It includes a search bar, a tree view of catalog elements (All elements, Automatic baseline documents, Baseline documents), and a specific policy named 'Policy 3'. The right side shows two options for data processing: 'Based on textual data' and 'Based on all data types'.

Добавляем картинку котика

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

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

Каталоги эталонных документов

+ ⚪ X ▾

Поиск по каталогам

Все элементы

Автоматические эталонные докум...

Эталонные документы

Политика 3

Политика 3

+ ⚪ X ▾

Название Формат файла Название файла Размер файла Дата создания Описание

Кот.png Изображение PNG Кот.png 8.11 KB 06.05.2022 13:02

10 ▾

Загрузка технологий

Эталонные документы

Кот.png ✓ Сохранено

The screenshot shows the configuration interface with the 'Baseline Document Catalogs' section selected. A file named 'Kot.png' has been added to the catalog under the 'Baseline documents' category. A confirmation message at the bottom right indicates the file was saved.

Добавляем объекты защиты

Вы редактируете конфигурацию

Создать

Название: Политика 3

Статус:

Описание:

Создать Отменить

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

Создание объекта защиты

Категории Текстовые объекты Эталонные документы 1 Бланки Печати Выгрузки из БД Графические объекты

Каталоги эталонных документов

Эталонные документы

Название	Формат файла	Название файла	Размер файла	Дата создания	Опции
<input checked="" type="checkbox"/> Kot.png	Изображение PNG	Kot.png	8.11 KB	06.05.2024	<input type="button" value="..."/>

Создать Отменить Создать объект защиты на каждый выбранный элемент

Условием – выбираем кортику Кота

Создание объекта защиты

Название Политика 3

Статус

Элементы технологий Условия обнаружения

Добавить условие

Условие

Кот.rpg
Эталонный документ

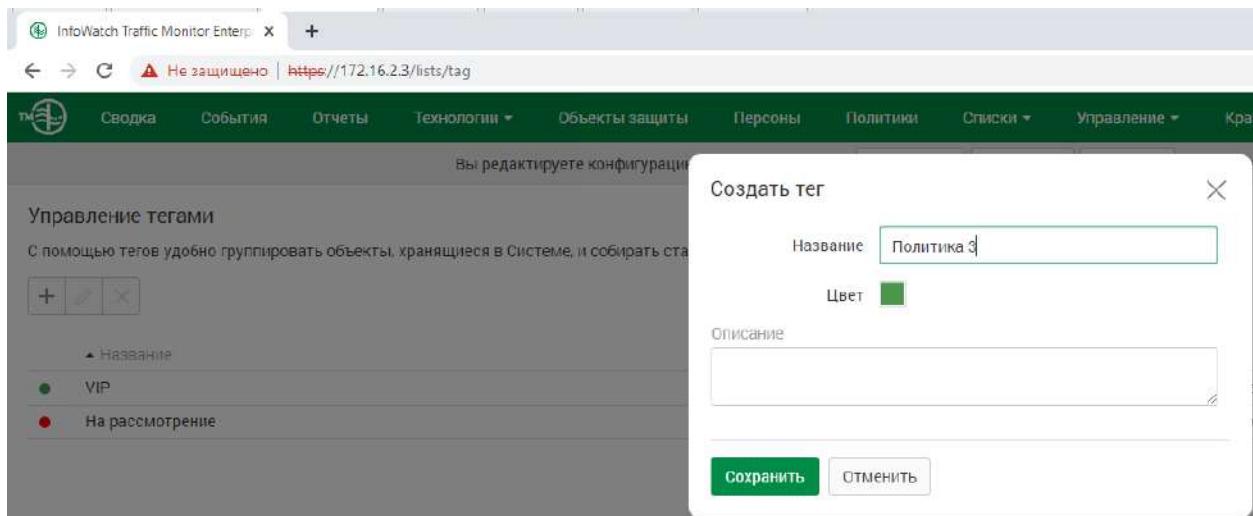
Описание

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			
<input type="button"/> П + <input type="button"/> <input type="button"/> X <input type="button"/>		<input type="text"/> Поиск <input type="button"/> Все			
Название	Элементы технологий	Дата создания	Дата изменения	Описание	
Политика 3	Кот.rpg	06.05.2022 13:07	06.05.2022 13:07		<input type="button"/> 10

