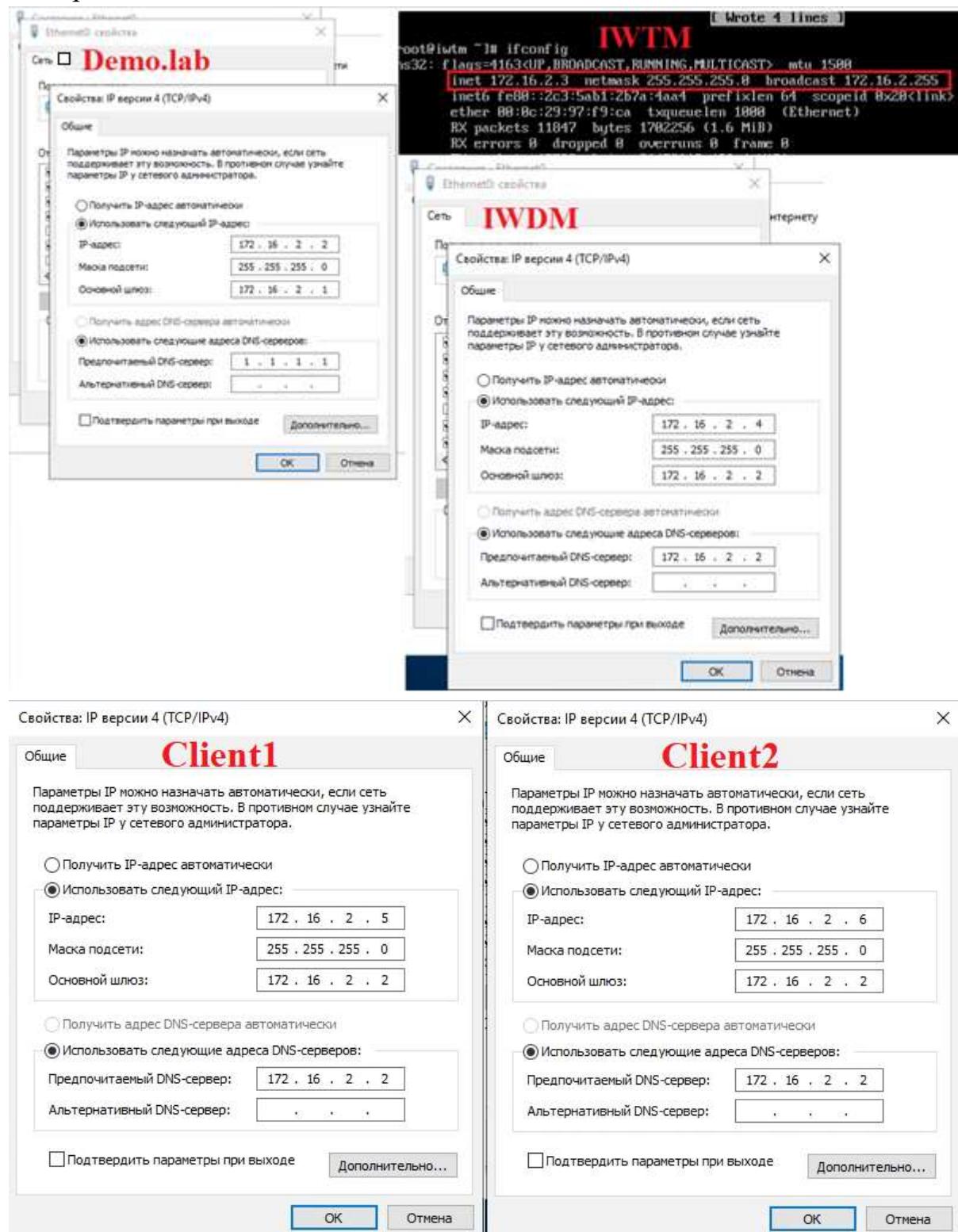


IP-адреса Demo.lab, IWTM, IWDM, Client1, Client2



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 two windows of the Active Directory Users and Computers snap-in. The top window displays a list of objects under the 'Champ' container in the 'demo.lab' domain. The bottom window shows the properties of the 'iw-admin' user object, specifically the 'Member of groups' tab, where the 'Administrators' group is selected.

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

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.

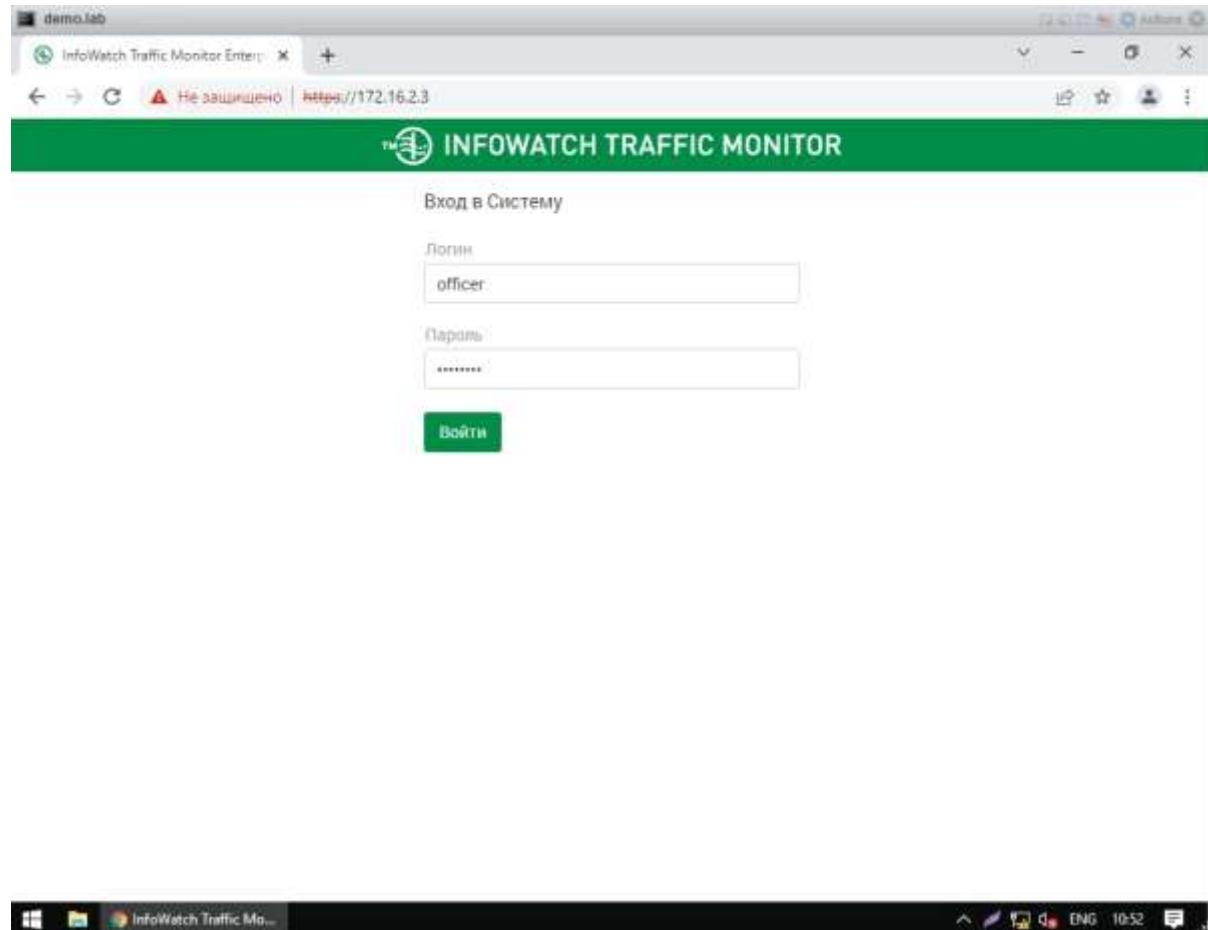
Для входа в веб-консоль необходимо настроить использование ранее созданного пользователя домена iwtm-officer с полными правами офицера безопасности и на администрирование системы, полный доступ на все области видимости.

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

172.16.2.3

LDAP-серверы

+ | Edit | X | ▾

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						
Пользователи								
Роль		Полим		Название	Email	Роли	Области видим.	Описание
<input type="checkbox"/>	<input checked="" type="radio"/> iv-admin	<input type="checkbox"/>	<input checked="" type="radio"/> iv-admin	iv-admin	231@mail.ru	Администратор, VIP; Полный дос		
<input type="checkbox"/>	<input checked="" type="radio"/> ivtm-officer	<input type="checkbox"/>	<input checked="" type="radio"/> ivtm-officer	ivtm-officer	23@mail.ru	Администратор, VIP; Полный дос		
<input type="checkbox"/>	<input checked="" type="radio"/> administrator	<input type="checkbox"/>	<input checked="" type="radio"/> Администратор			Администратор	Предустановлен	
<input type="checkbox"/>	<input checked="" type="radio"/> officer	<input type="checkbox"/>	<input checked="" type="radio"/> Офицер безопас			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 xxXX1234.

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

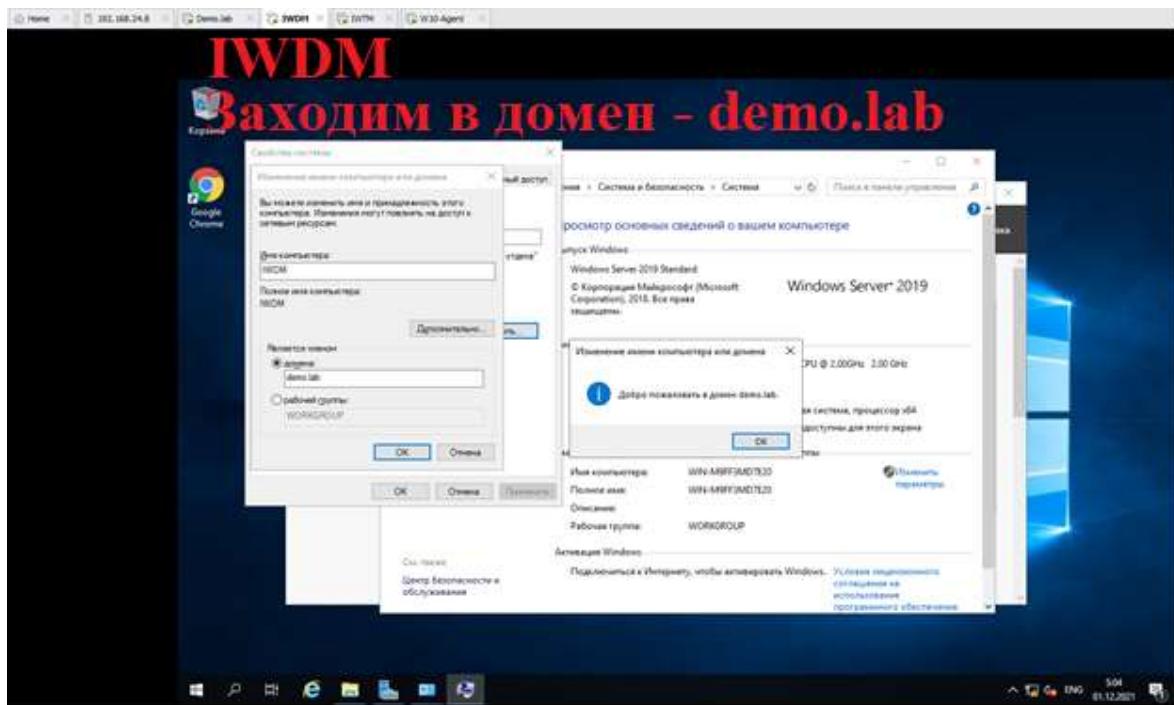
При установке сервера агентского мониторинга необходимо установить соединение с DLP-сервером по IP-адресу и токену, но можно сделать это и после установки. При установке настроить локального пользователя консоли

управления: officer с паролем xxXX1234

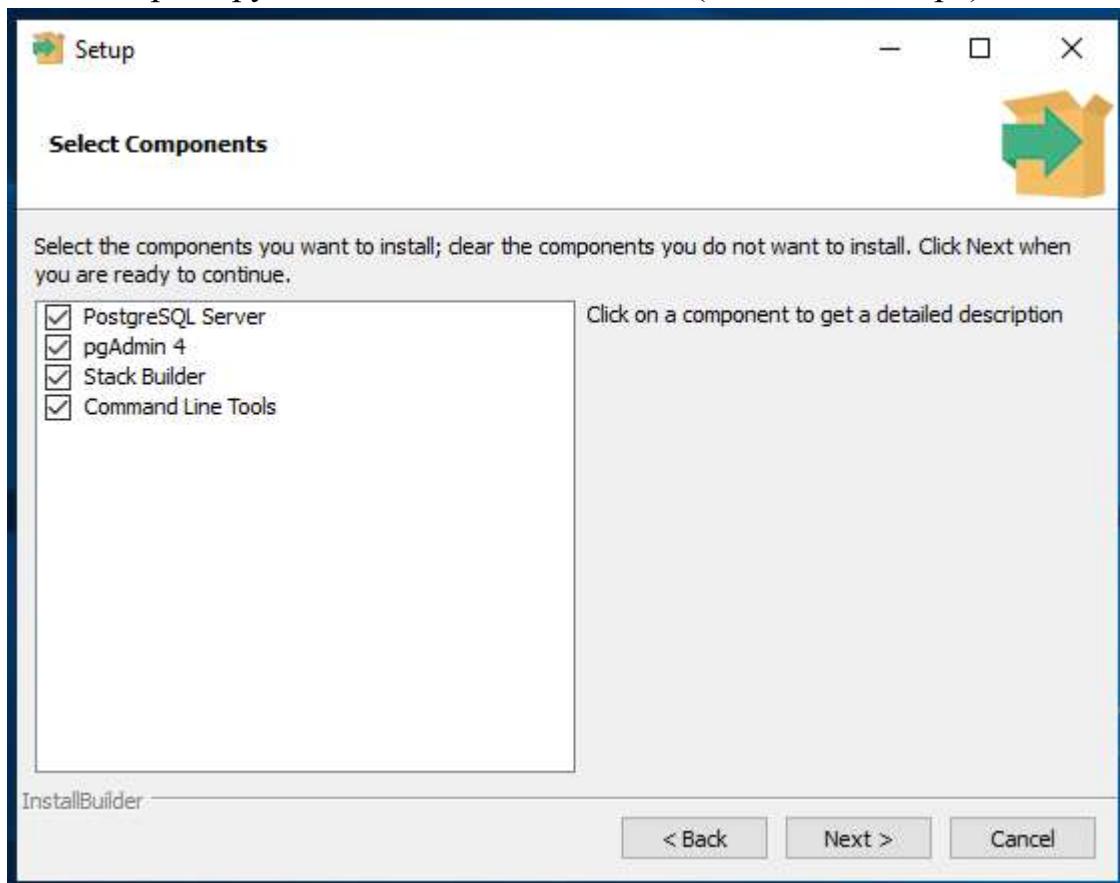
Синхронизировать каталог пользователей и компьютеров с Active Directory.

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

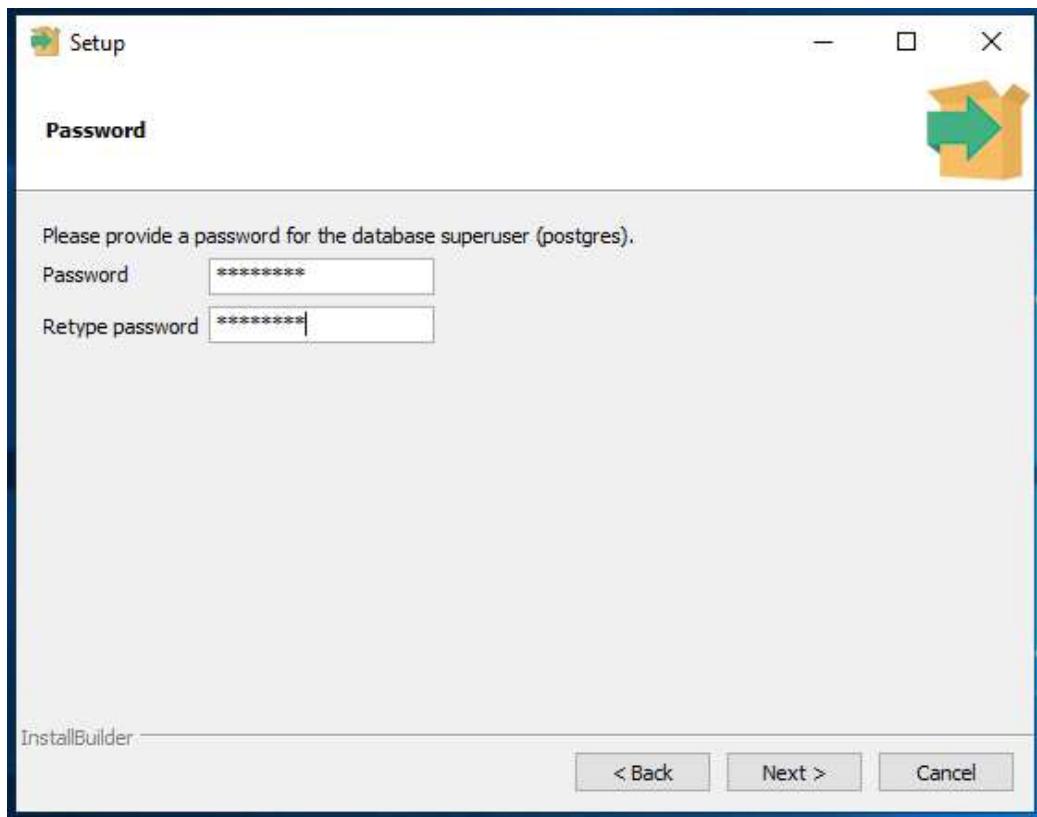
Проверить работоспособность входа в консоль управления без ввода пароля. Если сервер не введен в домен или работает от другого пользователя, данная опция работать не будет.



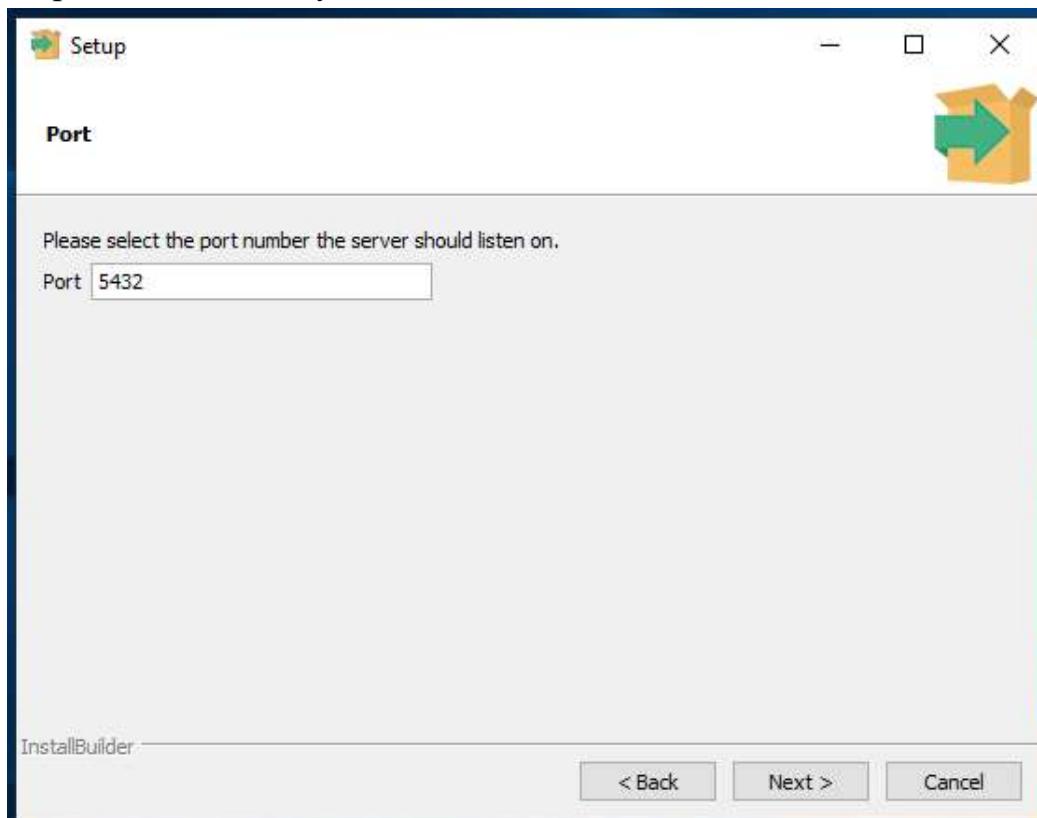
После перезагрузки заходим под iw-admin (без стак билдера)