Списки – Теги, создаем новый тег



Переходим в политики, создаем политику защиты данных

Добавляем правило передачи

Правило передачи

Компьютеры: CLIENT1, CLIENT2, DEMO-DC, DEMOLAB, IWM

Отправители: Любой отправитель

Направление маршрута: CLIENT1 → CLIENT2

Получатели: CLIENT1, CLIENT2, DEMO-DC, DEMOLAB, IWM

Дни действия правила: Любой день недели

Часы действия правила: 0:00 - 0:00

Действия при срабатывании правила:

- Отправить почтовое уведомление: Напишите вводить текст
- Заблокировать
- Назначить событие вердикт: Низкий
- Назначить событие типа: Политика 5
- Назначить отправителю статус: Выберите статус
- Удалить событие

Сохранить Отменить

Политика 5

Переходим в объекты защиты и создаем новый объект защиты

Создать

Название: Политика 5

Статус: Активны

Описание

Создать Отменить

Добавляем

Создание объекта защиты

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

Q 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

Q Поиск по каталогам

▼ Все элементы Текстовые объе...

Текстовые объекты

Q 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 (16ци...)	17.11.2021 05:29	Мировое сообщество	Номер кредитной карты

К < 1 2 3 4 > K 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

Поиск 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

10

Создать Отменить Создать объект защиты на каждый выбранный элемент

Вот так выглядит

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

Каталоги объектов защиты

Политика 5

Название	Элементы технологии	Дата создания	Дата изменения	Описание
Графический объект: Кредитная карта	Кредитная карта	06.05.2022 12:18	06.05.2022 13:18	
Текстовый объект: Номер кредитной карты	Номер кредитной карты	06.05.2022 12:18	06.05.2022 13:18	
Текстовый объект: Номер кредитной карты (16 цифр)	Номер кредитной карты (16 цифр)	06.05.2022 12:18	06.05.2022 13:18	

Переходим, списки – теги, создаем новый тег

Создать тег

Название Политика 5

Цвет

Описание

Сохранить Отменить

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

The screenshot shows the InfoWatch Traffic Monitor Enterprise web interface. The main menu includes: Сводка, События, Отчеты, Технологии, Объекты защиты, Персоны, Политики, Списки, Управление, Краулер, Помощник, and Офицер безопасности. The title bar indicates "Вы редактируете конфигурацию с 06.05.2022 12:15." A toolbar at the top right includes: Применить, Сохранить, Сбросить, and Версия действующей конфигурации - № 9.

The main content area displays a "Политики" (Policies) section with a "Политика защиты данных #1" (Data Protection Policy #1) expanded. This policy is described as "Политика на любые данные" (Policy for all data). It includes tabs for Передача (Transfer), Копирование (Copy), Хранение (Storage), and Работа в приложениях (Work in applications).

To the right, a "Политика защиты данных #1" (Data Protection Policy #1) configuration window is open. It shows the policy name "Политика 5" and a status toggle switch set to "Все время" (All the time). A "Зашieldedные данные" (Protected data) section contains a "Выбрать" (Select) button. Below it, a note states: "Политика сработает при обнаружении хотя бы одного вхождения в каждый из типов данных." A "Каталоги объектов защиты" (Protection object catalogs) section lists "Политика 5". A detailed view of "Политика 5" shows its description field ("Описание: Введите описание"), creation date ("Создан: 06.05.2022 13:10"), and last update ("Изменен: 06.05.2022 13:19").

At the bottom right are "Сохранить" (Save) and "Отменить" (Cancel) buttons.

Правило передачи

The screenshot shows the InfoWatch Traffic Monitor Enterprise web interface with the same navigation and toolbar as the previous screenshot.

The main content area displays a "Политики" (Policies) section with a "Политика защиты данных #1" (Data Protection Policy #1) expanded. It includes tabs for Передача (Transfer), Копирование (Copy), Хранение (Storage), and Работа в приложениях (Work in applications).

To the right, a "Правило передачи" (Transfer Rule) configuration window is open. It shows the rule type "Тип" (Type) set to "Компьютеры" (Computers) with entries for "CLIENT1" and "CLIENT2". It also shows settings for "Направление маршрута" (Route direction) set to "→ В одну сторону" (→ One-way) and "В оба направления" (In both directions). Other fields include "Отправители" (Senders), "Получатели" (Recipients), "Дни действия правила" (Rule validity days), "Часы действия правила" (Rule validity hours), and "Действия при срабатывании правила" (Actions upon rule triggering).