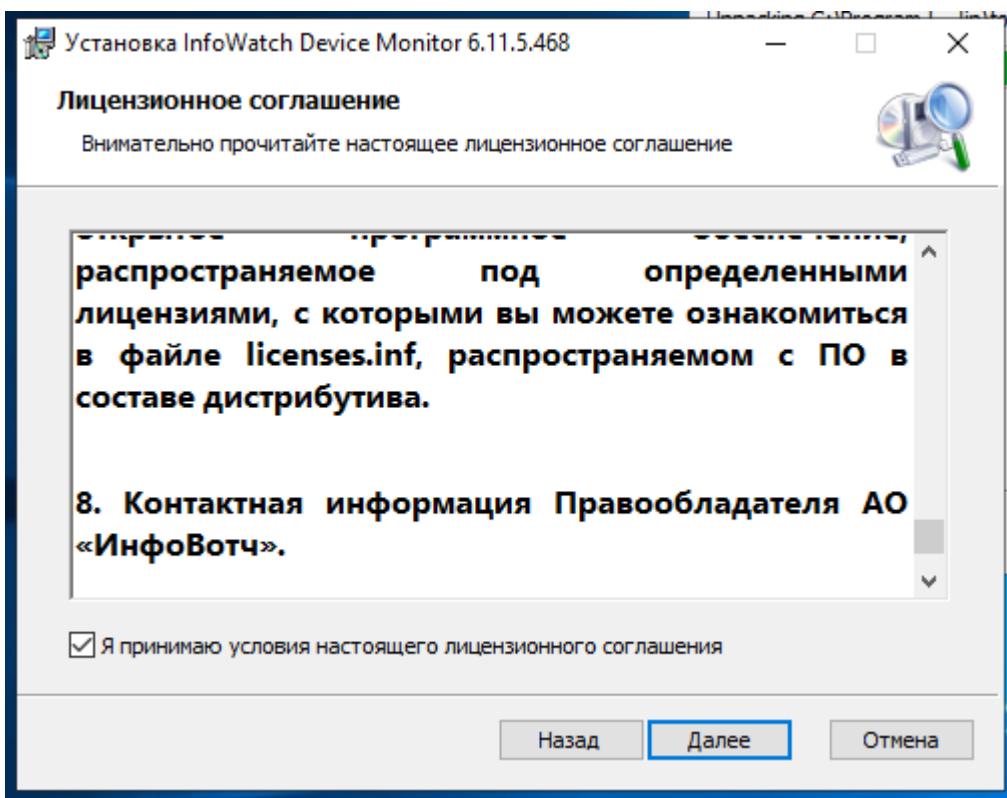
Вводим стандартный пароль



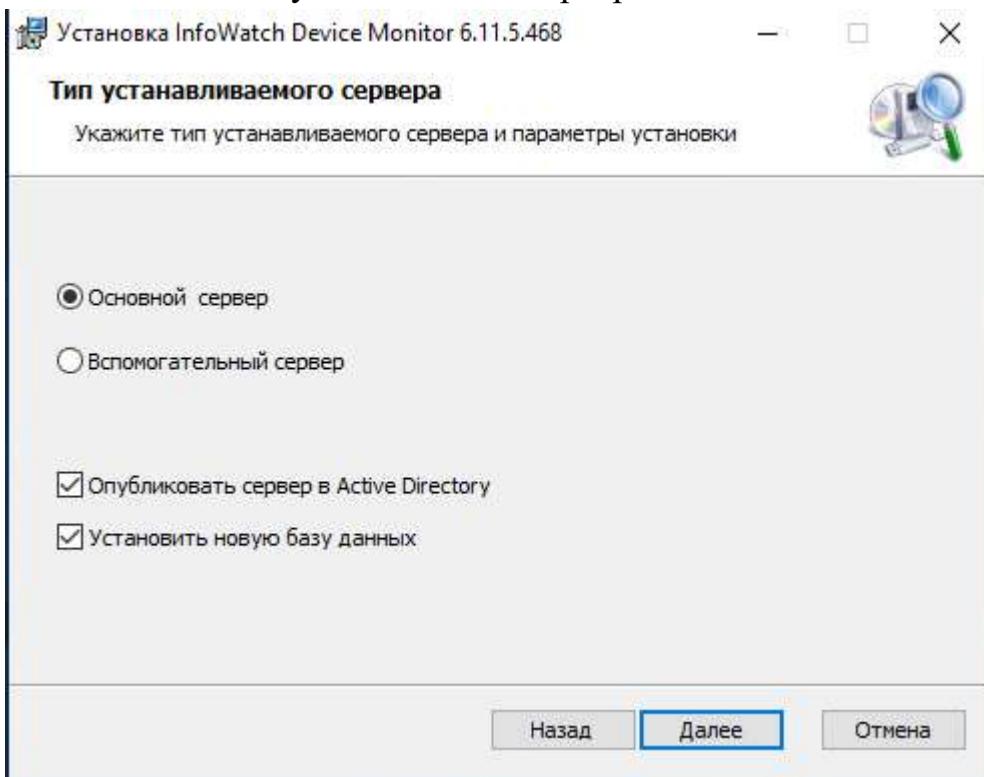
Порт оставляем по умолчанию

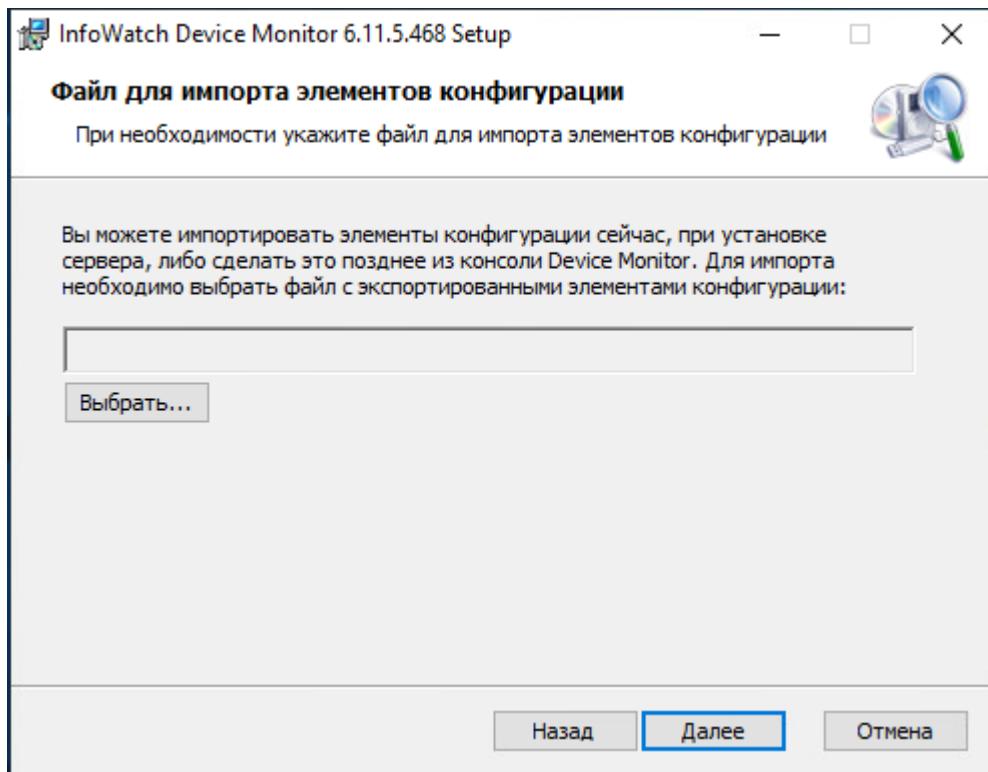


Затем, переходим к установке InfoWatch Device Monitor

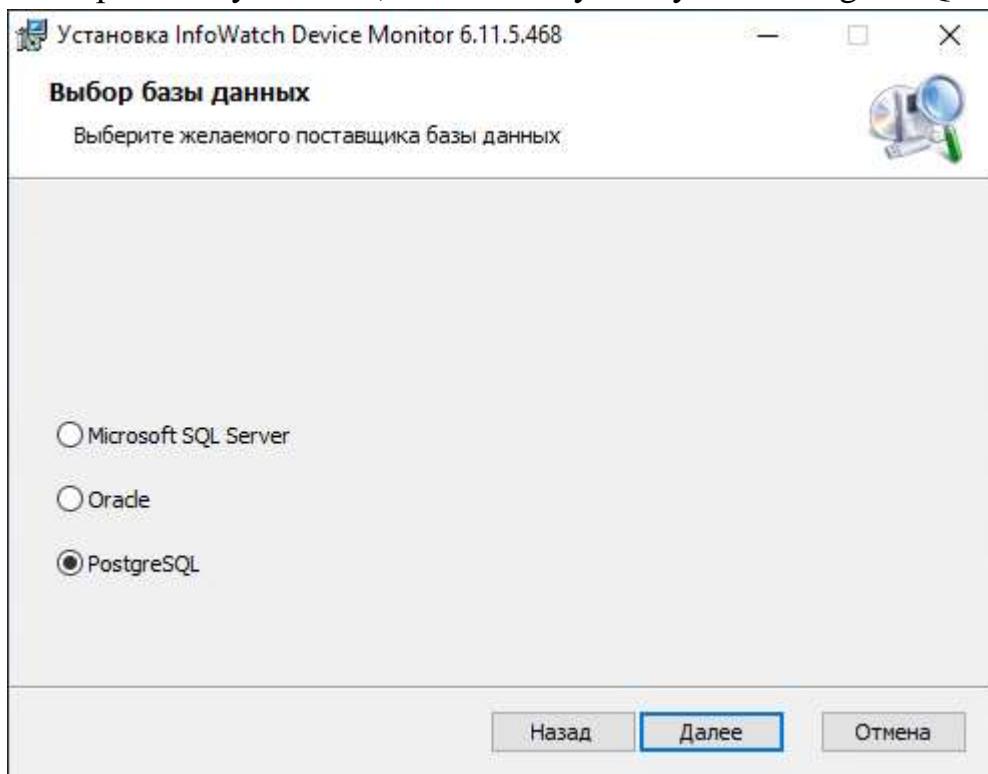


Оставляем галочку на основном сервере

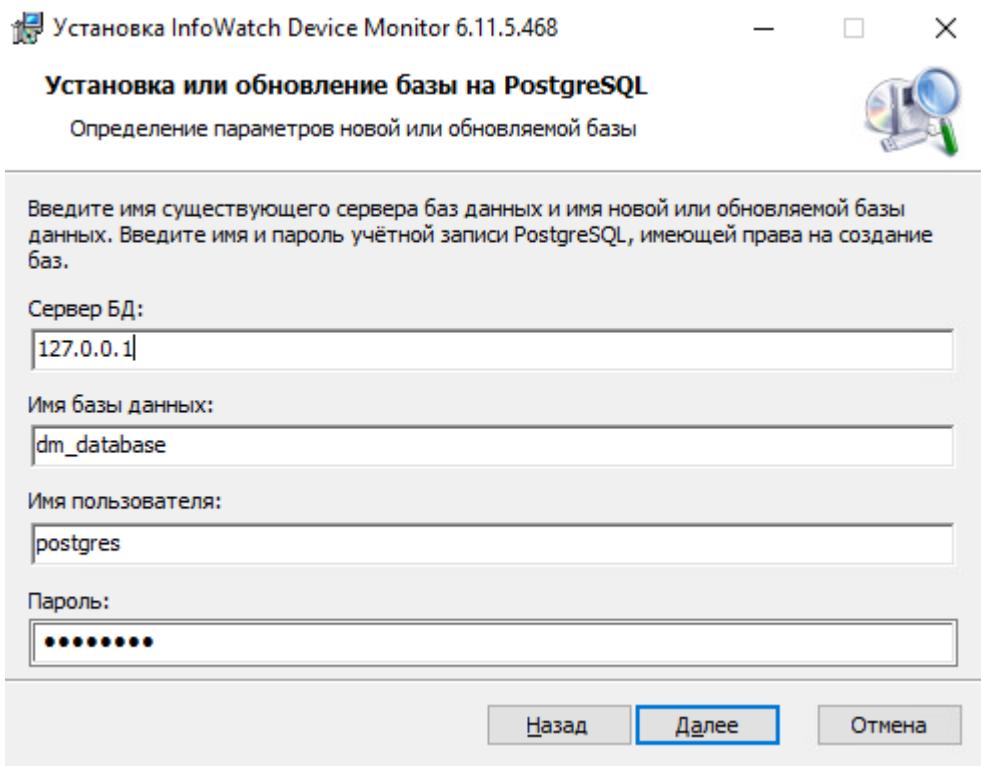




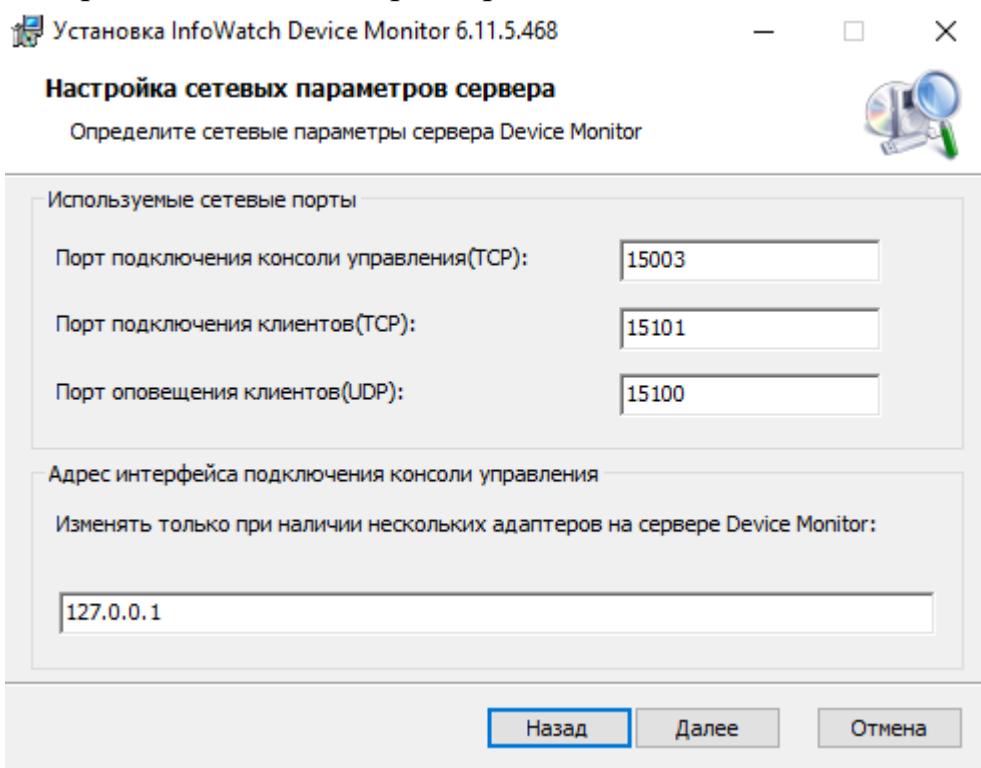
Выбираем базу данных, в нашем случае будет - PostgreSQL



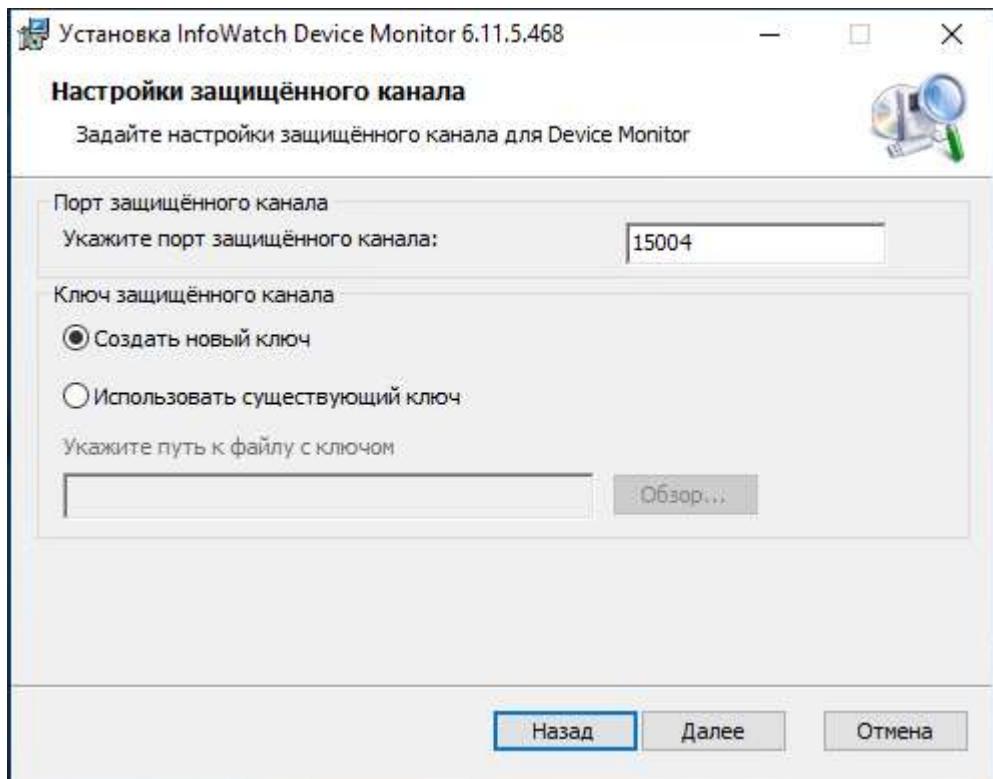
Задаем сервер БД – 127.0.0.1; Имя БД – dm_database, имя пользователя – postgres и стандартный пароль



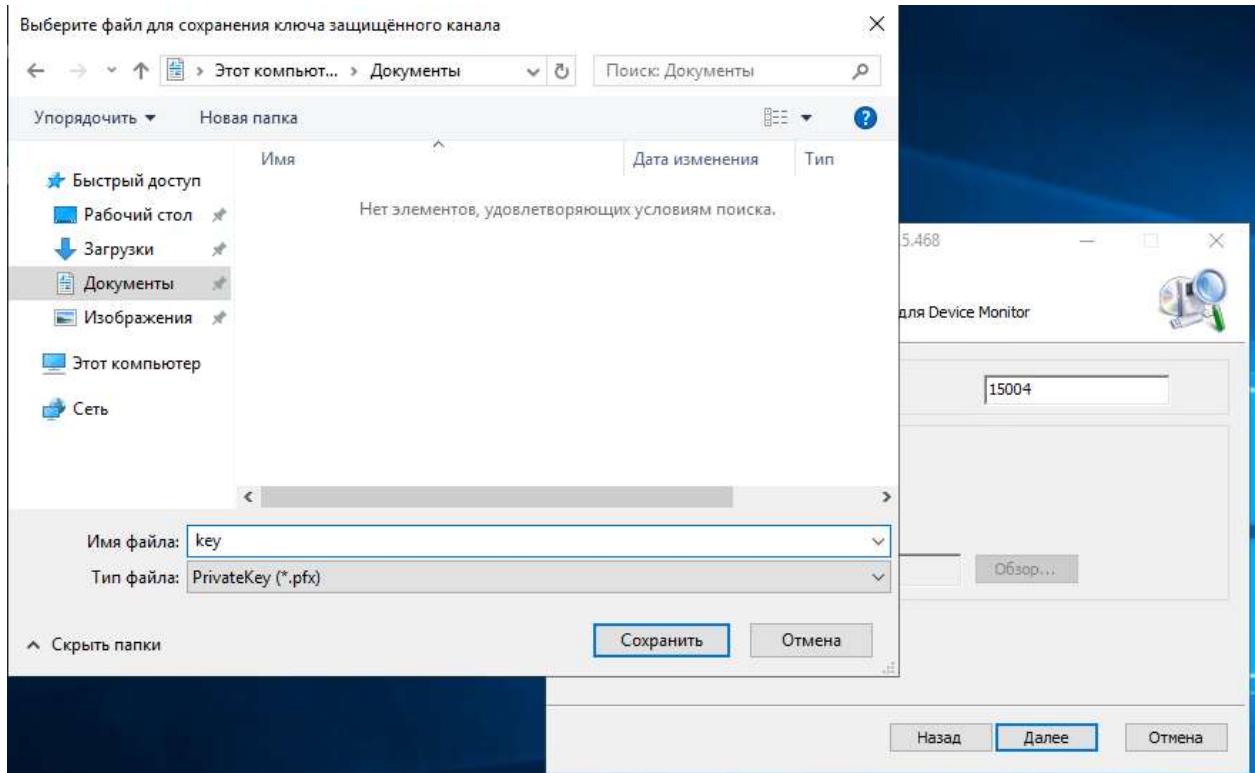
Настраиваем сетевые параметры



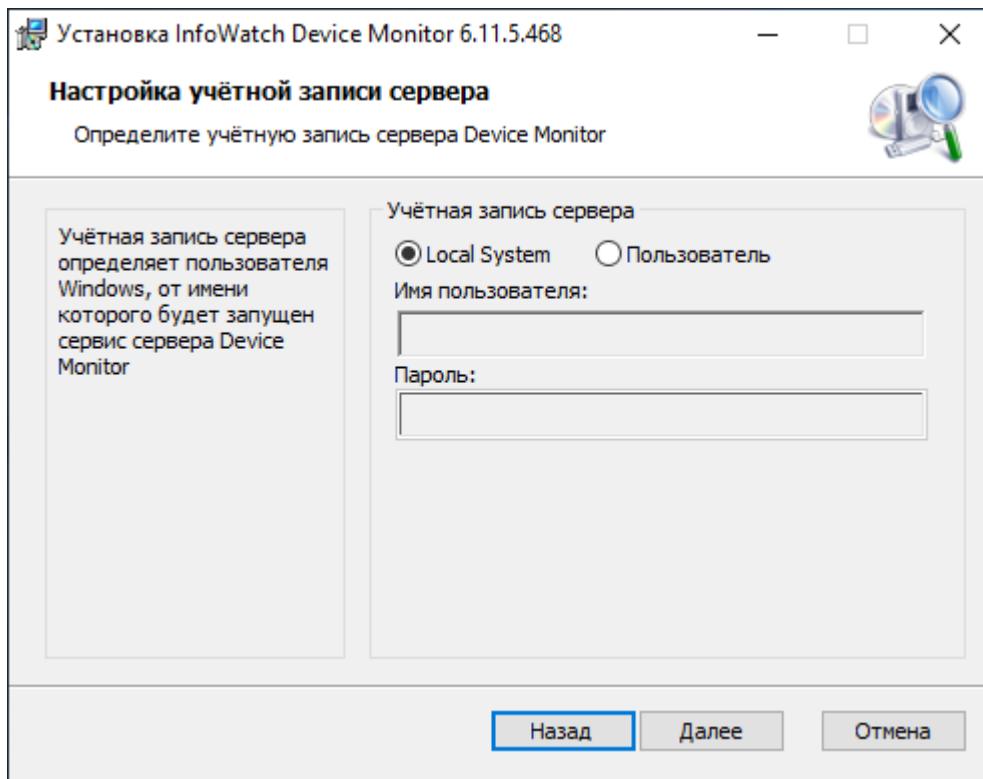
Настраиваем защищённый канал и создаём новый ключ



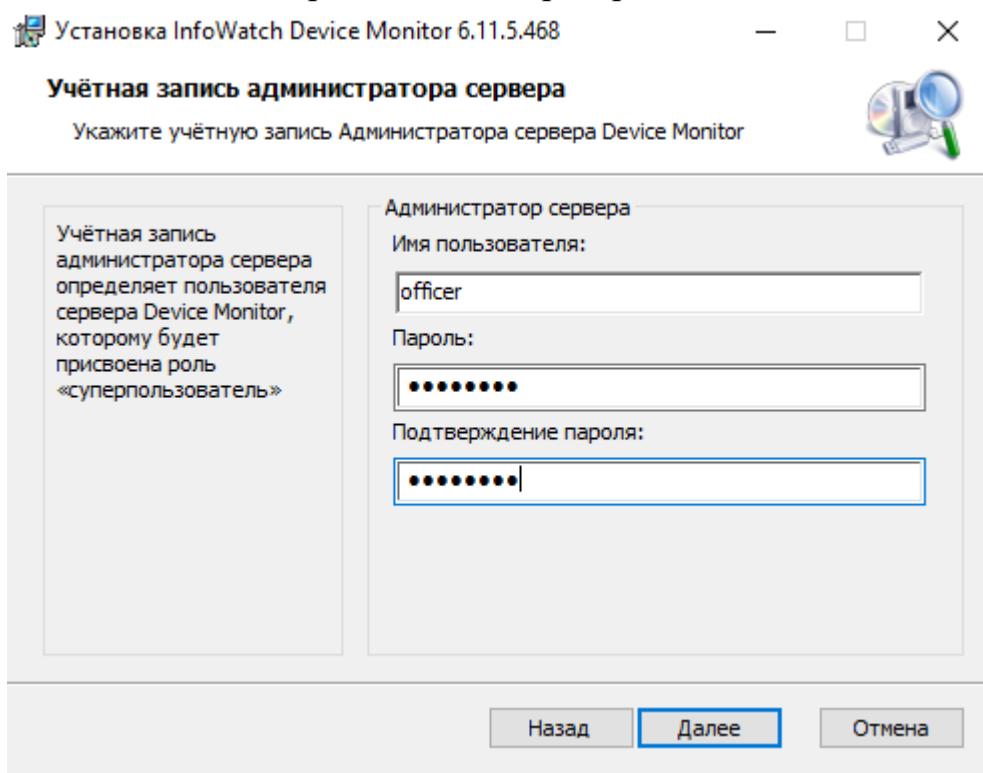
Сохраняем ключ



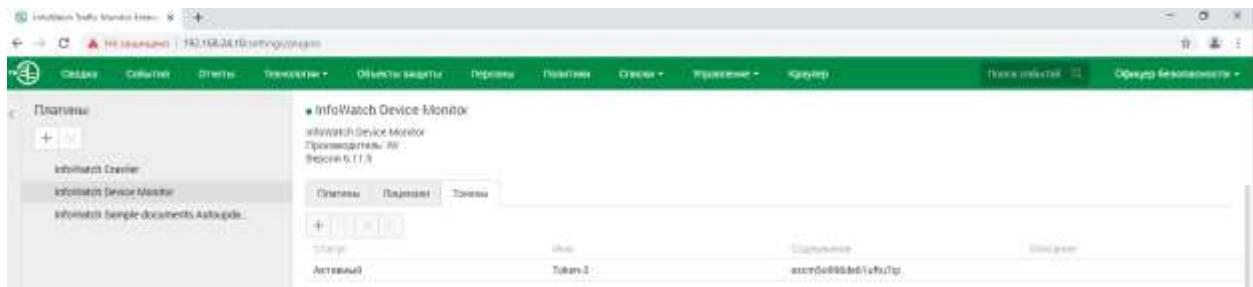
Оставляем локальную учётную запись



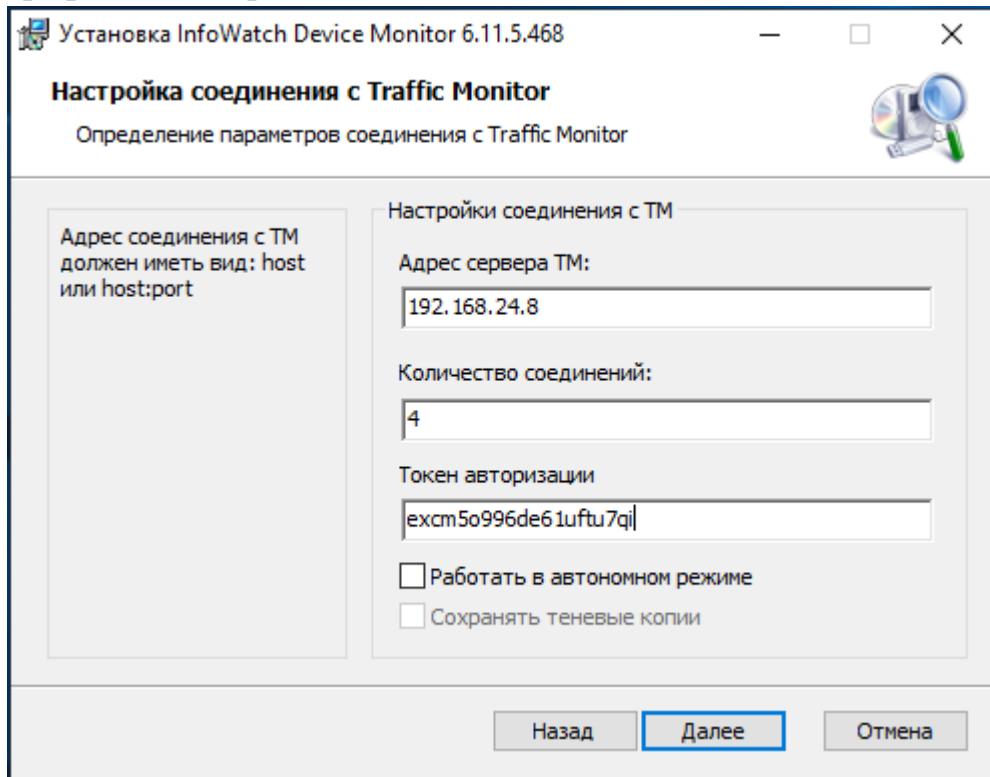
Вводим логин и пароль администратора



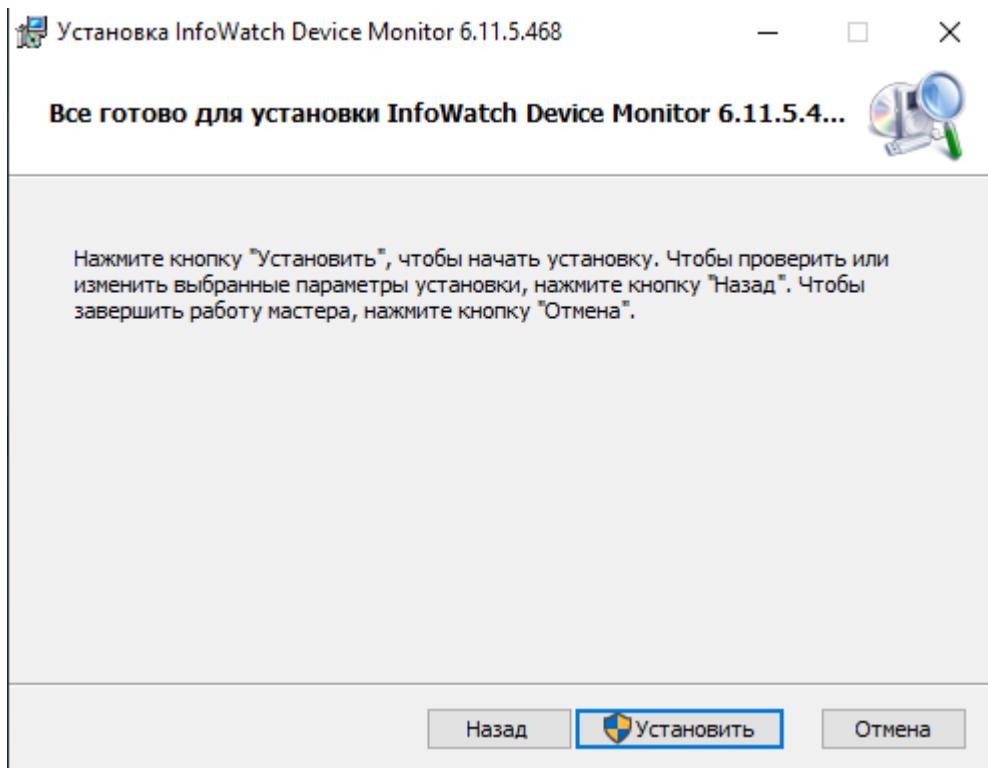
Сморим токен



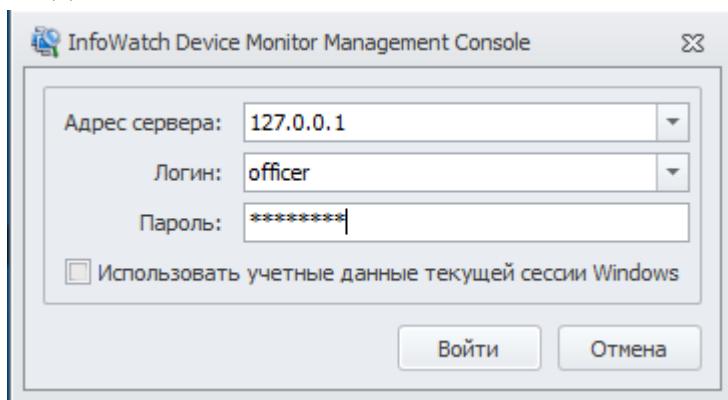
Указываем Ip-адрес IWTM и токен (который только что посмотрели в трафик мониторе)



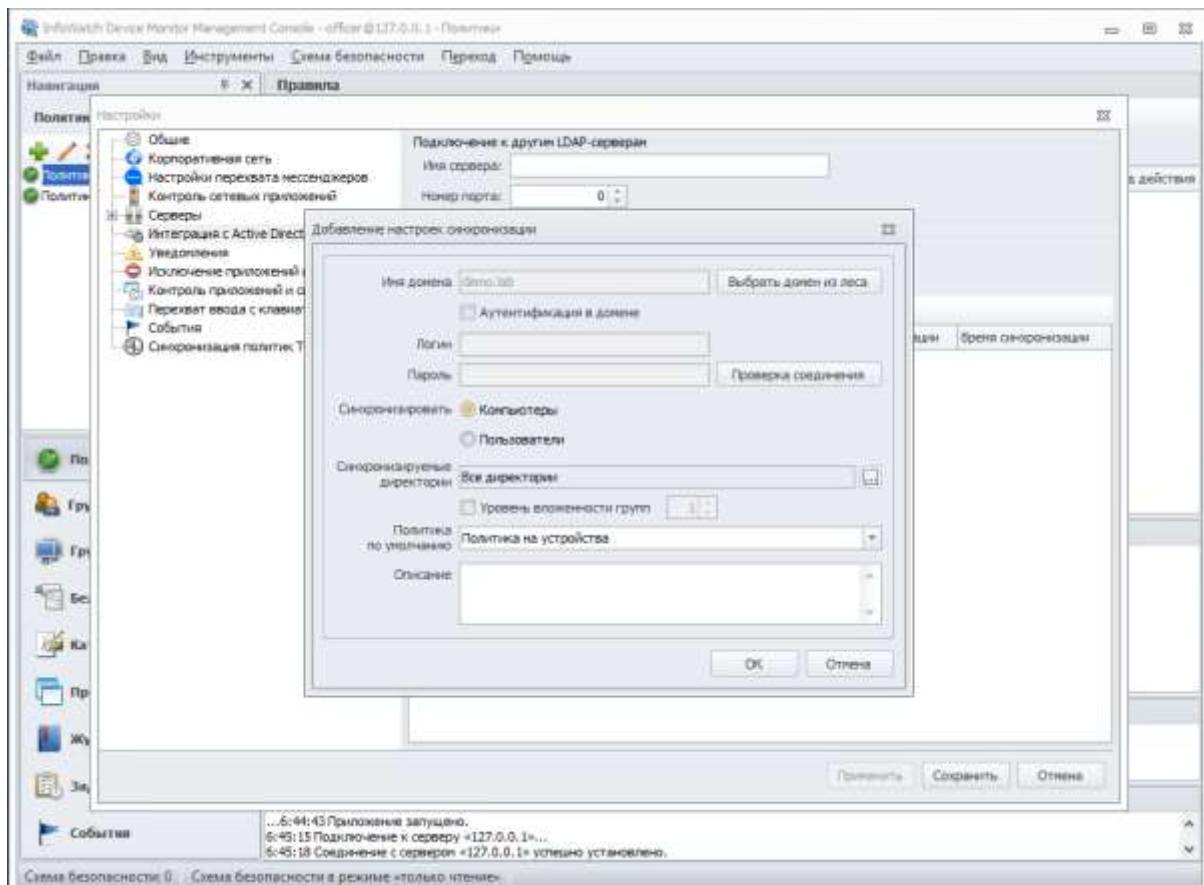
Устанавливаем



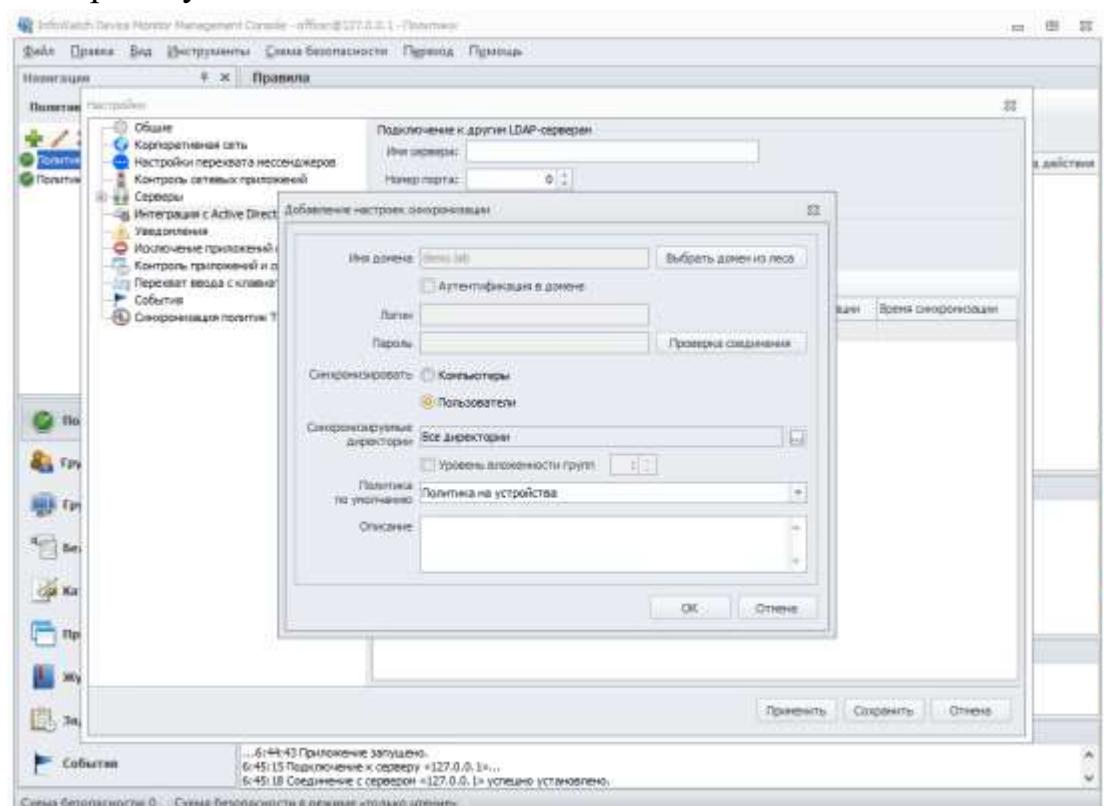
Подключаемся к InfoWatch Device Monitor Management Console



Синхронизуем компьютеры



Синхронизуем пользователей



Указываем Ip-адрес сервера demo.lab и порт

Синхронизация у компьютеров и пользователей

InfoWatch Device Monitor Management Console - officer@127.0.0.1 - Группы компьютеров

Файл Помощь Использование Справка Помощь Помощь

Настройки

Группы

Серверы

Интеграция с Active Directory

Уведомления

Исключение приложений из перехвата

Контроль приложений и снимки экрана

Перехват ввода с клавиатуры

События

Синхронизация политик Traffic Monitor

Подключение к другим LDAP-серверам

Имя сервера: 172.16.2.2

Номер порта: 389

Настройки синхронизации

Период синхронизации: 60 МИН.

+ ⌂ ⌂ ✎ ✎ ✎

Домен	Синхронизировать	Директории	Статус синхронизации	Время синхронизации
demo.lab	Компьютеры	Все директории	Успешно	14.04.2022 10:59:16
demo.lab	Пользователи	Все директории	Успешно	14.04.2022 10:59:16

Применить Сохранить Отмена

The screenshot shows the 'Integrations' settings for Active Directory. The connection is set to '172.16.2.2' on port '389'. The synchronization period is set to '60 МИН.' (60 minutes). The synchronization status table shows two entries for the domain 'demo.lab': 'Компьютеры' (Computers) and 'Пользователи' (Users), both with a status of 'Успешно' (Successful) at the time '14.04.2022 10:59:16'.

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

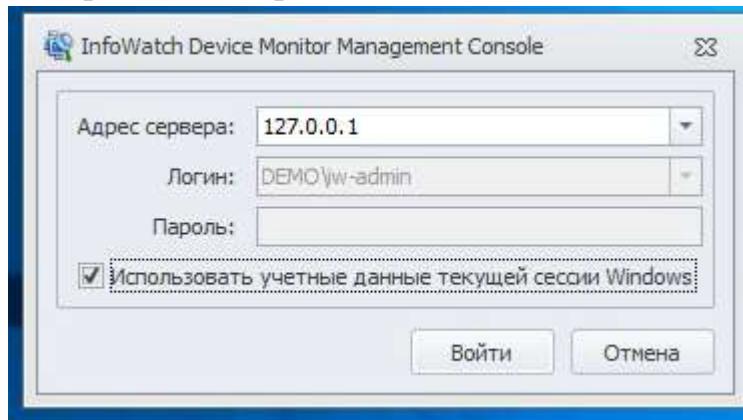
Офицер безопасности	Выбрать
Администратор	Удалить

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

Свойства: IP версии 4 (TCP/IPv4)

Общие

Параметры IP можно назначать автоматически, если сеть поддерживает эту возможность. В противном случае узнайте параметры IP у сетевого администратора.

Получить IP-адрес автоматически

Использовать следующий IP-адрес:

IP-адрес:

172 . 16 . 2 . 5

Маска подсети:

255 . 255 . 255 . 0

Основной шлюз:

172 . 16 . 2 . 2

Получить адрес DNS-сервера автоматически

Использовать следующие адреса DNS-серверов:

Предпочитаемый DNS-сервер:

172 . 16 . 2 . 2

Альтернативный DNS-сервер:

. . .

Подтвердить параметры при выходе

[Дополнительно...](#)

OK

Отмена

Клиент2

Свойства: IP версии 4 (TCP/IPv4)

Общие

Параметры IP можно назначать автоматически, если сеть поддерживает эту возможность. В противном случае узнайте параметры IP у сетевого администратора.

Получить IP-адрес автоматически

Использовать следующий IP-адрес:

IP-адрес:

172 . 16 . 2 . 6

Маска подсети:

255 . 255 . 255 . 0

Основной шлюз:

172 . 16 . 2 . 2

Получить адрес DNS-сервера автоматически

Использовать следующие адреса DNS-серверов:

Предпочитаемый DNS-сервер:

172 . 16 . 2 . 2

Альтернативный DNS-сервер:

. . .

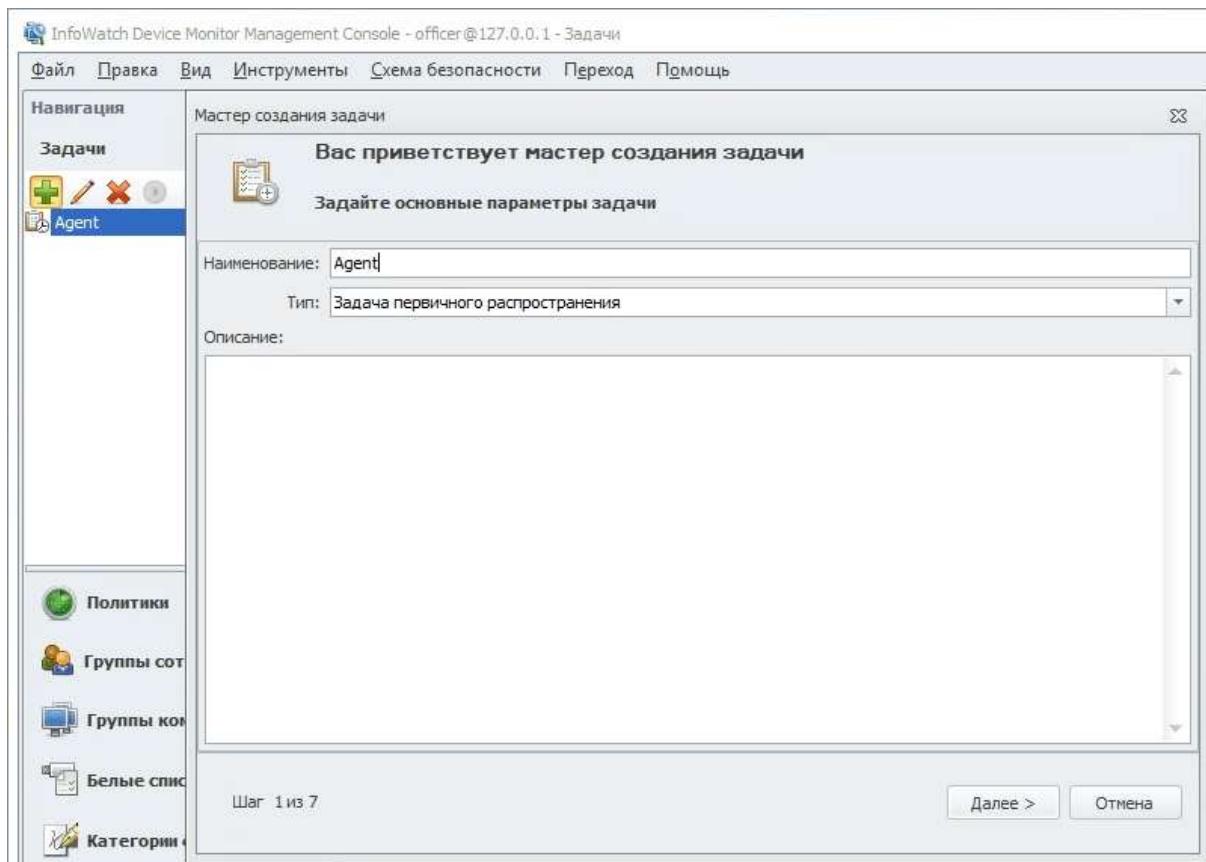
Подтвердить параметры при выходе

[Дополнительно...](#)