At the bottom right are "Сохранить" (Save) and "Отменить" (Cancel) buttons.

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 center says 'Вы редактируете конфигурацию с 06.05.2022 12:15.' Below this, there are two policy configuration windows: 'Политика 5' and 'Политика 2'. The right side of the screen displays the 'Правило передачи' (Transmission Rule) configuration panel, which includes fields for 'Направление маршрута' (Route direction), 'Тип события' (Event type), 'Компьютеры' (Computers), 'Отправители' (Senders), 'Получатели' (Recipients), 'Дни действия правила' (Rule validity days), and 'Часы действия правила' (Rule validity hours). Below this is the 'Действия при срабатывании правила' (Actions upon rule trigger) section, which includes options for sending notifications, marking events as errors, setting severity levels, and assigning tags. At the bottom are 'Сохранить' (Save) and 'Отменить' (Cancel) buttons.

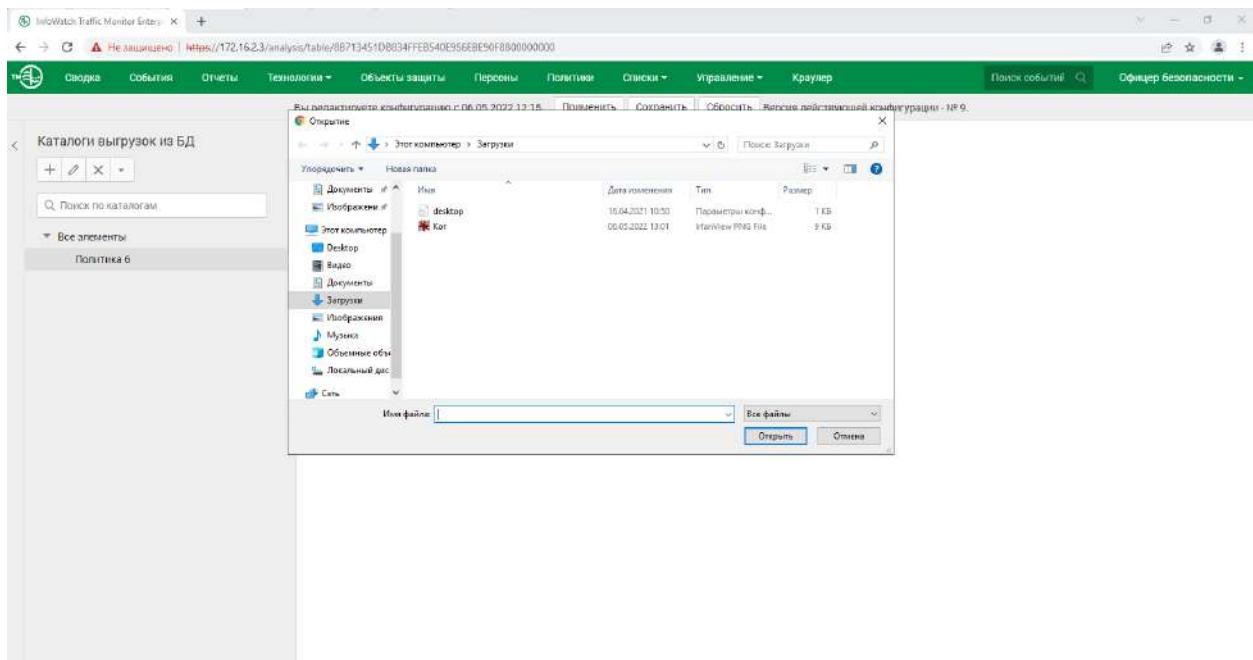
Политика 6

Переходим, технологии – выгрузки из бд

Создаем каталог

The screenshot shows the 'Каталоги выгрузок из БД' (Data Extraction Catalogs) section of the InfoWatch Traffic Monitor Enterprise interface. On the left, there is a list of existing catalogs. On the right, a 'Создать' (Create) dialog box is open, prompting for 'Название' (Name) and 'Описание' (Description). The 'Название' field is filled with 'Политика 6'. The 'Описание' field has a placeholder 'Добавить описание' (Add description). At the bottom of the dialog are 'Создать' (Create) and 'Отменить' (Cancel) buttons.

Выгрузка из БД



Дальше не знаю

Создайте каталог выгрузок «Политика З». 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...	$5 + 7 + 10 + 14 + 16 + 18$	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
<input type="button" value="Сохранить"/> <input type="button" value="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	<input type="text" value="Начните вводить текст"/> <input type="button" value="+"/>
Отправители	<input type="text" value="Начните вводить текст"/> <input type="button" value="+"/>
Получатели	<input type="text" value="Начните вводить текст"/> <input type="button" value="+"/>
Дни действия правила	Любой день недели
Часы действия правила	0:00 <input type="button" value=""/> - 0:00 <input type="button" value=""/>
Действия при срабатывании правила	
Отправить почтовое уведомление	<input type="text" value="Начните вводить текст"/> <input type="button" value="+"/>
Назначить событию вердикт	<input checked="" type="checkbox"/> Разрешить
Назначить событию уровень нарушения	<input checked="" type="radio"/> Низкий
Назначить событию теги	Политика 3 <input type="button" value="+"/>
Назначить отправителю статус	<input type="text" value="Выберите статус"/> <input type="button" value=""/>
<input type="button" value="Удалить событие"/>	

Рисунок 86 – «Правило передачи политики 3»

Модуль 4

The screenshot displays two windows of the InfoWatch Traffic Monitor application running in VMware Workstation.

Top Window: Role Creation

The main window shows the "Управление доступом" (Access Management) section. On the left, there's a tree view for "Пользователи" (Users) and "Области видимости" (Visibility Areas). The central pane lists roles: "Администратор" (Administrator) and "Офицер безопасности" (Security Officer). The right pane is titled "Создание роли" (Create Role) and shows a form with the role name "DLP" and a detailed list of permissions under "Сводка" (Summary) and "События" (Events). The "Сводка" section includes checkboxes for "Редактирование запросов" (Edit queries) and "Удаление запросов" (Delete queries). The "События" section includes checkboxes for "Выполнение запросов и просмотр событий" (Execute queries and view events), "Выгрузка событий" (Export events), and "Изменение ролей пользователя" (Change user role).