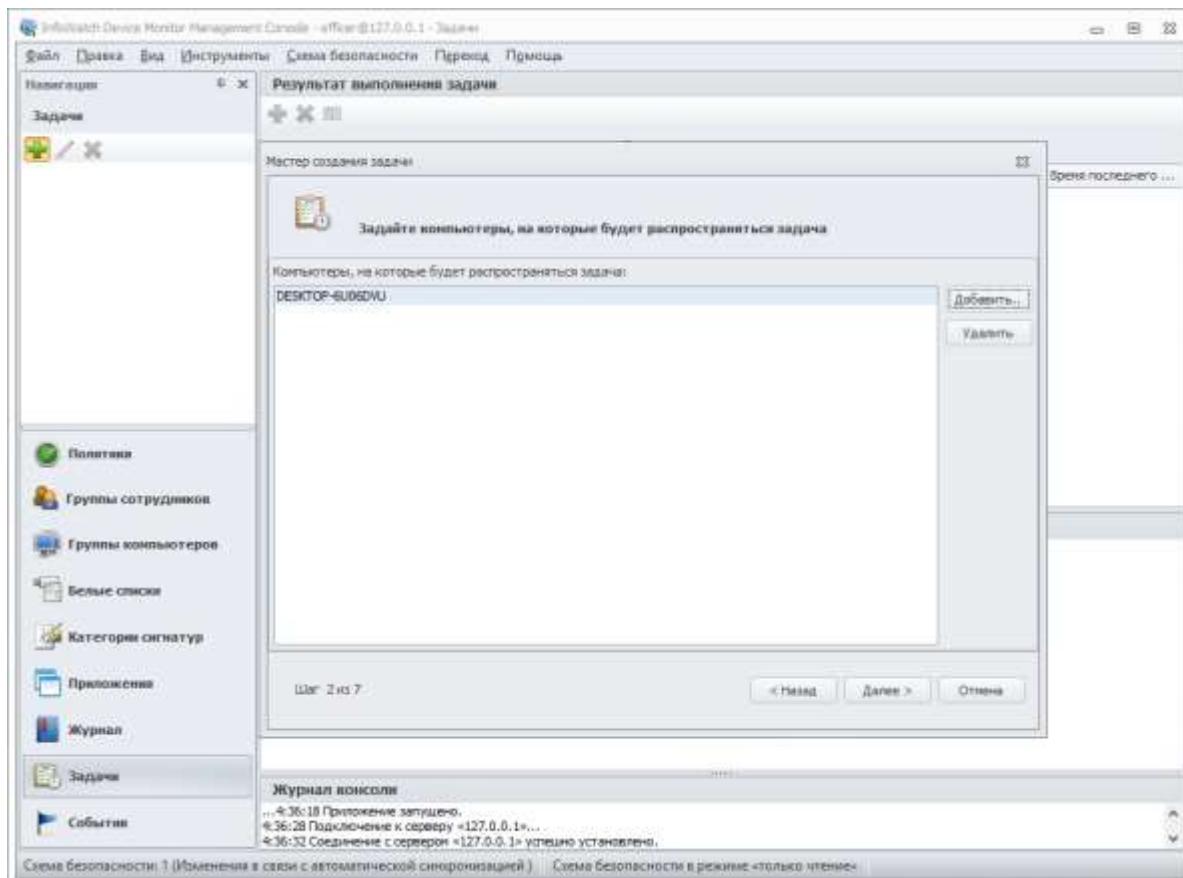
OK

Отмена

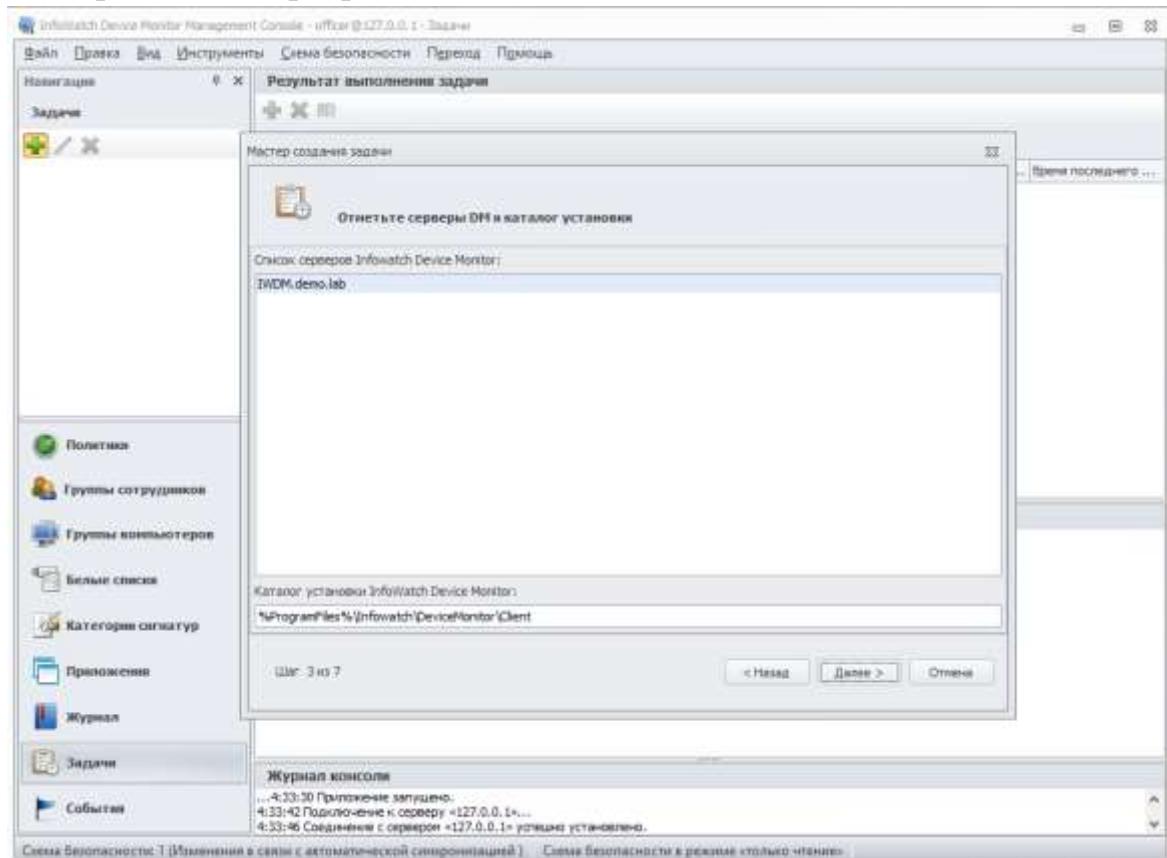
Создаем новую задачу

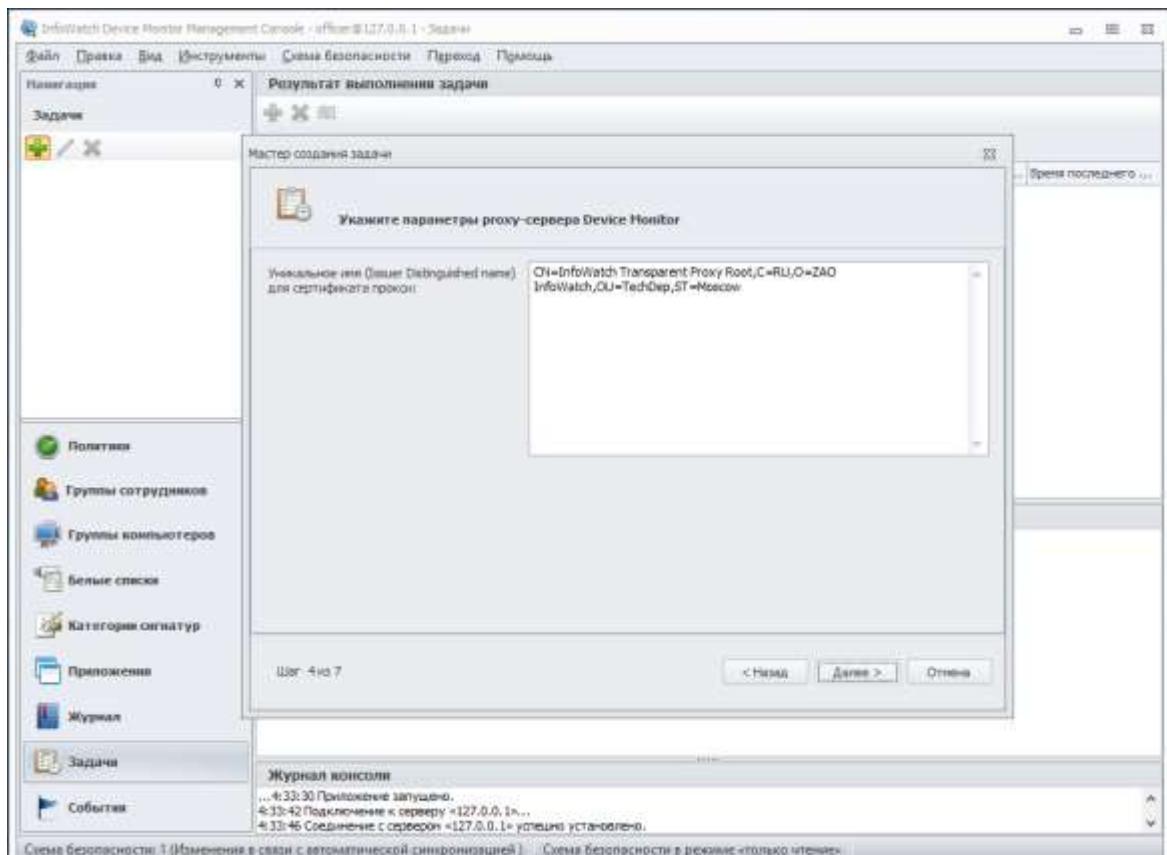


Выбираем компьютер агента

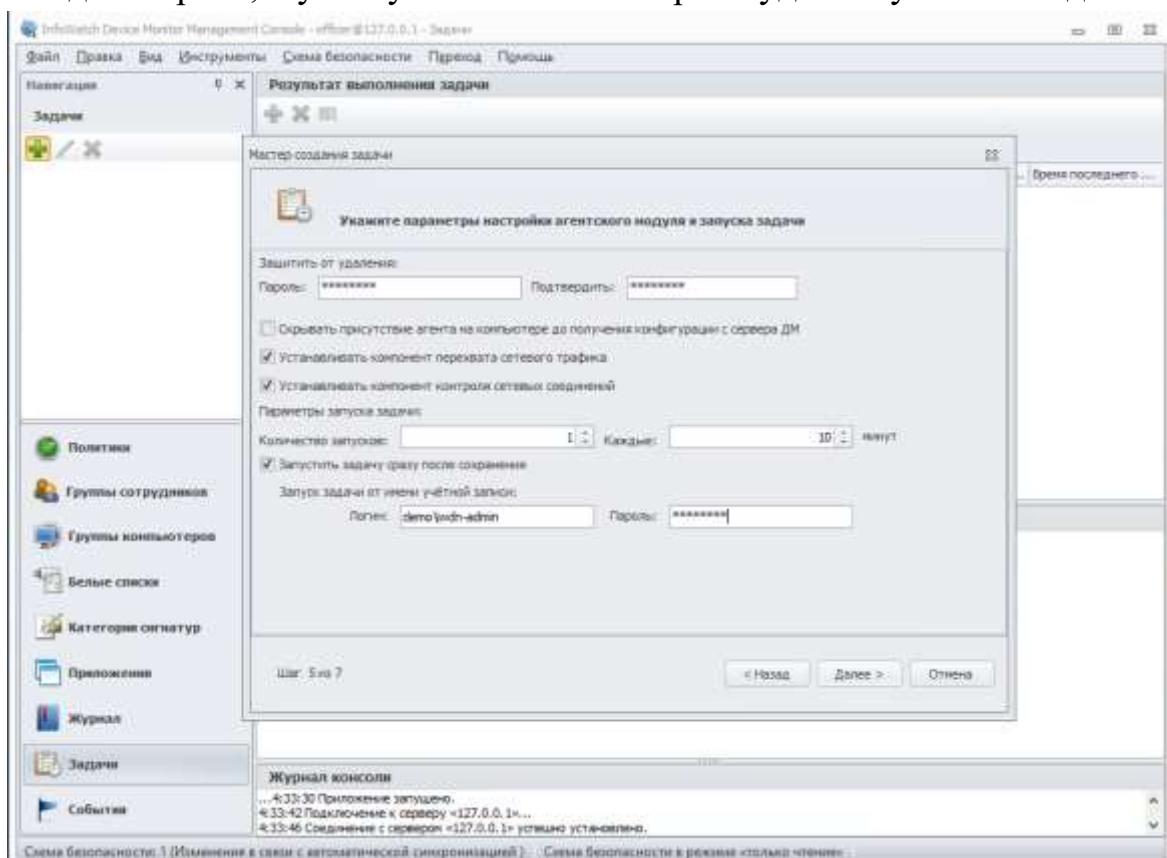


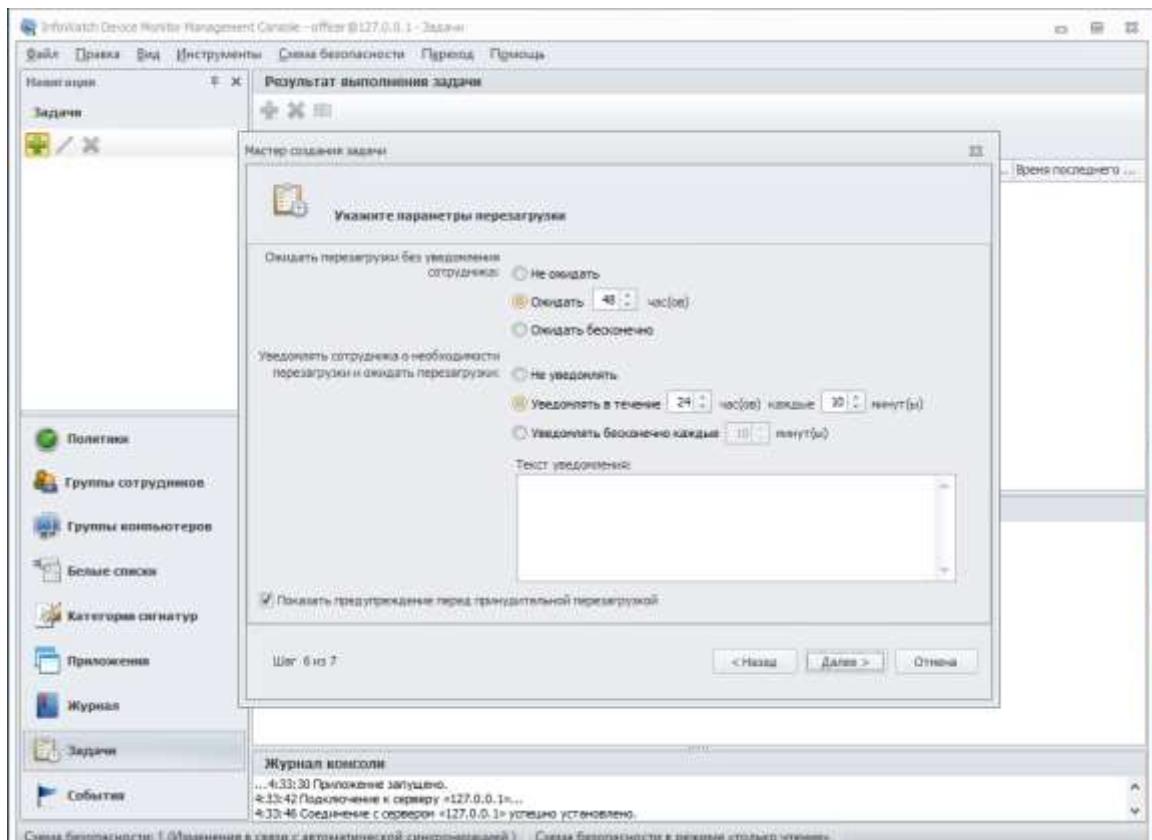
Выбираем наш сервер IWDM



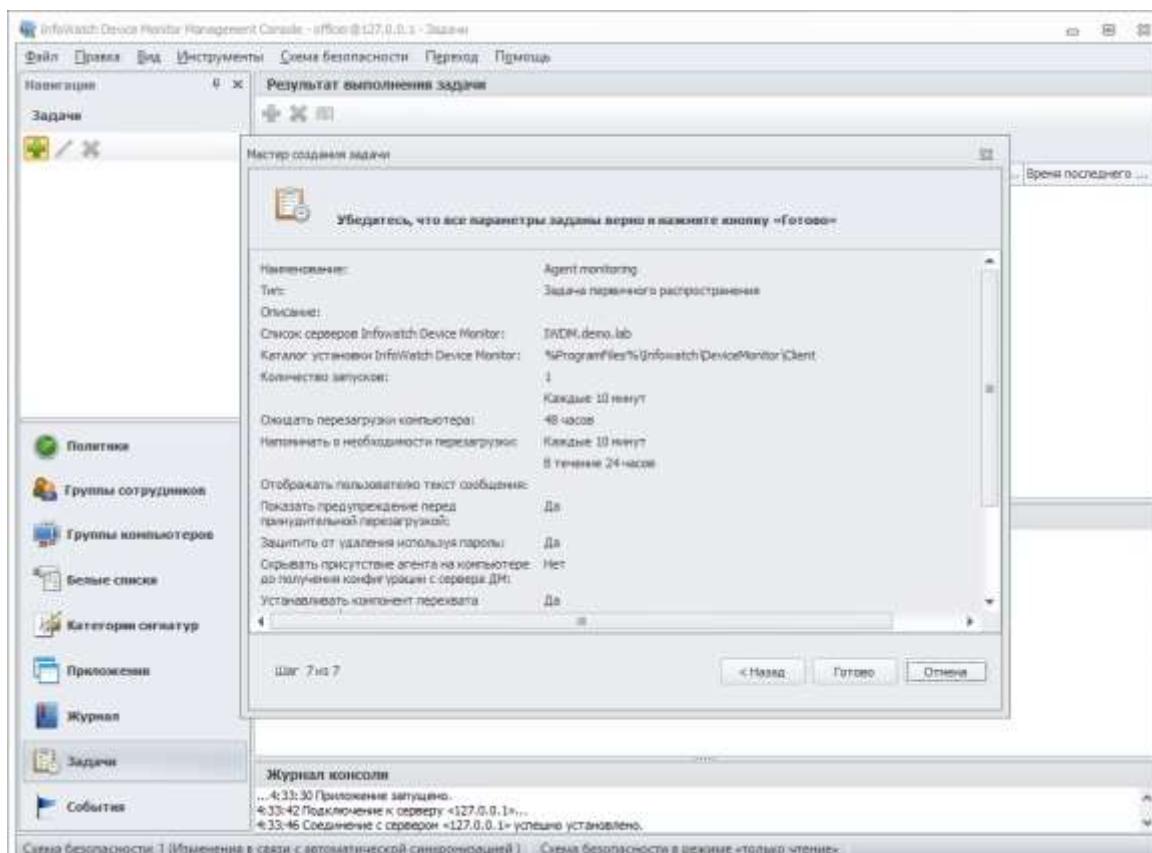


Вводим пароль, и учётную запись от которой будет запускаться задача





Готово



Ожидаем подготовку

The screenshot shows the InfoWatch Device Monitor Management Console interface. On the left, there's a sidebar with navigation links: Политики, Группы сотрудников, Группы компьютеров, Белые списки, Категории сигнатур, Приложения, Журнал, and Задачи. The 'Задачи' link is highlighted.

The main area has a title bar 'InfoWatch Device Monitor Management Console - office@127.0.0.1 - Задачи'. Below it is a toolbar with icons for New Task, Open Task, Save Task, and Delete Task. A message 'Результат выполнения задачи' (Task execution result) is displayed above a table.

The table has columns: Имя, Статус выполнени..., Версия агента, Операционная сис..., Разрядность опер..., Количество подключ..., Время последнего ...

A single row is shown: DESKTOP-BI0BDW\... with status 'Подготовка' (Preparation), timestamp '1 03.12.2021 7:35:08'.

Below the table, a 'Подробно' (Detailed) section shows task configuration:

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

At the bottom, there's a 'Журнал консоли' (Console log) entry: '... 7:33:35 ПРИЛОЖЕНИЕ ЗАПИЩЕНО.'

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 displays the 'Результат выполнения задачи' (Task Execution Result) section, which includes a table with columns: Имя (Name), Статус выполнени... (Status), Версия агента (Agent Version), Операционная сис... (Operating System), Гардность опер... (Operability), Количество подкл... (Number of connections), and Время последнего ... (Last update time). One row is shown: DESKTOP-6U060WU... (Status: В процессе - In progress), Windows 10, x64, and 1 03-12-2021 7:36:01.

The left sidebar contains navigation links: Навигация (Navigation), Задачи (Tasks), Политики (Policies), Группы сотрудников (Employee Groups), Группы компьютеров (Computer Groups), Белые списки (Whitelists), Категории сигнатур (Signature Categories), Приложения (Applications), Журнал (Journal), and Задачи (Tasks). The 'Задачи' link is currently selected.

The 'Подробно' (Detailed) section shows the configuration of the selected task:

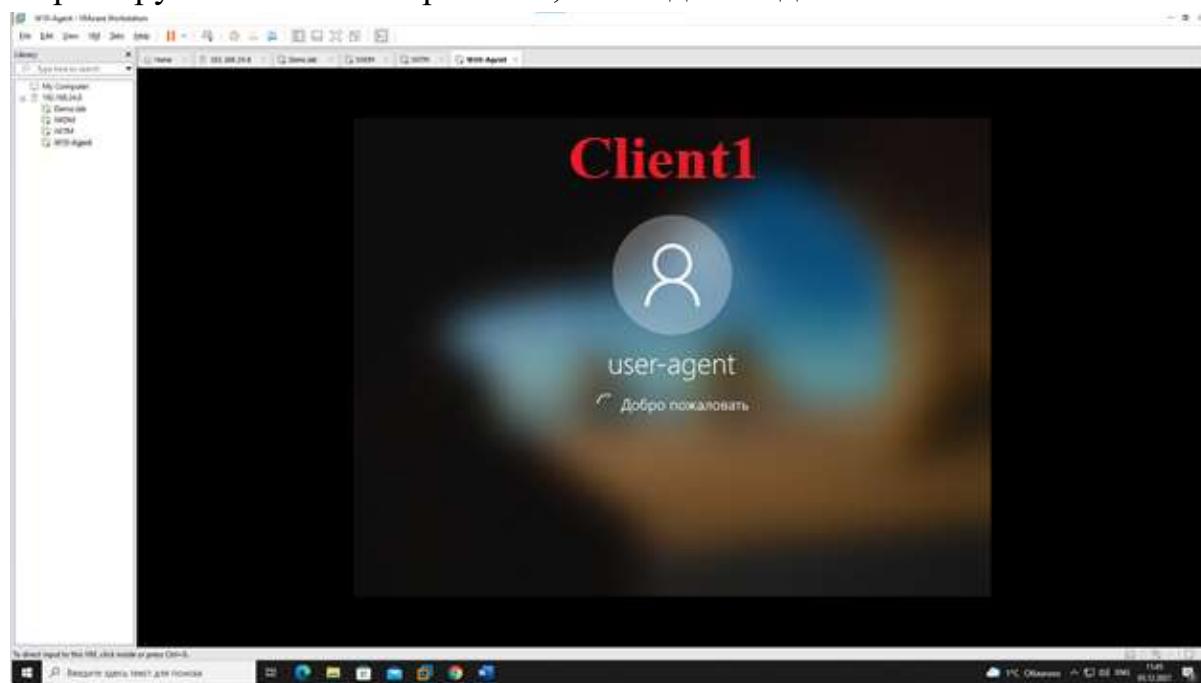
Задача
Название: monitor
Описание:
Тип: Первичное распространение
Статус: Выполняется
Период повторного запуска, мин: 10
Количество попыток повторного запуска: 1
Выводить сотруднику уведомления о работе Device Monitor Client: Да
Скрывать присутствие агента на компьютере до получения конфигурации: Нет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

Журнал консоли: 7:33:35 Приложение запущено.

Компьютер агента ожидает перезагрузки

The screenshot shows the InfoWatch Device Monitor Management Console interface. The top menu bar includes: Файл, Правка, Вид, Инструменты, Схема безопасности, Переход, Помощь. The left sidebar navigation menu lists: Навигация, Задачи, Помощь, Политики, Группы сотрудников, Группы компьютеров, Белые списки, Категории сигнатур, Приложения, Журналы, and Задача. The main content area displays the 'Результат выполнения задачи' (Task Execution Result) window. It shows a table with one row for a task named 'monitor'. The columns are: Имя (Name), Статус выполнения задачи (Task execution status), Версия агента (Agent version), Операционная с... (Operating system), Разрядность оп... (Architecture), Количество под... (Number of sub...), and Время последнего... (Last update time). The task details show it's a 'Первичное распространение' (Initial distribution) task named 'monitor' that is currently being executed ('Выполняется'). It has a period of 10 minutes for a second attempt, 1 attempt made, and is configured to send notifications to users ('Да') and monitor network traffic ('Да'). The bottom section shows the 'Журнал консоли' (Console log) with the message '7:33:35 Приложение запущено.' (Application started.)

Перезагружаем компьютер агента, и заходим под пользователя



Возвращаемся на компьютер IWDM и смотрим статус выполнения задачи – выполнено

InfoWatch Device Monitor Management Console - officer@127.0.0.1 - Задачи

Файл Правка Вид Инструменты Схема безопасности Переход Помощь

Навигация Задачи 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-BU06DUU...	Выполнено	6.11.5.468	Windows 10	x64		1 03-12-2021 7:47:05

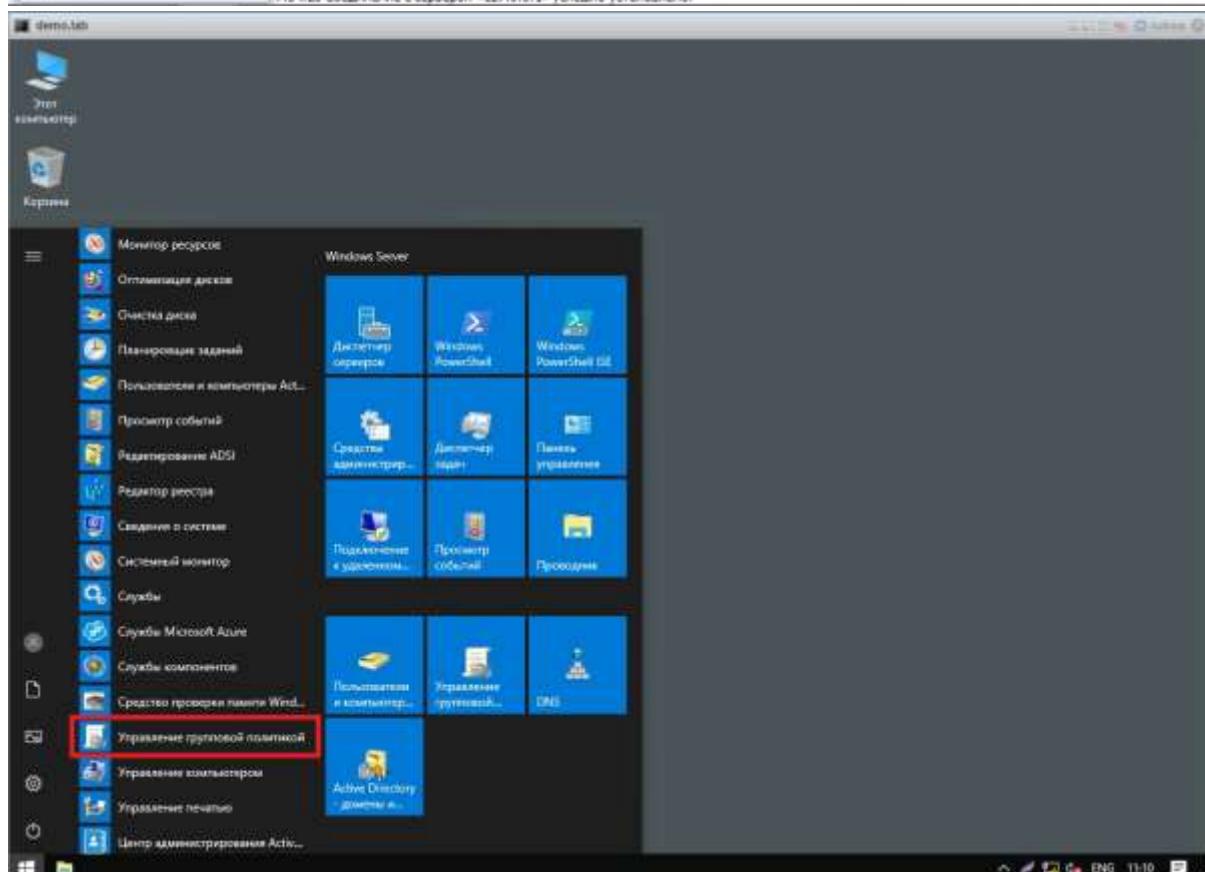
Политики
Группы сотрудников
Группы компьютеров
Белые списки
Категории сигнатур
Приложения
Журнал
Задачи
События

Подробно

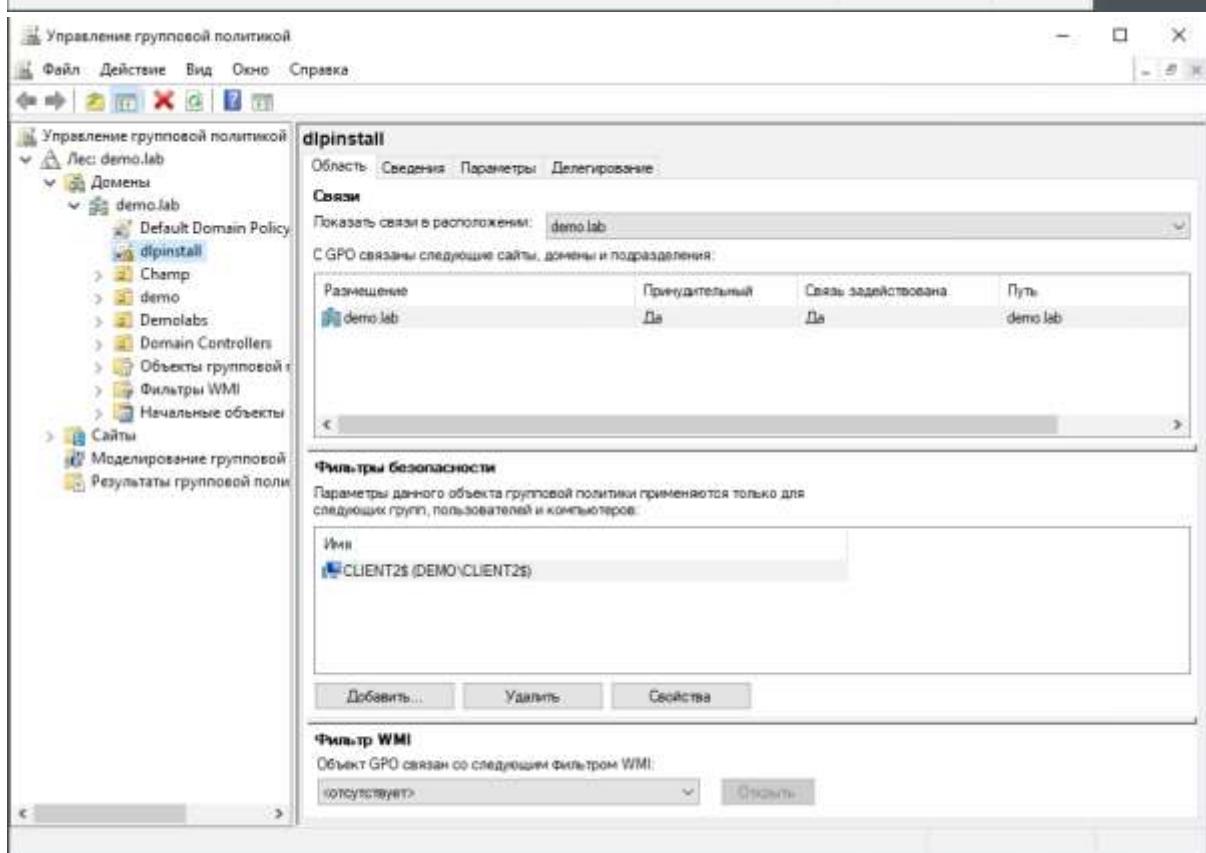
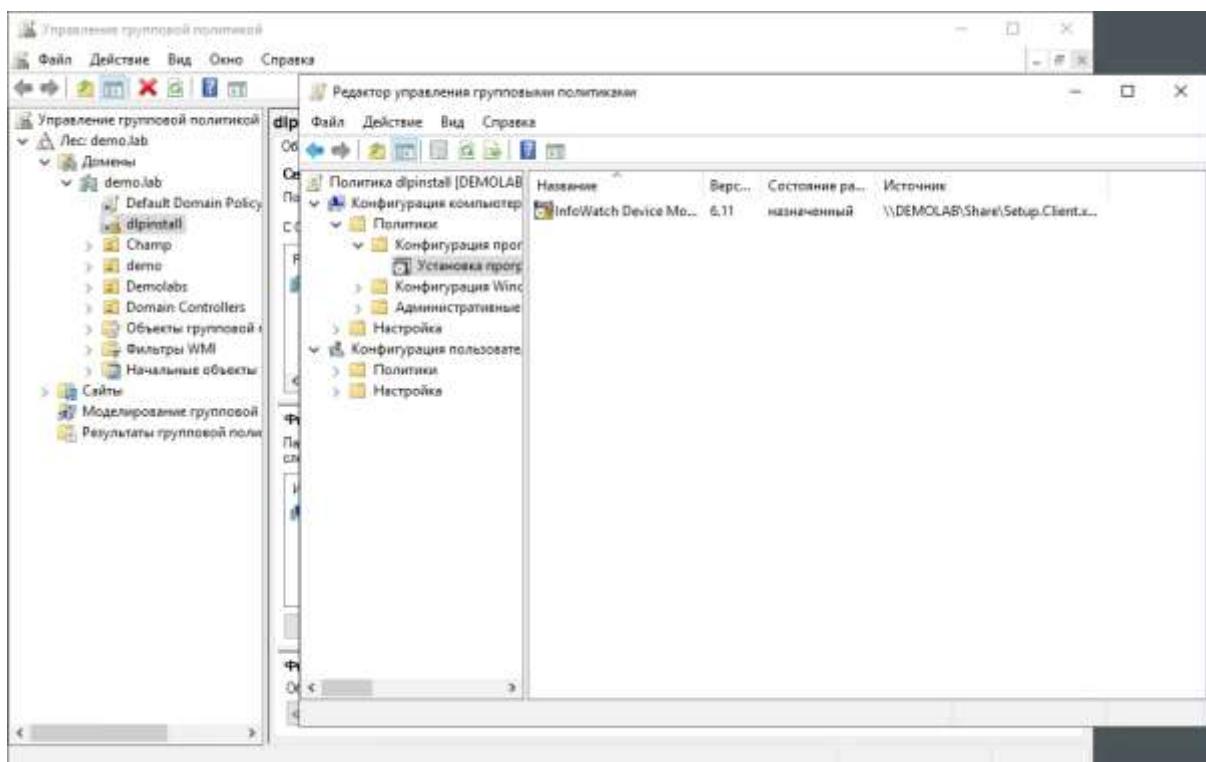
Задача	Название	Описание	Тип	Статус	Первичное распространение
monitor	monitor		Период повторного запуска, лин	10	Выполнена. Для каждого компьютера проверьте статус в поле "Статус..."

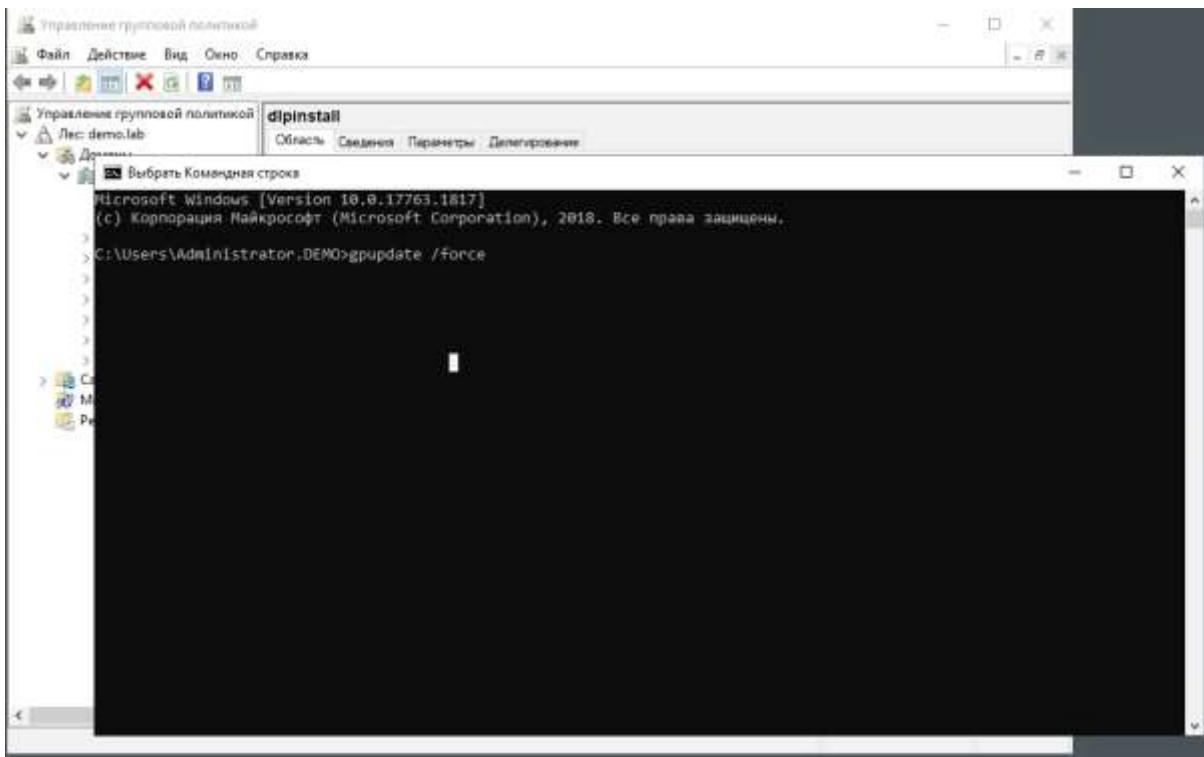
Журнал консоли

... 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





После этого перезапускаем компьютер – Клиент2

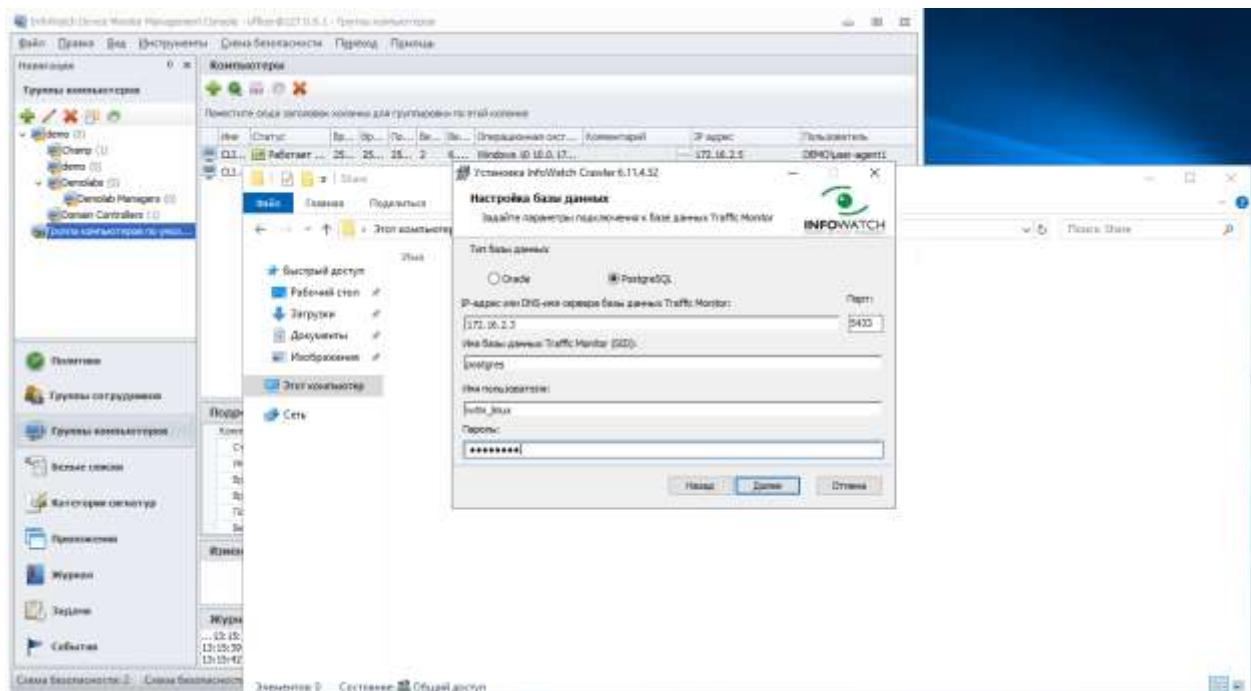
Необходимо создать общий каталог Share в корне диска сервера IWDM и установить права доступа на запись и чтение для всех пользователей домена.

Крауль – ДЕЛАТЬ В ПОСЛЕДНЮЮ ОЧЕРЕДЬ

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

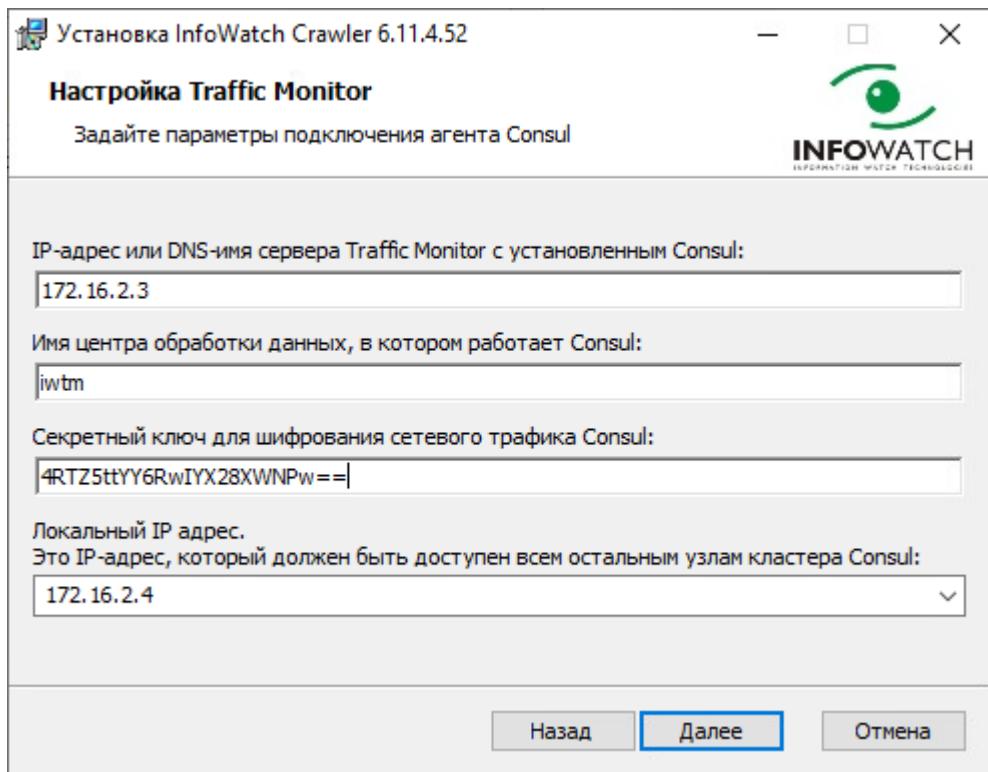


```
}[root@iwtm etc]# cd /opt/iw/tm5/etc/consul_
```

```
[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]#
```



Платформы

- + InfoWatch Crawler
- InfoWatch Device Monitor
- InfoWatch Sample documents Acropolis

InfoWatch Crawler

Платформа: InfoWatch Crawler
Время создания: 19.07.2018
Версия: 6.11.8

Платформы Платформы Токены

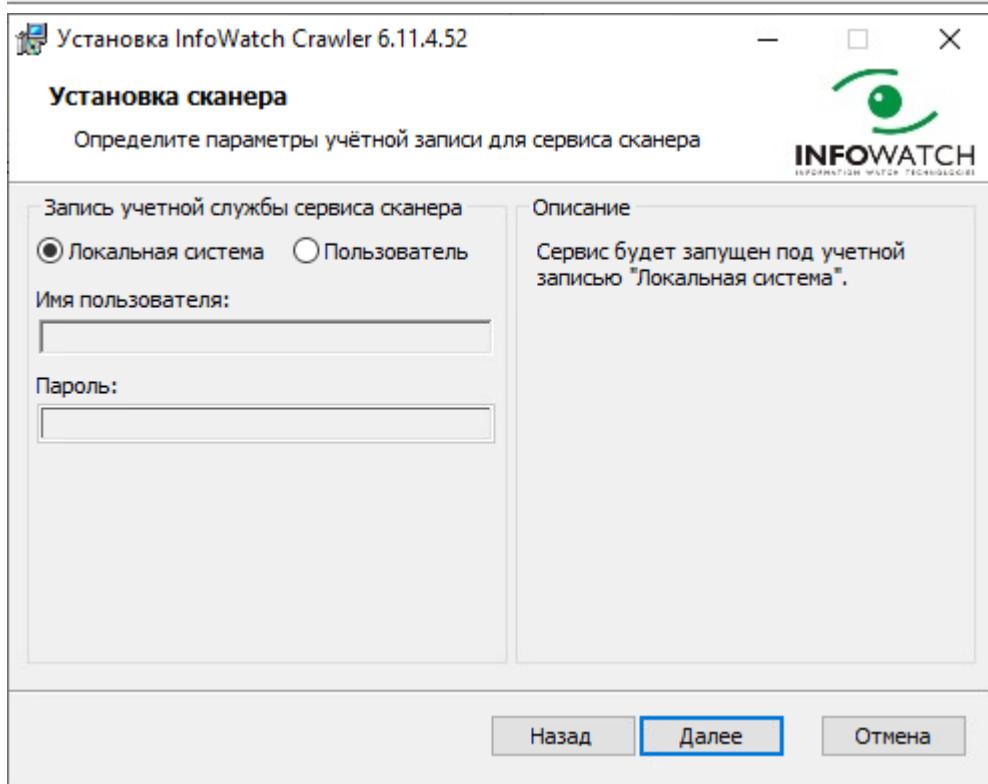
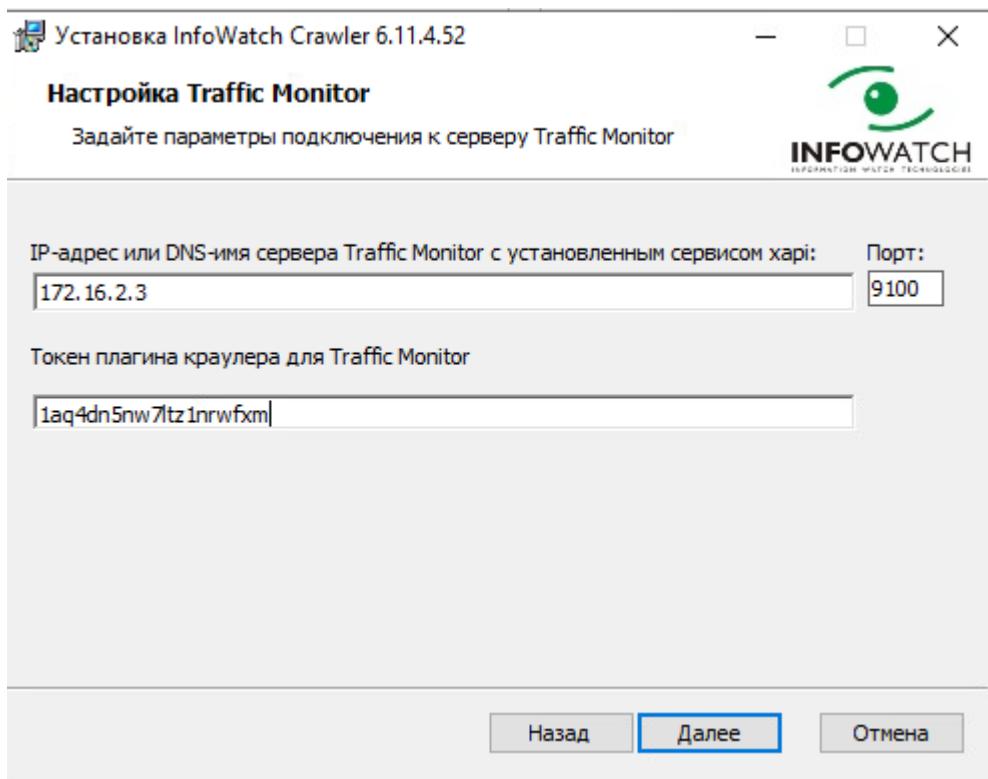
Статус Имя Содержание

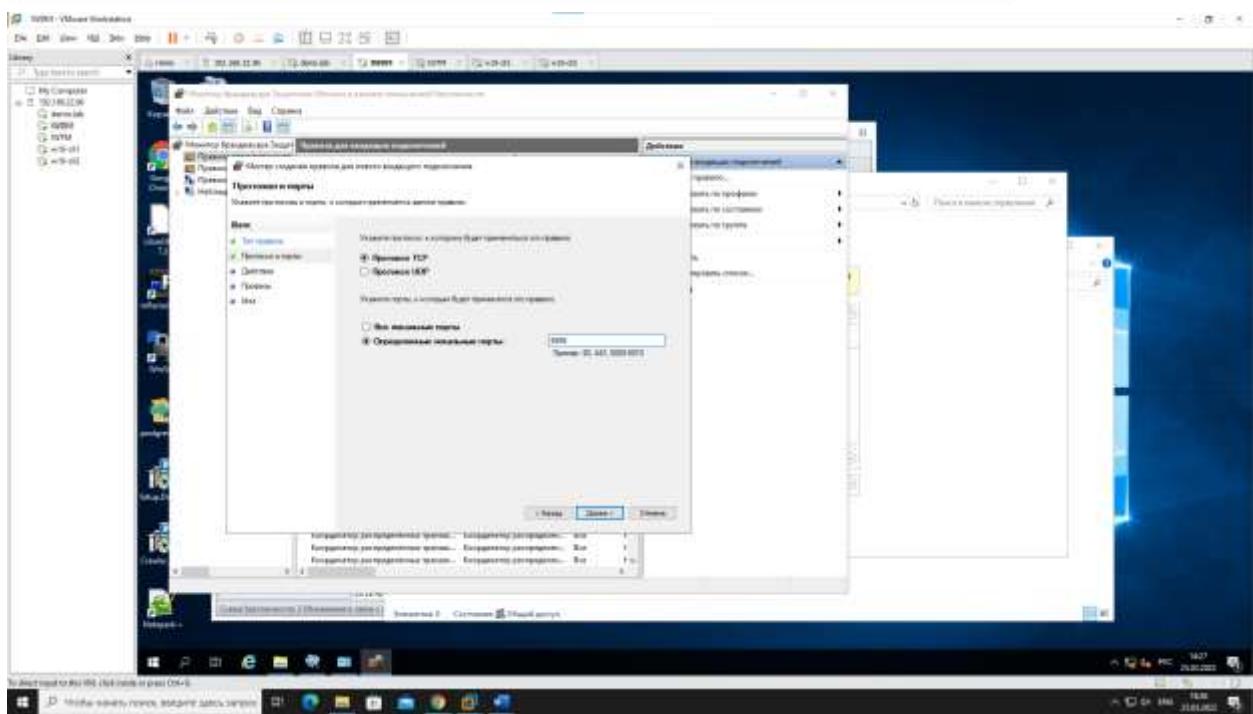
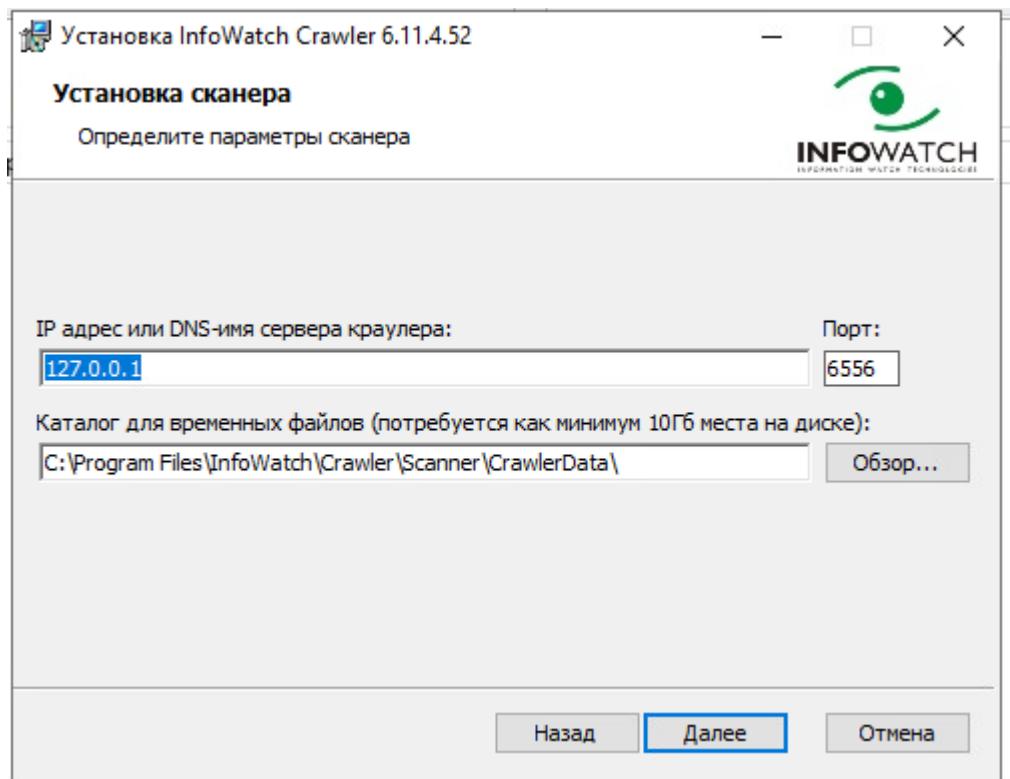
Активный	Token-2	1aq4dn5nw7ltz1nrwfxm
----------	---------	----------------------

```
[root@iwtm etc]# cd /opt/iwtm5/etc
```

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

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

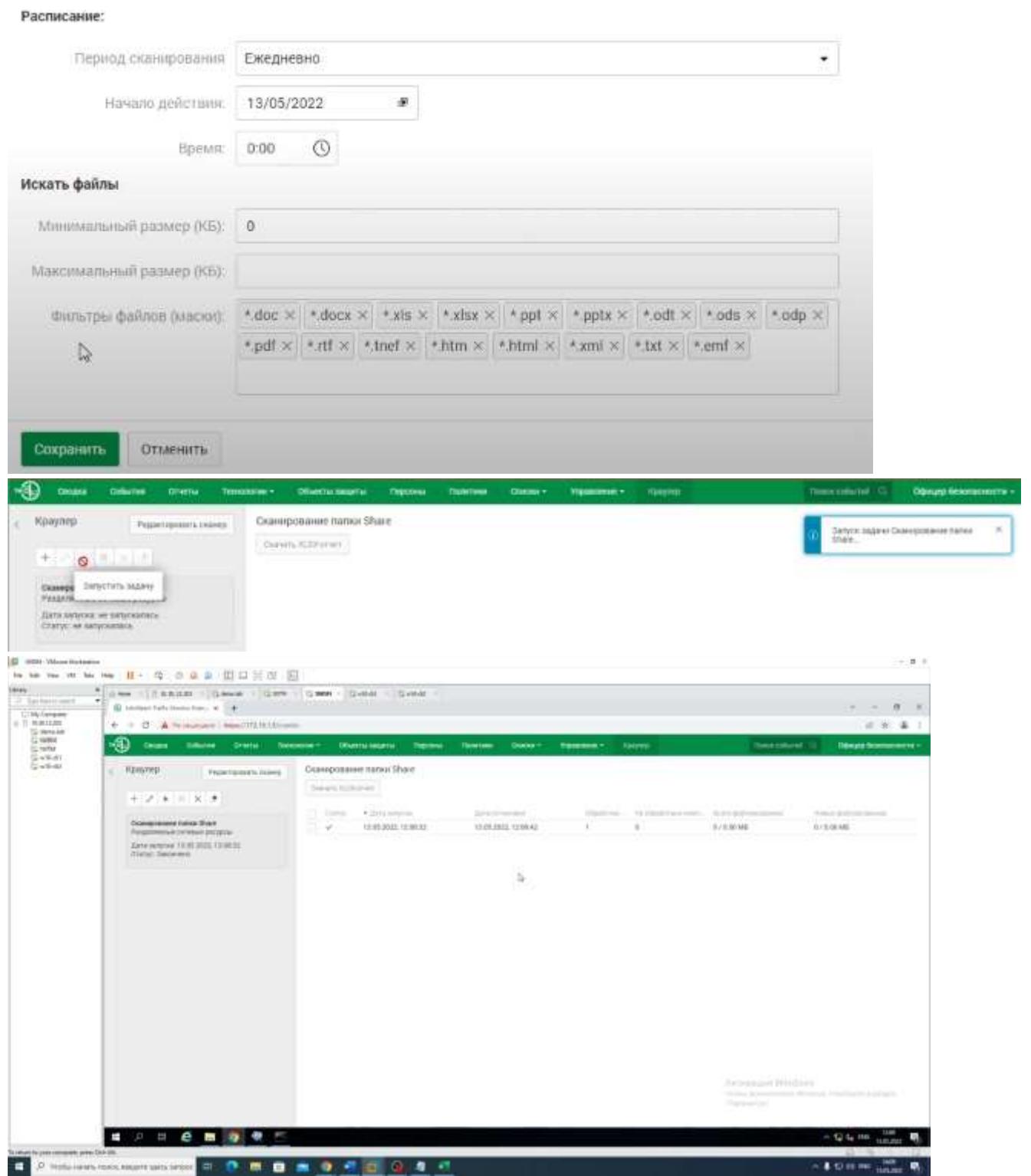




The screenshot shows a Windows desktop environment with several open windows:

- Network Connections window:** Displays network adapters (Intel PRO/100 MT Desktop, Intel PRO/100 MT, Intel PRO/100 MT), connection status (Status: Enabled), and connection type (Protocols and ports). It includes sections for Protocols and ports (TCP/IPv4, TCP/IPv6, NetBIOS over TCP/IP) and Firewall (Windows Firewall with Advanced Security).
- File Explorer window:** Shows the path "C:\Windows\system32\drivers\etc" and lists files like hosts, ipconfig, and netsh.
- Terminal window:** Titled "GNU nano 2.3.1 File: /etc/hosts", it contains the following content:

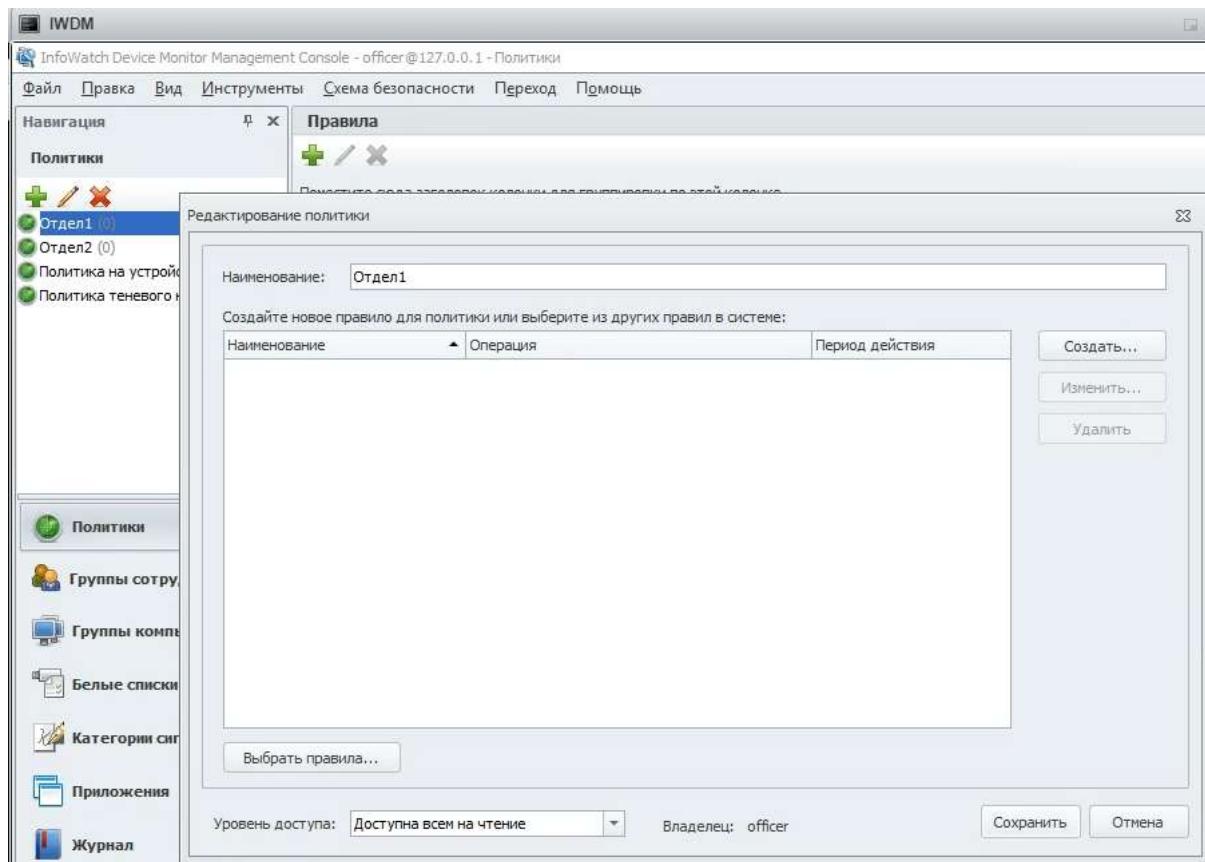
```
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
172.16.2.3 iwtm.demo.lab iwtm
172.16.2.4 iwdm.demo.lab iwdm
```
- Krauler application window:** Titled "Создание задачи" (Create Task), it is used for creating scheduled tasks. It includes fields for Name (Название: "Сканирование папки Share"), Description (Описание: empty), Scan Object (Объект сканирования: "Разделенные сетевые ресурсы"), Scan Targets (Сканируемые группы и компьютеры: "IWDM"), Scan Mode (Режим сканирования: "Только папки"), Filter (Фильтр: "Share", "*Share", "C:\Share"), and Exclusion (Исключая системные папки). The "Авторизация сканера" (Scanner Authorization) toggle switch is turned on.