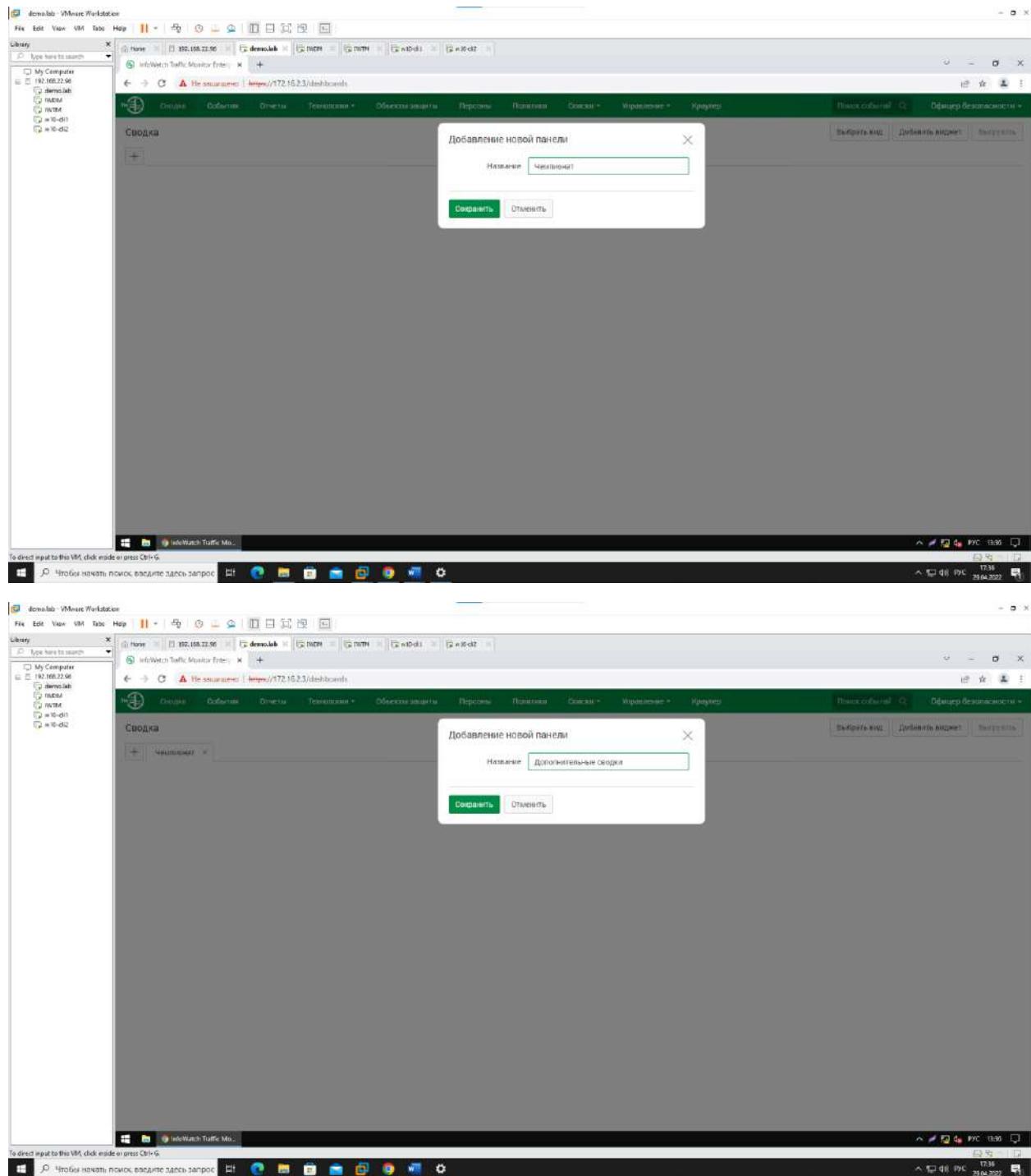
Bottom Window: User Creation

This window also shows the "Управление доступом" section. It lists users: "iwm-officer" (iwm-officer), "admin" (admin), and "officer" (officer). The right pane is titled "Создание пользователя" (Create User) and shows a form for creating a new user named "DLP@main.ru". The "Статус" (Status) dropdown is set to "Активен" (Active). A modal dialog titled "Выбор роли (1)" (Select Role (1)) is open, listing "iwm-officer" and "admin" as available roles. Both checkboxes are checked, and the "DLP" role is selected. The "Сохранить" (Save) button is highlighted.

The screenshot shows the InfoWatch Traffic Monitor interface within a VMware Workstation window. The main window displays a list of users under 'Управление доступом' (Access Management). The columns include 'Логин' (Login), 'Назначение' (Assignment), 'Email', 'Роль' (Role), and 'Области видимости' (Visibility Scope). Three users are listed: 'iwtm-officer' (iwtm-officer@info.ru, iwtm-officer, Администратор ИР Полный доступ), 'administrator' (Администратор, Администратор, Представитель), and 'officer' (Офицер безопасности, Администратор Полный доступ Представитель). On the right side, there is a 'Создание пользователя' (Create User) form with fields for 'Логин' (DLP-user), 'Статус' (Активен), 'Email' (DLP@mail.ru), 'Пароль' (DLP-X), 'Подтверждение пароля' (DLP-X), and 'Описание' (Описание). Buttons for 'Сохранить' (Save) and 'Отменить' (Cancel) are at the bottom.

Удаляем все сводки

The screenshot shows the InfoWatch Traffic Monitor interface within a VMware Workstation window. The main window displays a dashboard section titled 'Сводка' (Summary). It includes four cards: 'Динамика нарушений за период' (Incident dynamics over period), 'Топ нарушителей' (Top offenders), 'Динамика статусов за период' (Status dynamics over period), and 'Статистика по каталогам объектов защиты' (Statistics by protection object catalogs). Each card has a date range selector (e.g., 23.04.2022 - 29.04.2022). At the bottom of the dashboard, there are buttons for 'Выбрать виджет' (Select widget), 'Добавить виджет' (Add widget), and 'Выгрузить' (Export).