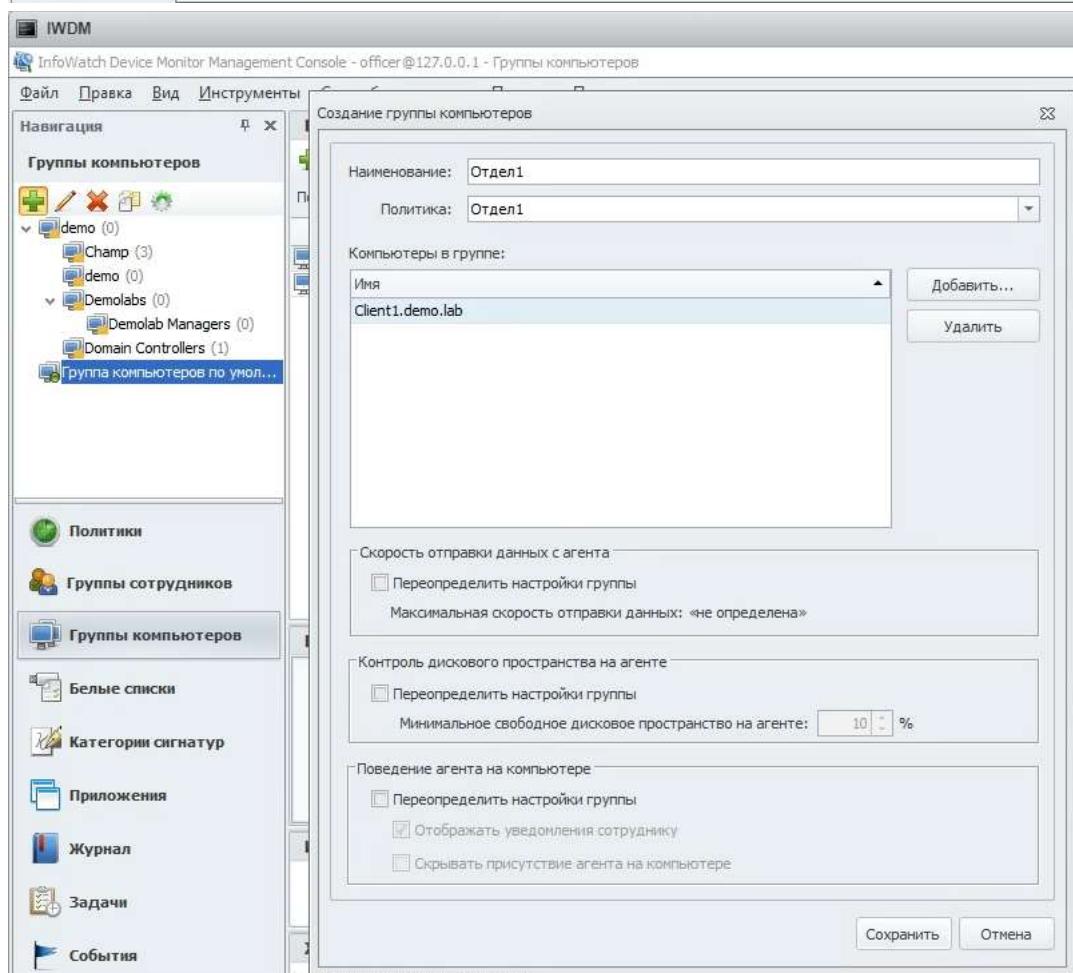
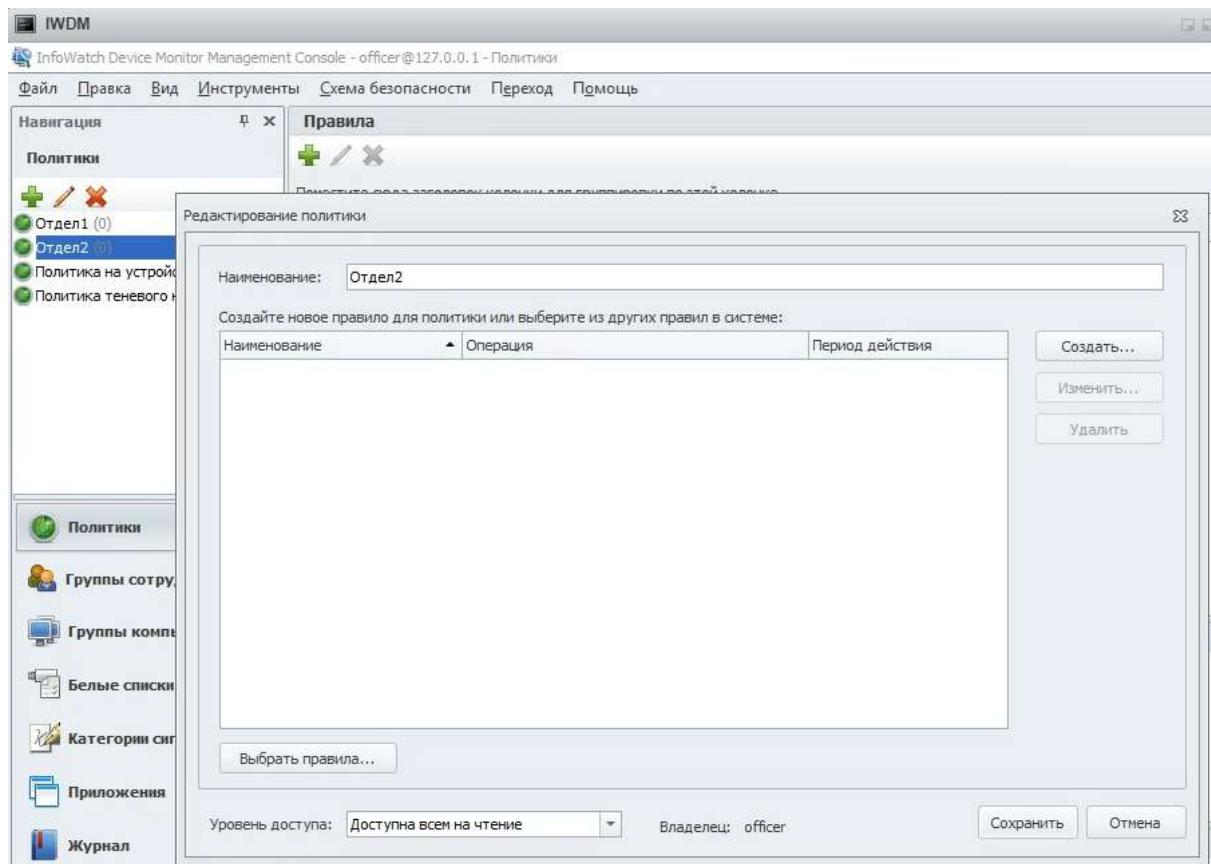


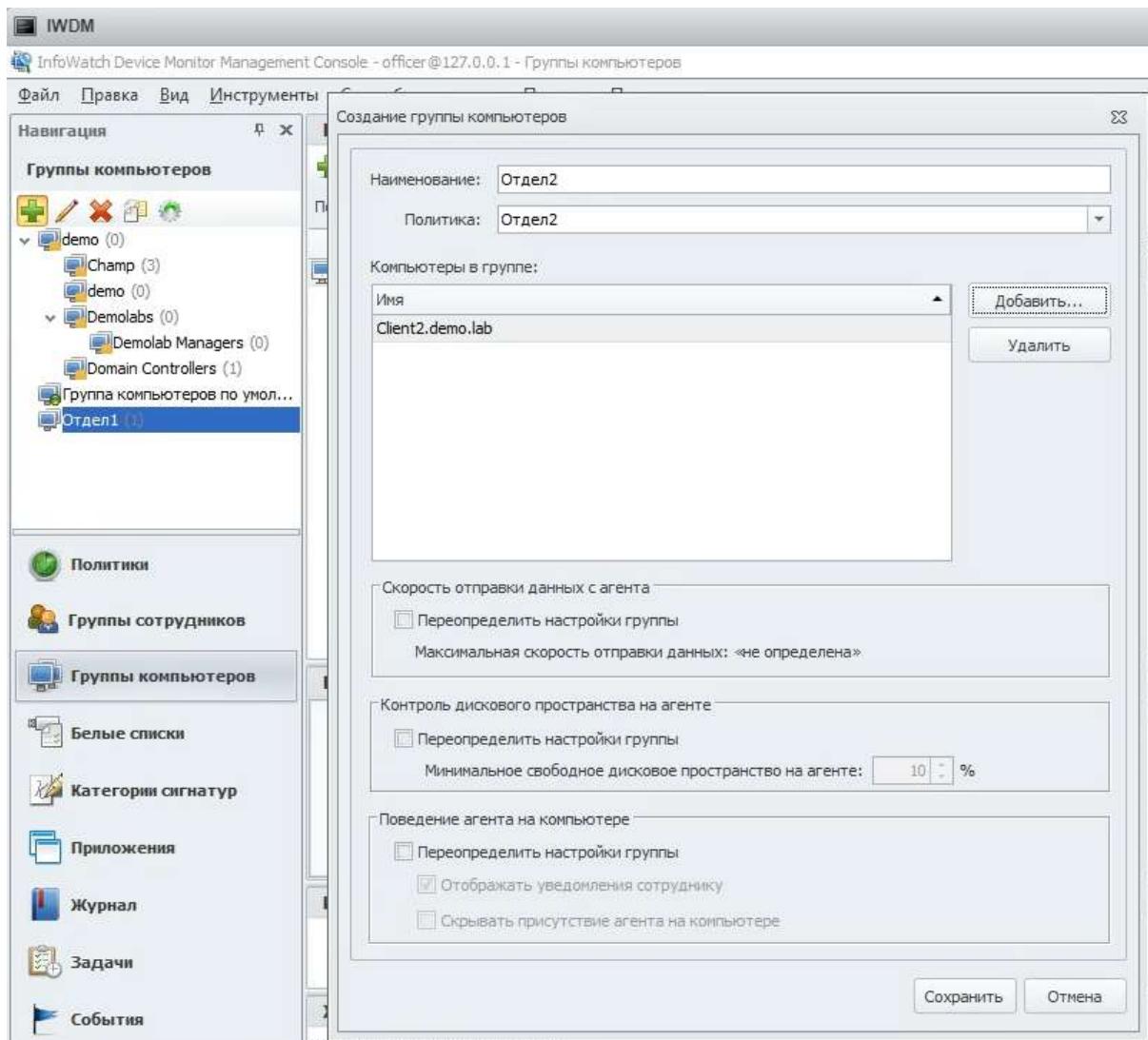
Модуль 2.

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.





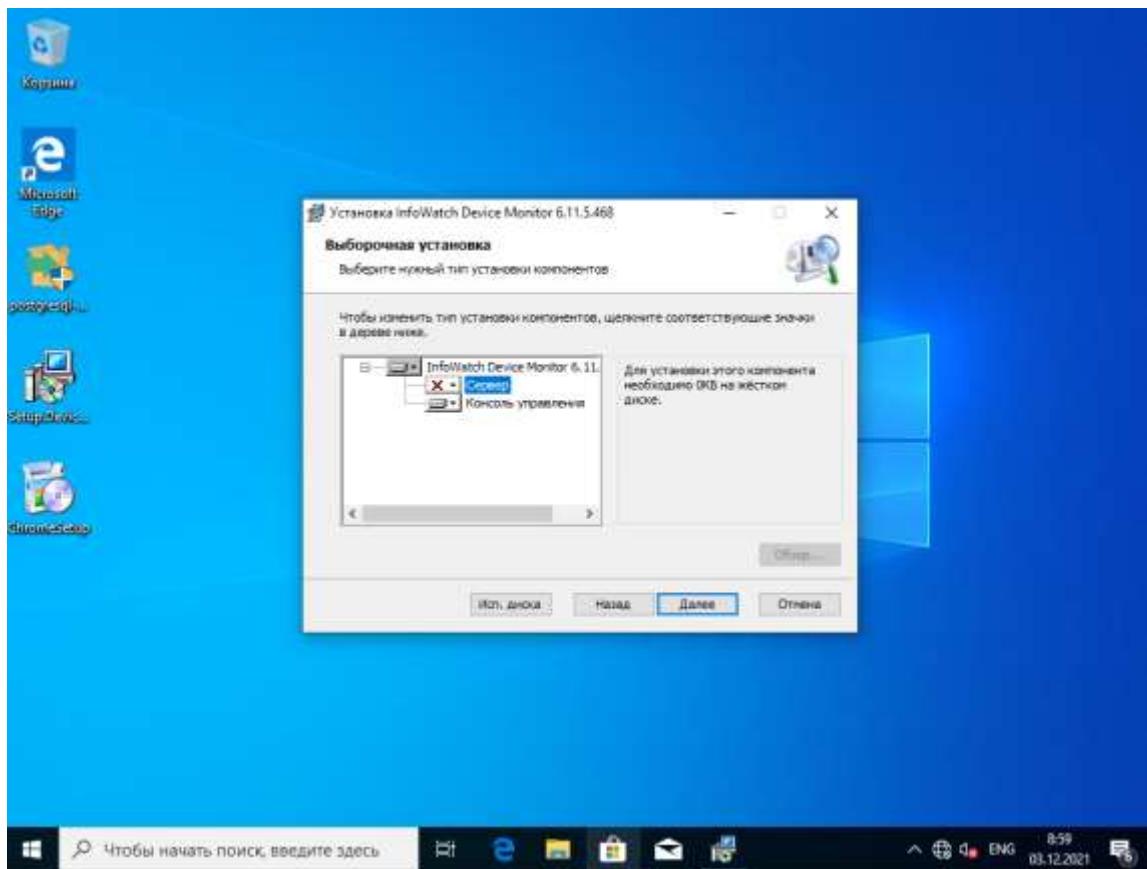


Задание 2

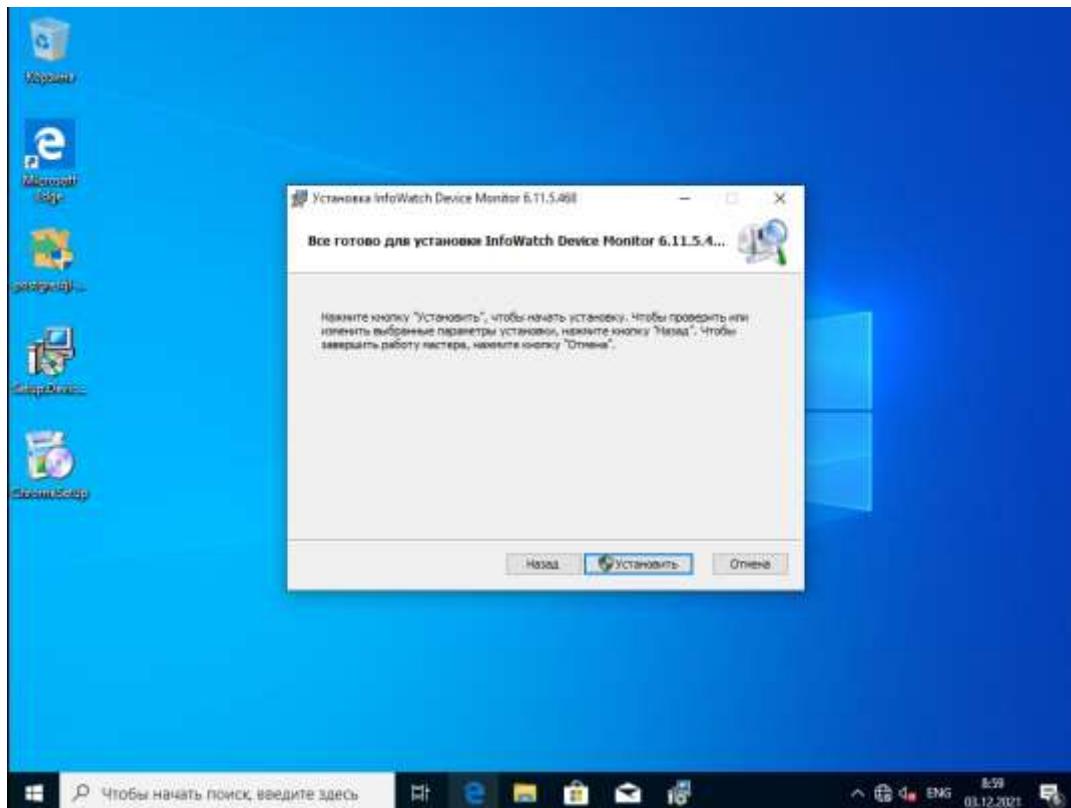
Для удобства работы офицера безопасности необходимо установить дополнительную консоль управления сервером агентского мониторинга на машину W10-agent1 для удаленного доступа к серверу агентского мониторинга.

Следующие правила создаются в политике «Отдел1».

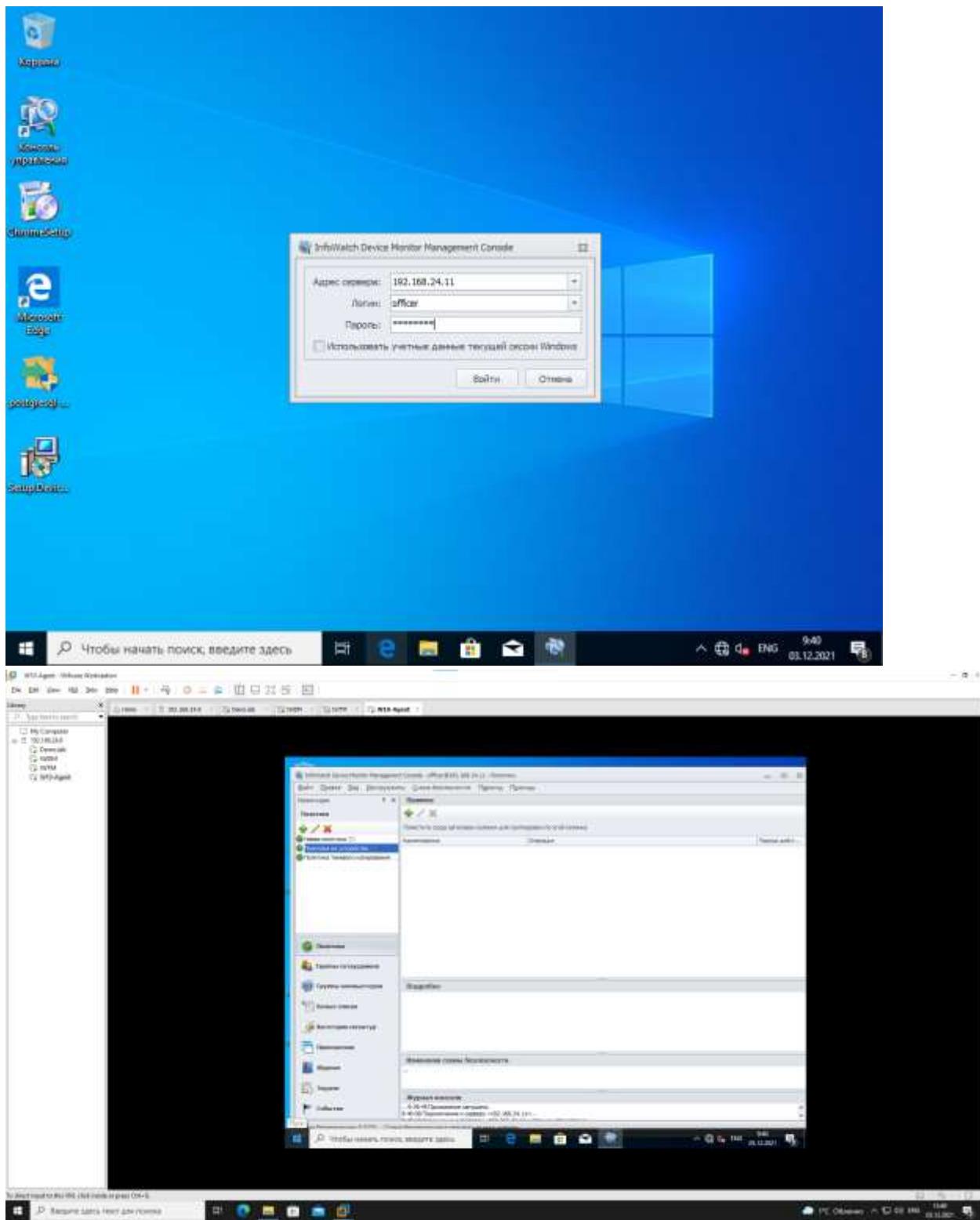
Убираем сервер, оставляем только консоль управления



Установили InfoWatch Device Monitor



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



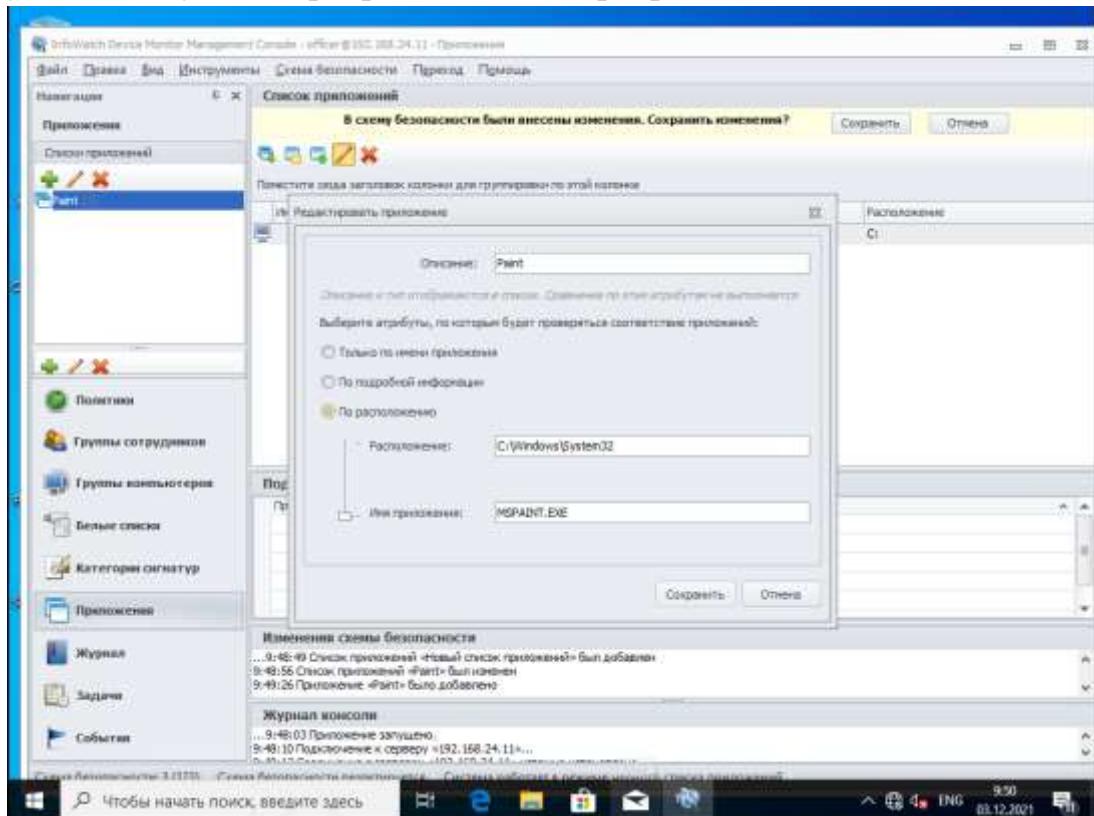
Следующие правила создаются в политике «Отдел1»

Правило 1

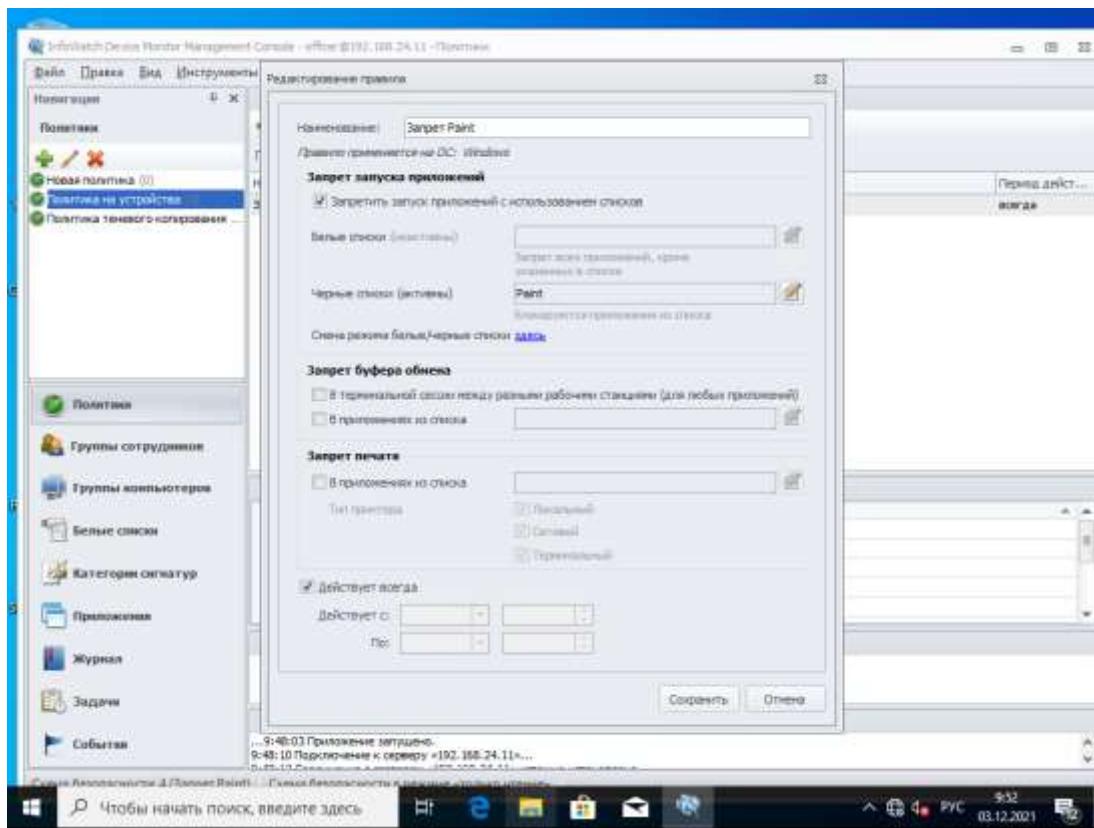
Необходимо запретить пользоваться Microsoft Paint, так как участились случаи подделки печатей компании.