Добавляем подборку

Выберите тип статистики

Топ нарушителей
Показывает топ нарушителей в соответствии с выбранной группой для выбранного временного интервала
Добавить виджет

Количество нарушений за период
Для каждого типа нарушений (передачи, приемки, копирования из системы, использования буфера обмена) отображается количество нарушений высокого среднего, низкого уровня за выбранный пользователем период
Добавить виджет

Подборка
Показывает события для выбранной подборки
Добавить виджет

Динамика статусов за период
Показывает динамику статусов для выбранного периода времени
Добавить виджет

Подборка

Для виджета не указан запрос

Статистика по политикам

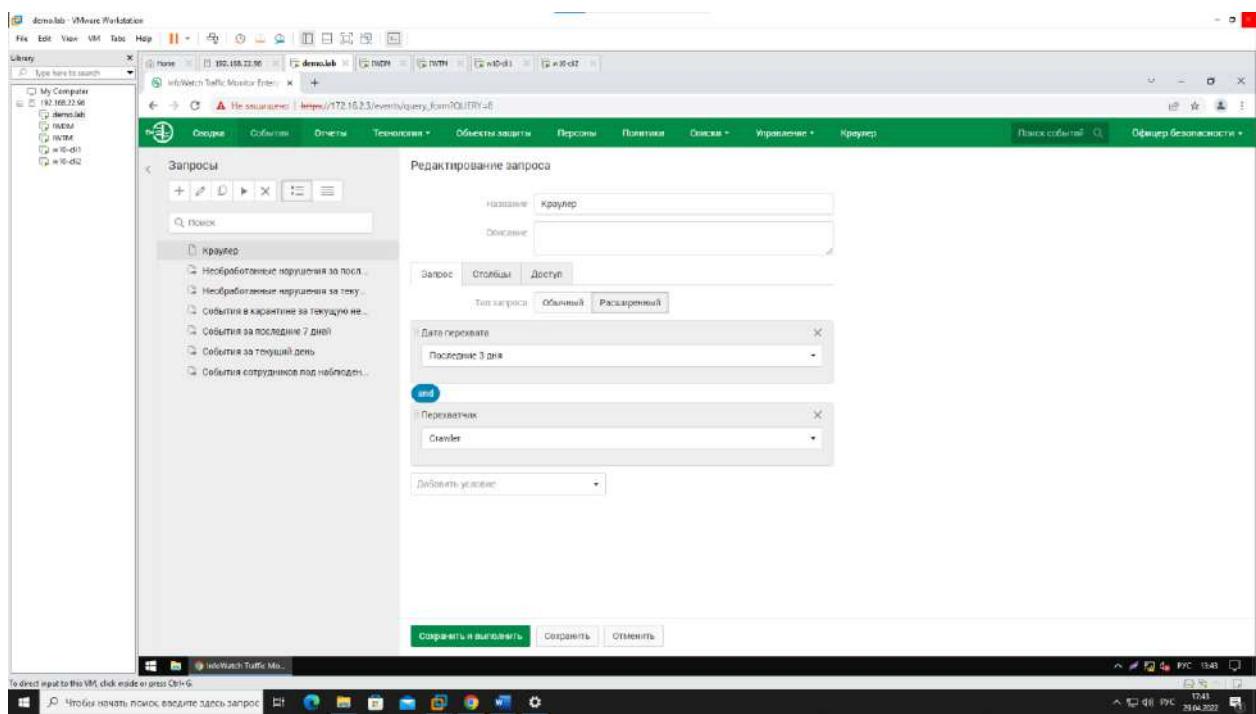
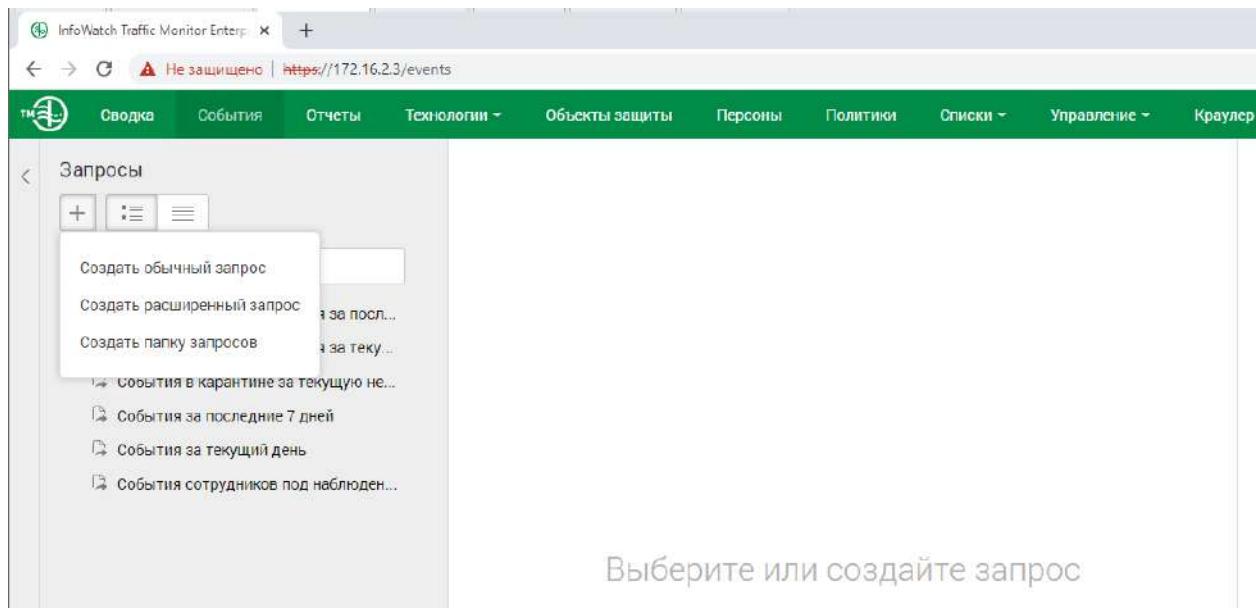
Политика