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



Зафиксировать скриншотами необходимо!

Правило 2

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

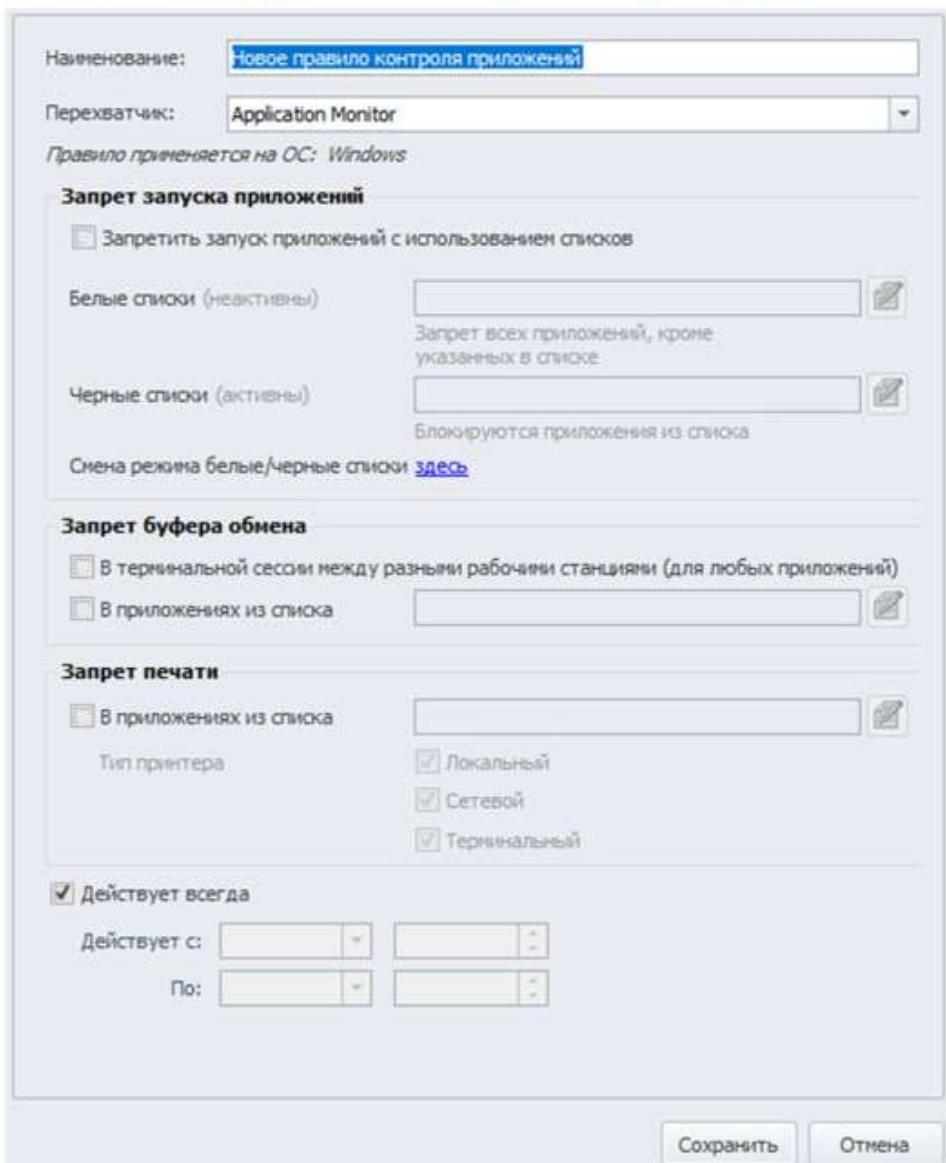


Рисунок 57 – «Создание правила»

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\uxim\
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\uxim\
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>	GoogleUpda...	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...	ShellFvirarie	Windows Sh...	Microsoft® ...	O=Microsoft...	c:\windows\leveteman

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.

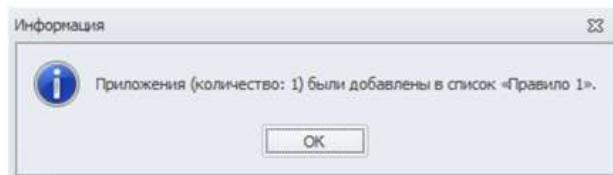


Рисунок 59 – «Успешное добавление приложения»

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

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: [From] [To]

По: [From] [To]

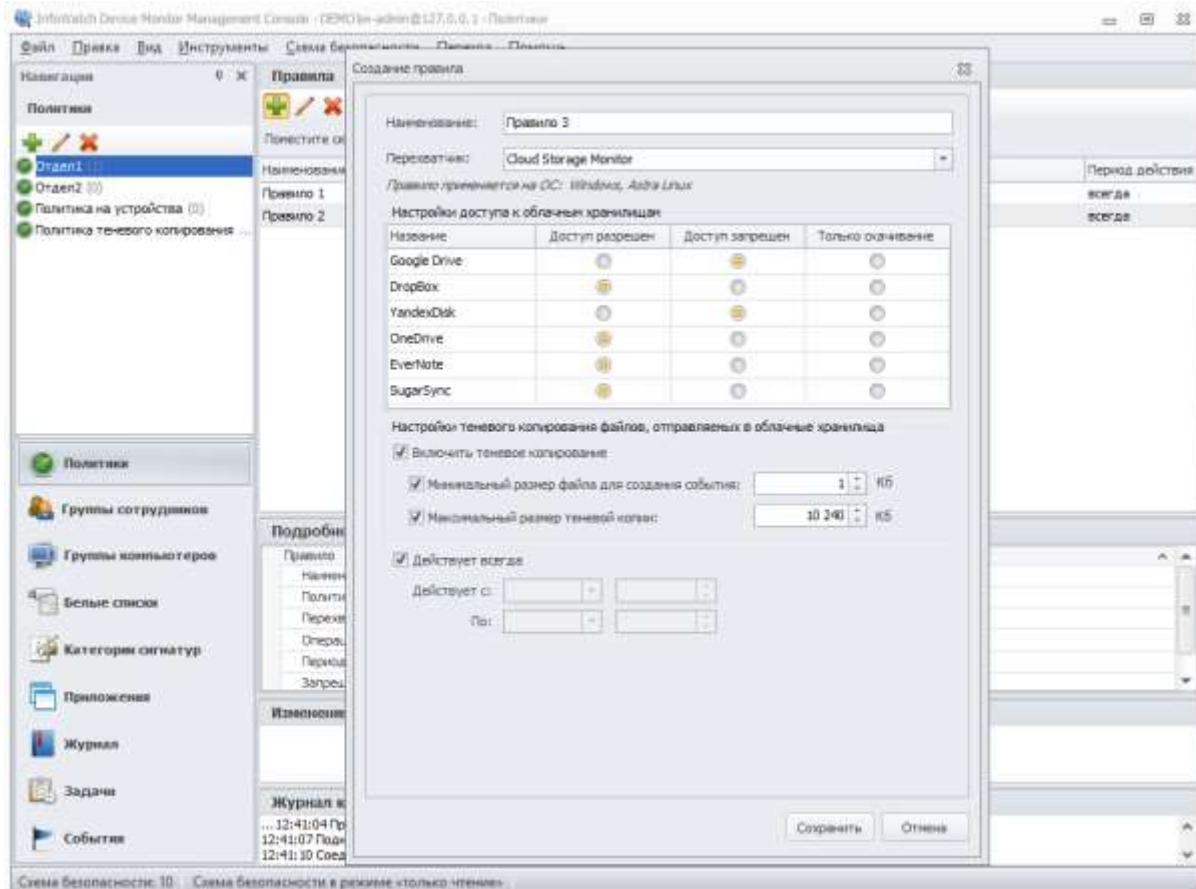
Рисунок 60 – «Правило 1»

Задокументировать скриншотами необходимо!

Правило 3

Ограничить доступ к облачным хранилищам GoogleDrive и YandexDisk.

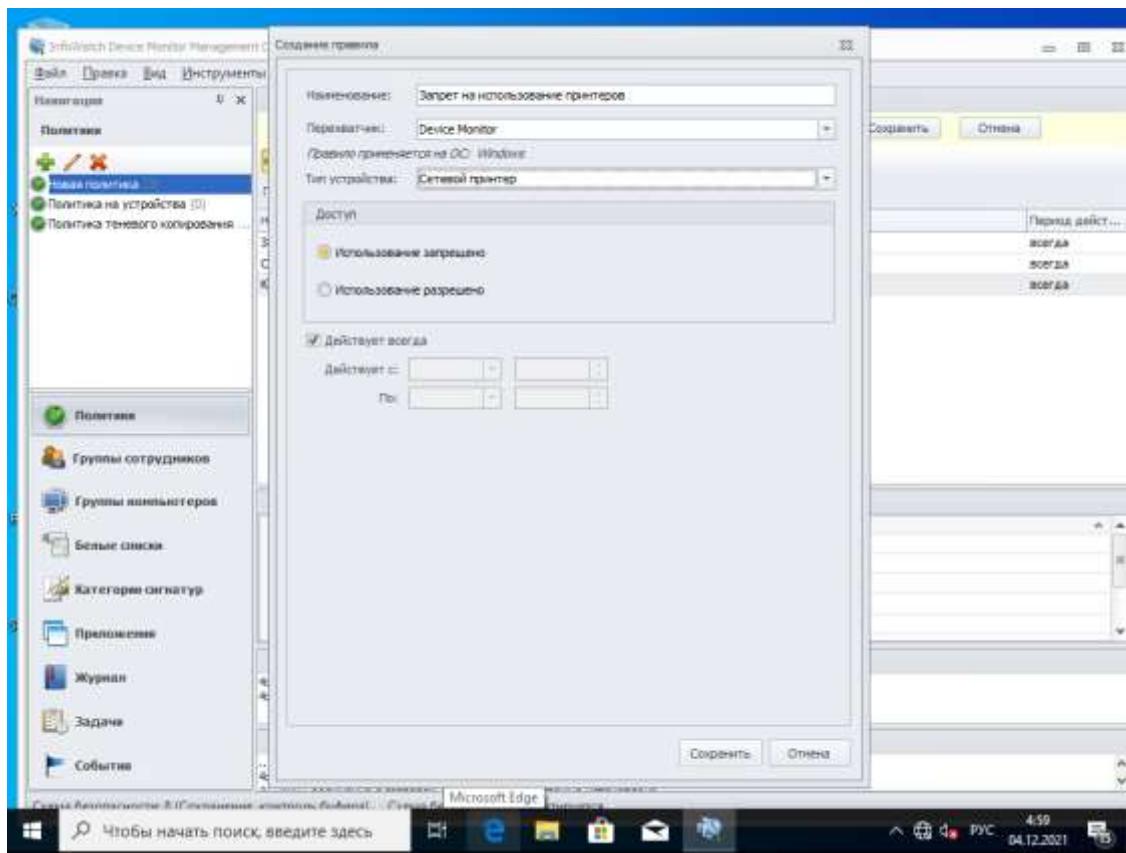
Проверить работоспособность и зафиксировать выполнение



Правило 4

Необходимо запретить печать на сетевых принтерах.

Зафиксировать создание политики скриншотом.



Задокументировать создание политики скриншотом.

Правило 5

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

Проверить работоспособность и задокументировать выполнение

Наименование: Правило 5
Перехватчик: Device Monitor
Правило применяется на ОС: Windows
Тип устройства: Съёмное устройство хранения

Доступ

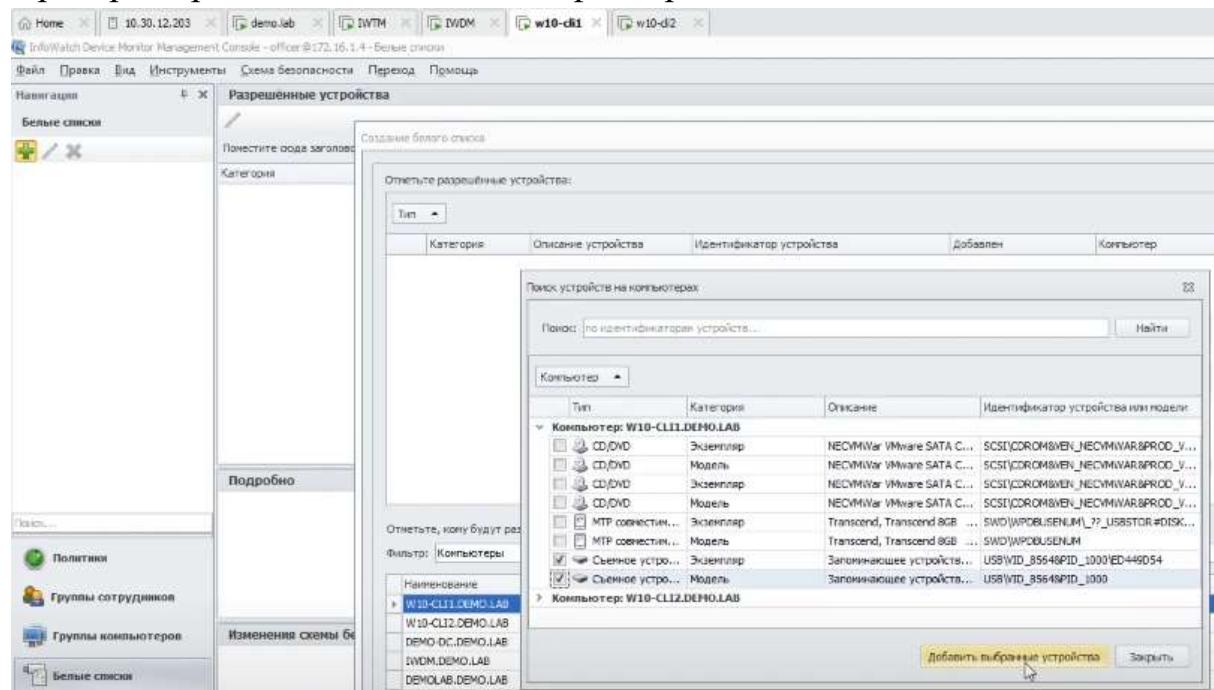
Нет доступа
 Только чтение
 Полный доступ на зашифрованные носители
 Использование разрешено

Проверить работоспособность и задокументировать выполнение

Правило 6

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

Проверить работоспособность и зафиксировать выполнение



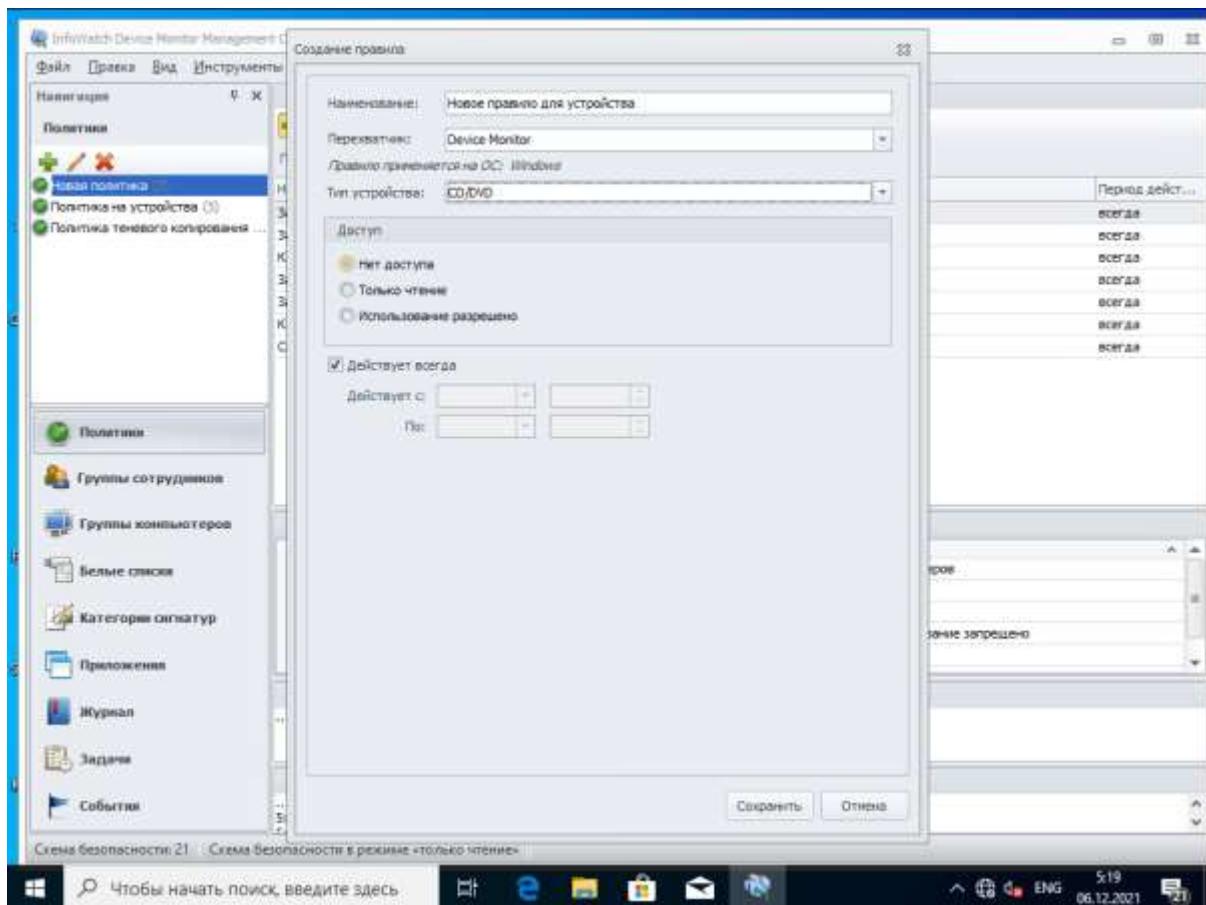
Категория	Описание устройства	Идентификатор устройства или подразделения	Добавлен	Компьютер
CD/DVD	Экземпляр	NECMiVar VMware SATA C...	SCSI\DR0M8VEN_NECMVAR\PROD_V...	Компьютер: W10-CL11.DEMO.LAB
CD/DVD	Модель	NECMiVar VMware SATA C...	SCSI\DR0M8VEN_NECMVAR\PROD_V...	Компьютер: W10-CL11.DEMO.LAB
CD/DVD	Экземпляр	NECMiVar VMware SATA C...	SCSI\DR0M8VEN_NECMVAR\PROD_V...	Компьютер: W10-CL11.DEMO.LAB
CD/DVD	Модель	NECMiVar VMware SATA C...	SCSI\DR0M8VEN_NECMVAR\PROD_V...	Компьютер: W10-CL11.DEMO.LAB
MTP соединен...	Экземпляр	Transcend, Transcend 8GB ...	SWD\WP0BLSENUM_?_U58STOR-#ISK...	Компьютер: W10-CL11.DEMO.LAB
MTP соединен...	Модель	Transcend, Transcend 8GB ...	SWD\WP0BLSENUM_?_U58STOR-#ISK...	Компьютер: W10-CL11.DEMO.LAB
Съемное устройс...	Экземпляр	Запоминающее устройств...	USB\VID_8564&PID_1000\ED449054	Компьютер: W10-CL11.DEMO.LAB
Съемное устройс...	Модель	Запоминающее устройств...	USB\VID_8564&PID_1000\ED449054	Компьютер: W10-CL11.DEMO.LAB

Проверить работоспособность и зафиксировать выполнение!

Правило 7

Полностью запретить использование CD/DVD-дисковода.

Проверить работоспособность и зафиксировать выполнение



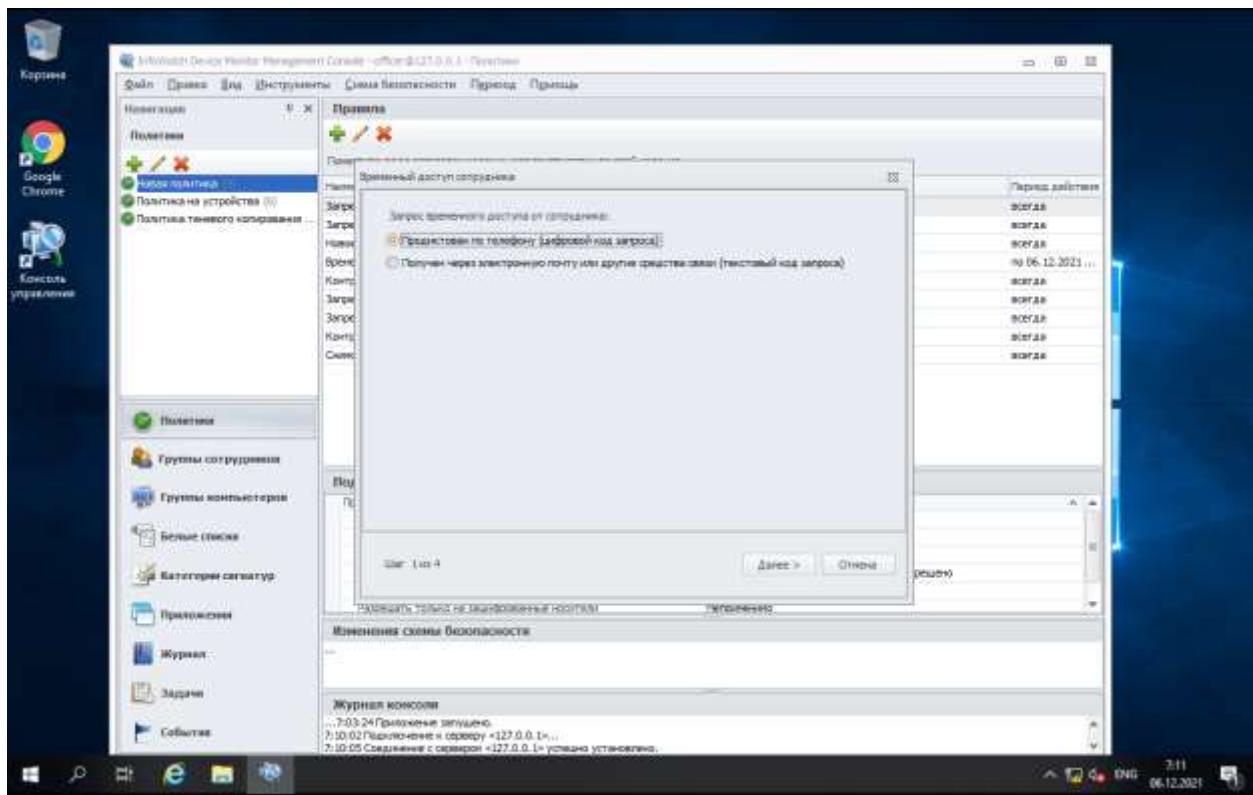
Проверить работоспособность и зафиксировать выполнение!

Правило 8

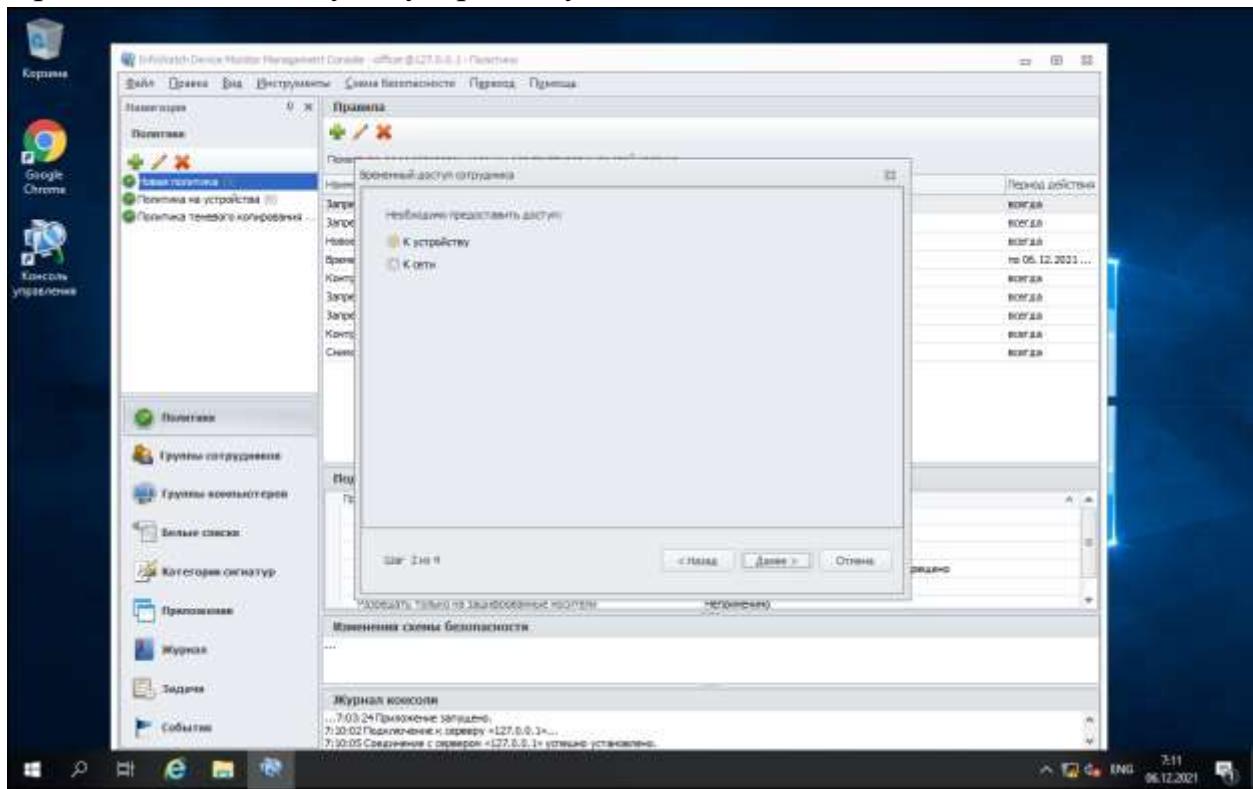
С учетом ранее выполненного запрета необходимо предоставить временный доступ для устройства на 7 минут для пользователя.