29.04.2022 - 29.04.2022

Топ нарушителей

без учета правил

29.04.2022 - 29.04.2022



Добавляем условие – технологии

Выбор результатов анализа

Категория	Заданные документы	Бланки	Текстовые объекты	Печати	Выгружен из БД	Графические объекты
Поиск						
Краупер						
<input checked="" type="checkbox"/> Несоблюдение нормативов						
<input checked="" type="checkbox"/> Кредитная карта						
<input checked="" type="checkbox"/> Паспорт гражданина РФ						

Сохранить Отменить

Создание запроса

Название: Новый запрос

Описание:

Запрос: Ошибки Доступ

Тип запроса: Обычный Расширенный

Фильтр: Кредитная карта AND Паспорт гражданина РФ

Изменения:

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

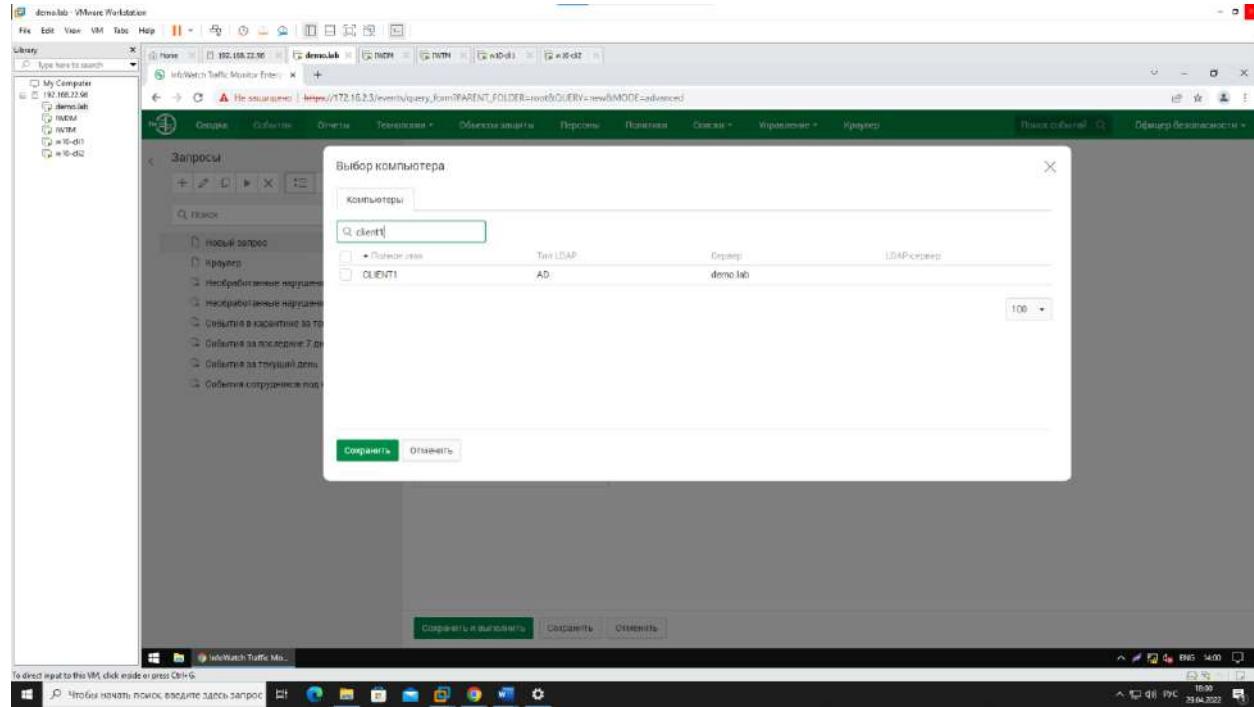
Название:	Статистика по политикам
Интервал обновления:	Не обновлять ▾
Период:	Текущий месяц ▾
Политики:	Начните вводить текст <input type="text"/> +
Сохранить Отменить	

Общие настройки виджета

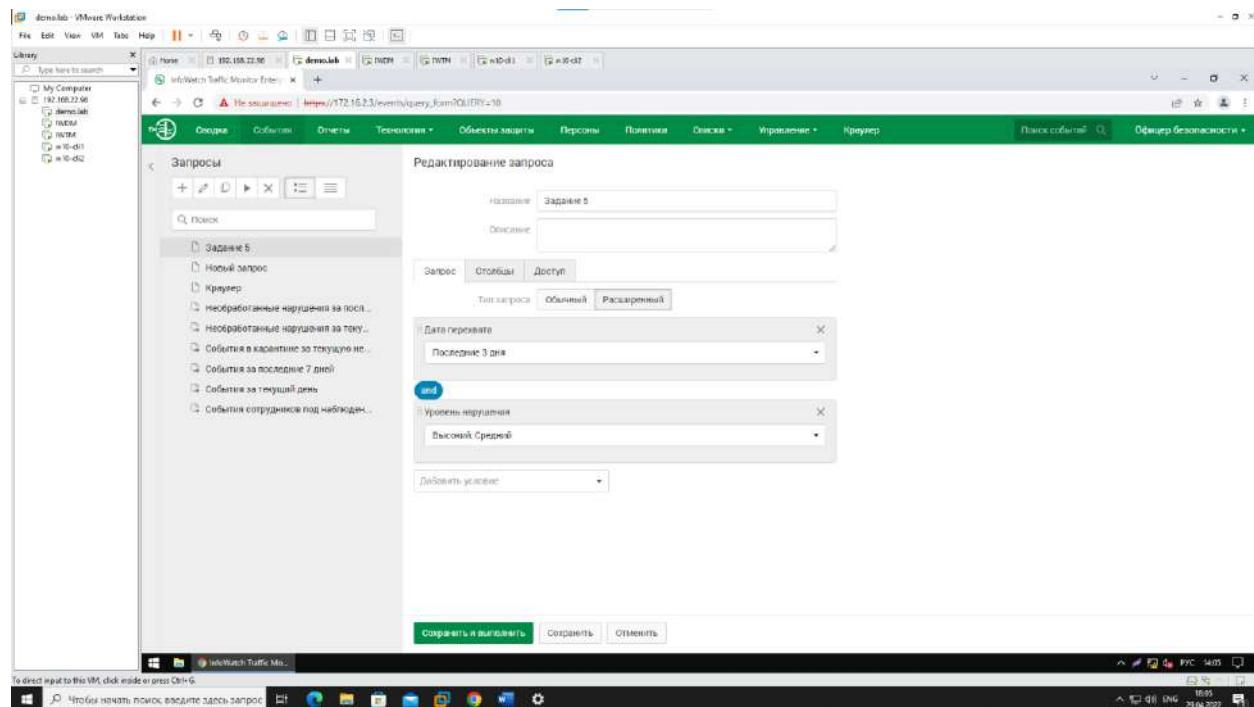
Название:	Топ нарушителей
Интервал обновления:	Не обновлять ▾
Период:	Последние 30 дней ▾
Количество нарушителей:	10 ▲ ▼
Группы:	Введите название группы <input type="text"/> +
Статусы:	Выберите статус <input type="text"/> +
Сохранить Отменить	

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 × ▾
Событий на странице	▲ ▾

Сохранить Отменить

Задание 4

Дополнительные сводки

Общие настройки виджета

Название	Высокий уровень угрозы на копирования
Интервал обновления:	Не обновлять ▾
Подборка	Задание 4 × ▾
Событий на странице	▲ ▾

Сохранить Отменить