Зафиксировать этапы выдачи доступа и работоспособность скриншотами.

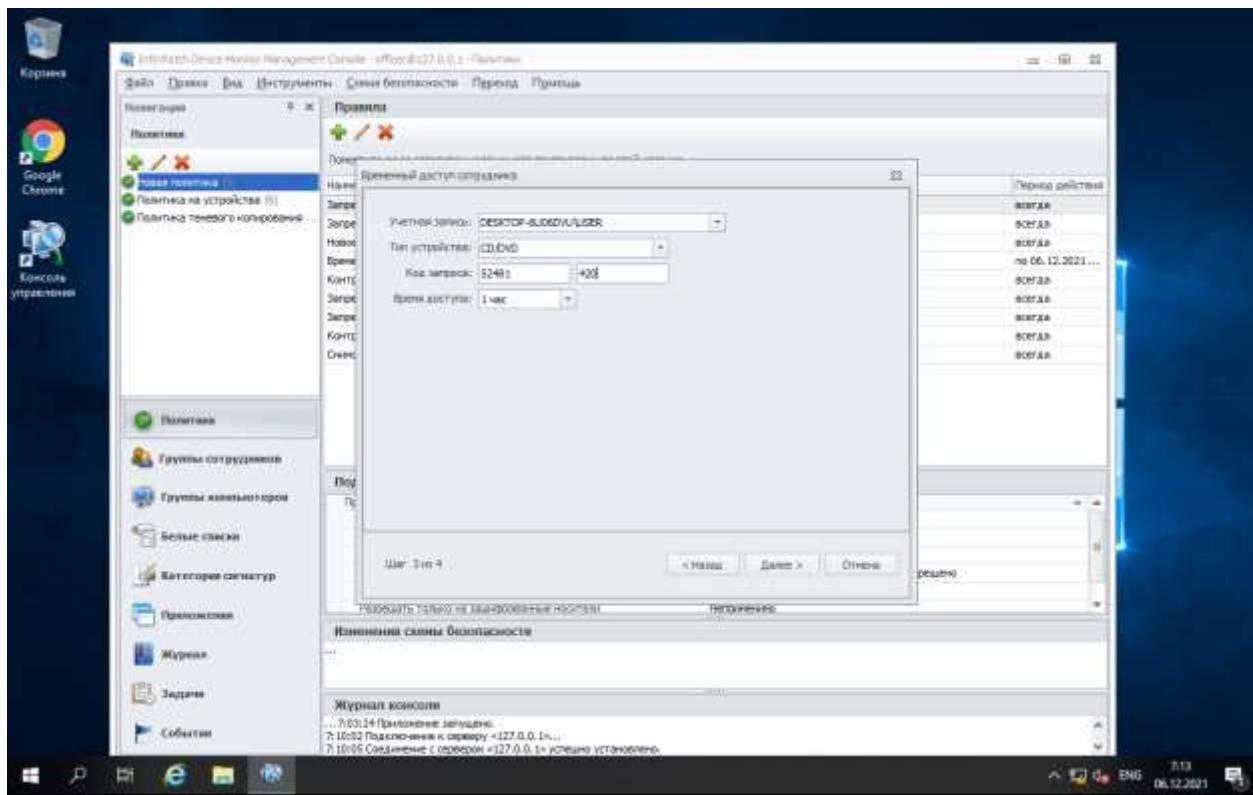
Выдаем временный доступ сотруднику



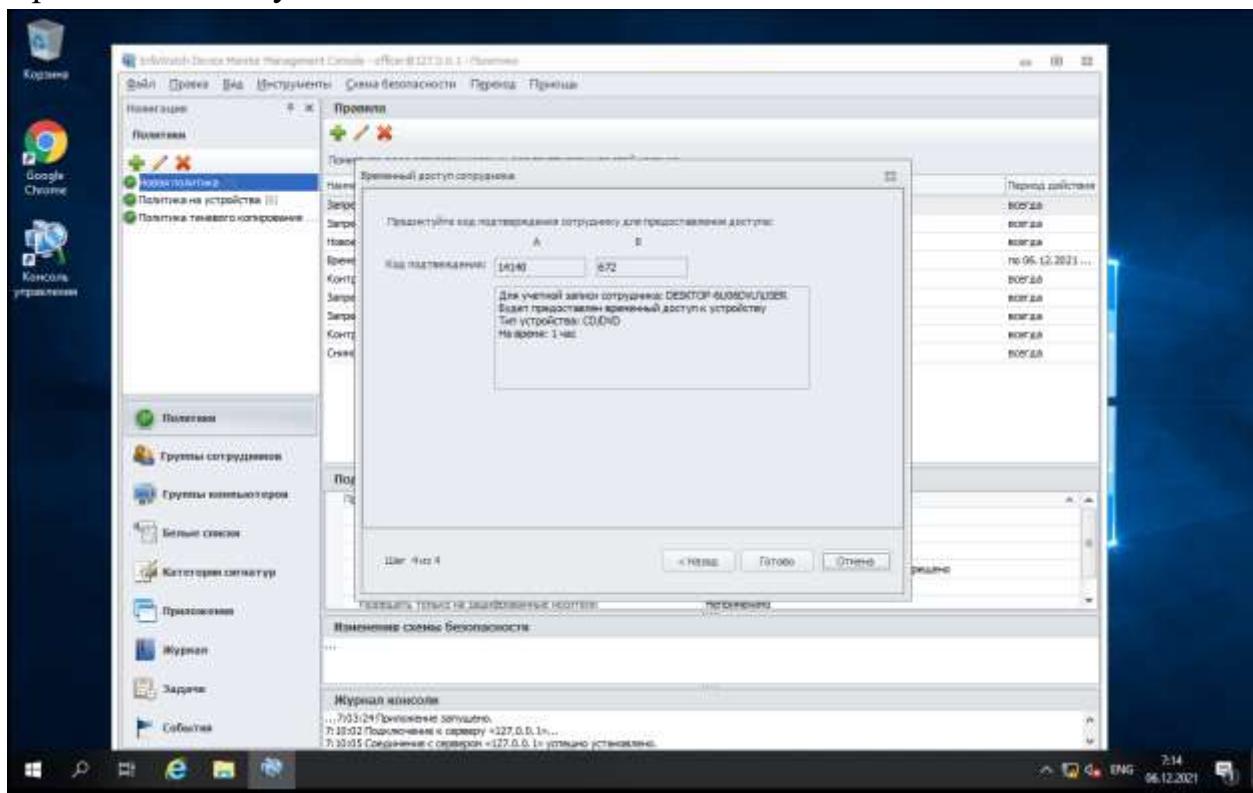
Предоставляем доступ к устройству



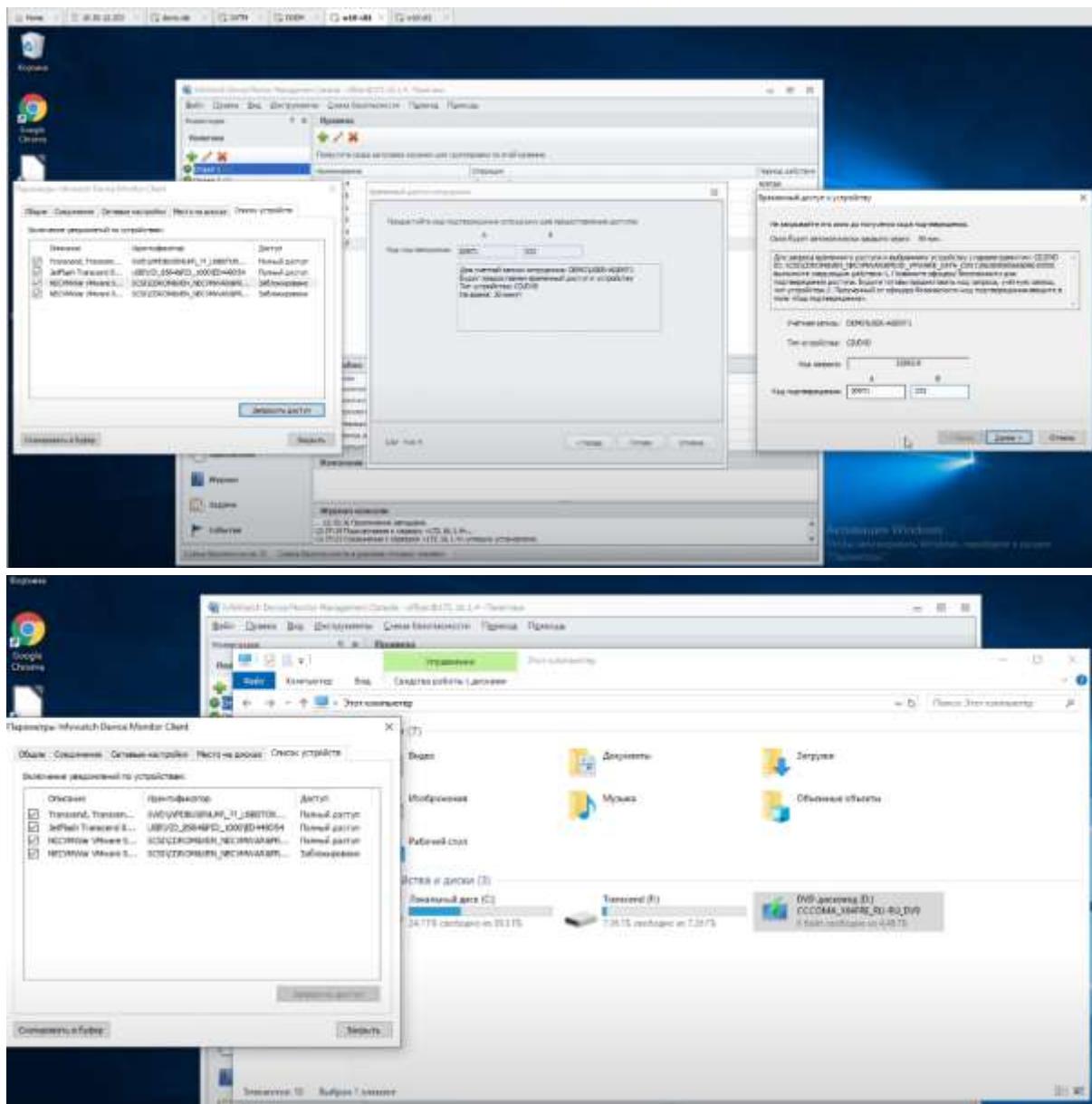
Выбираем компьютер, время доступа



Временный доступ



Скриншотим



Зафиксировать этапы выдачи доступа и работоспособность скриншотами.

Следующие правила создаются в политике «Отдел2».

Следующие правила создаются в политике «Отдел2».

Правило 9

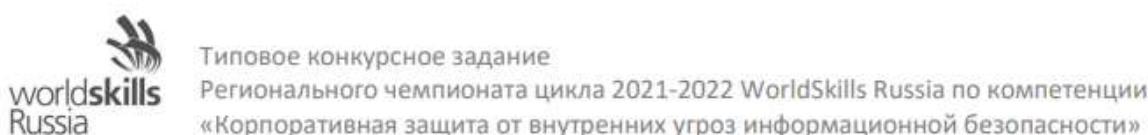
Необходимо поставить на контроль буфер обмена в блокноте и notepad++.

Проверить занесение нескольких событий в WEB-консоль.

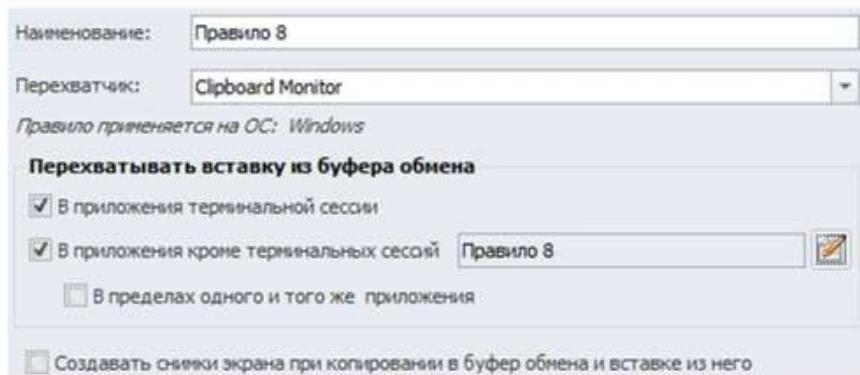
Проверить работоспособность и зафиксировать выполнение скриншотом.

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



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.

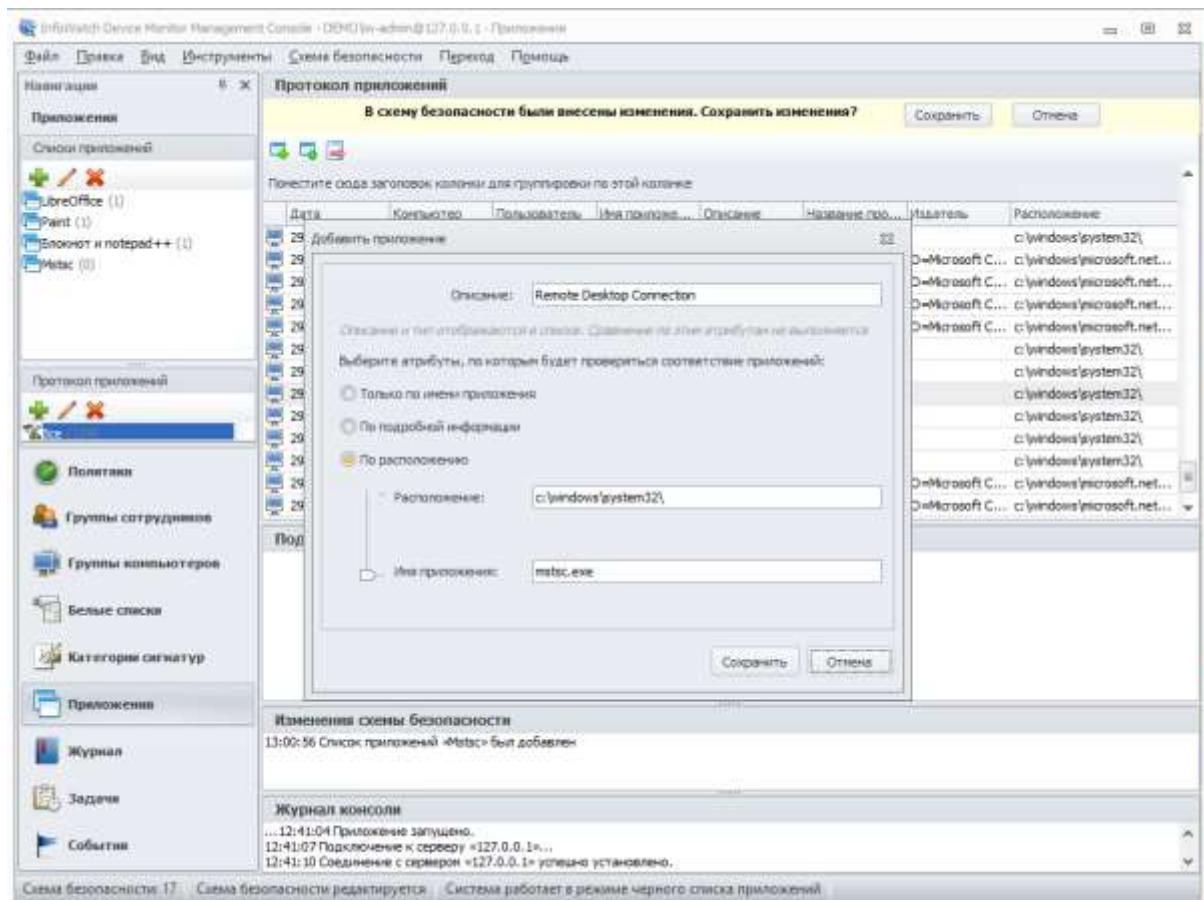


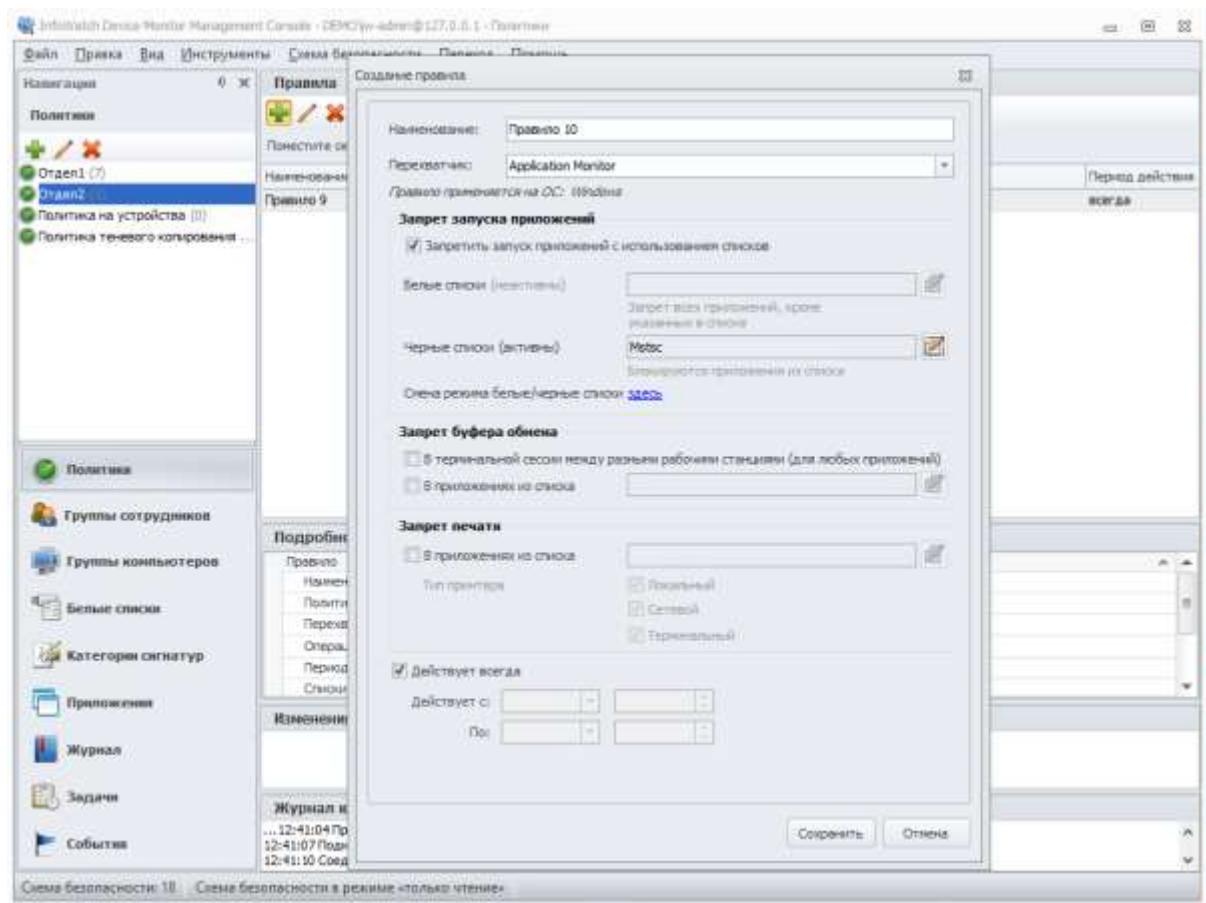
Проверить работоспособность и зафиксировать выполнение скриншотом. Чтобы проверить работоспособность нужно зайти в Device Monitor, затем журнал и там создать фильтр на 1000 записей, только после этого зафиксировать скриншотом

Правило 10

Необходимо запретить использовать терминальные сессии для пользователя.

Проверить работоспособность и зафиксировать выполнение



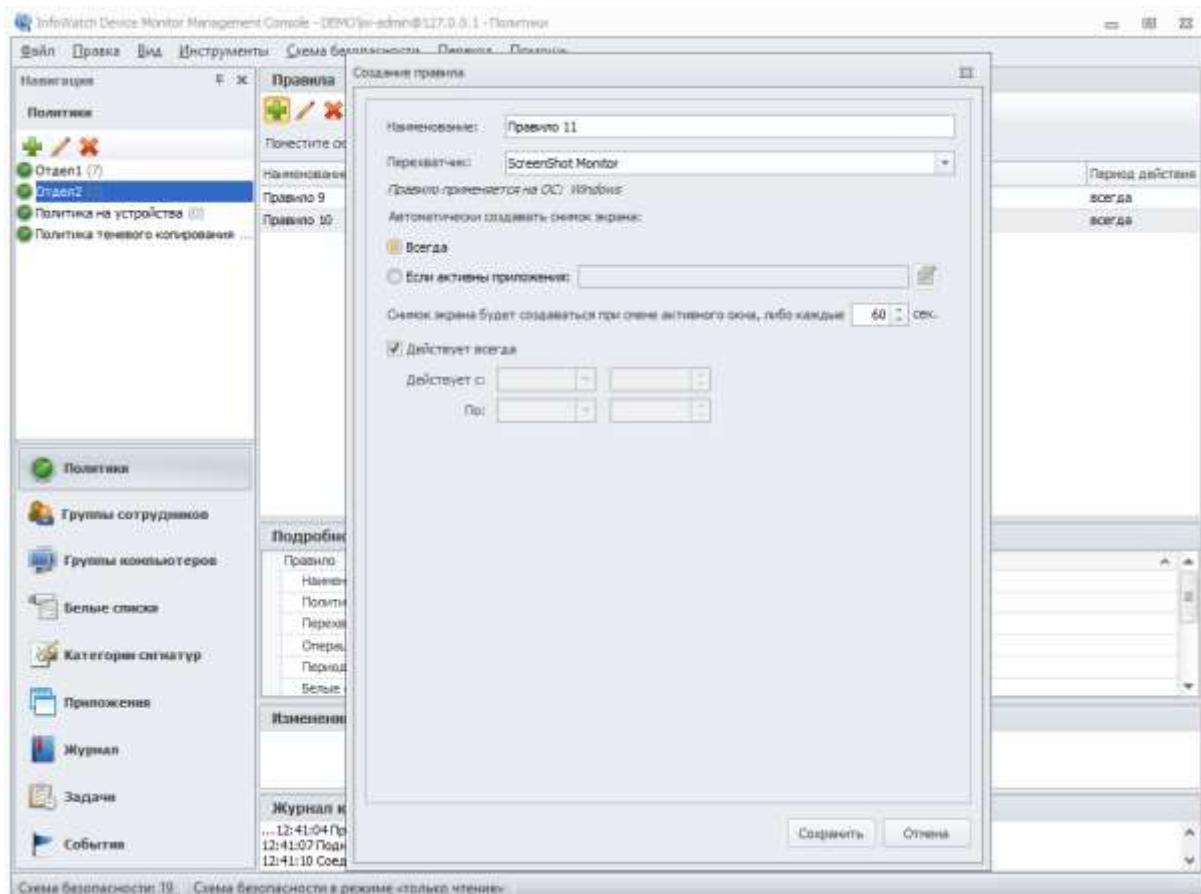


Проверить работоспособность и зафиксировать выполнение!

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

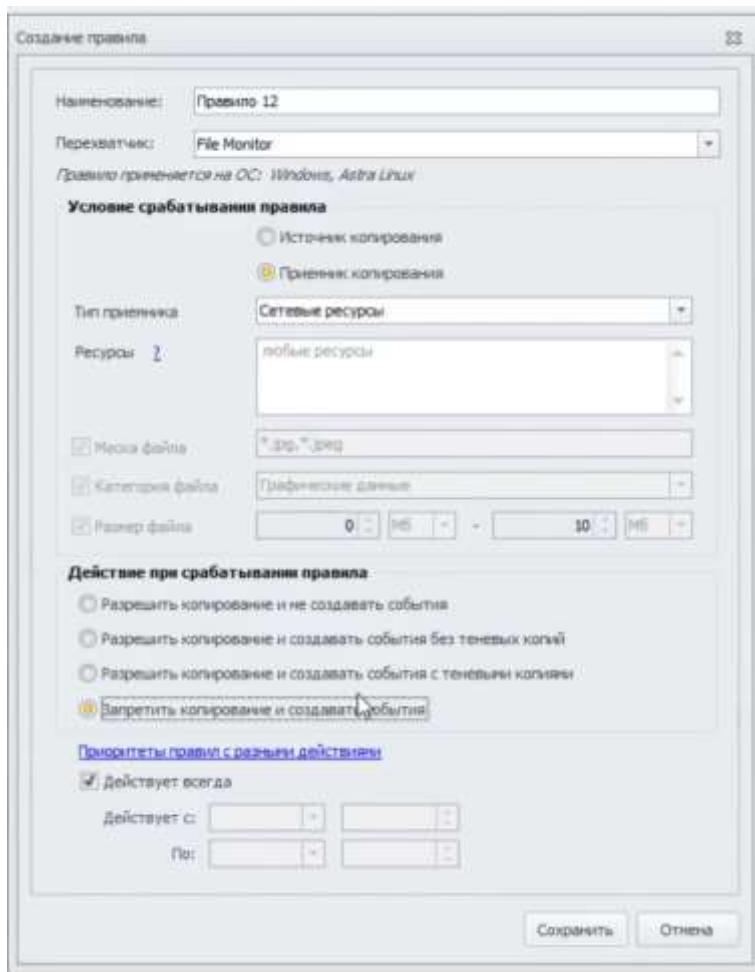
Проверить работоспособность и зафиксировать выполнение

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!

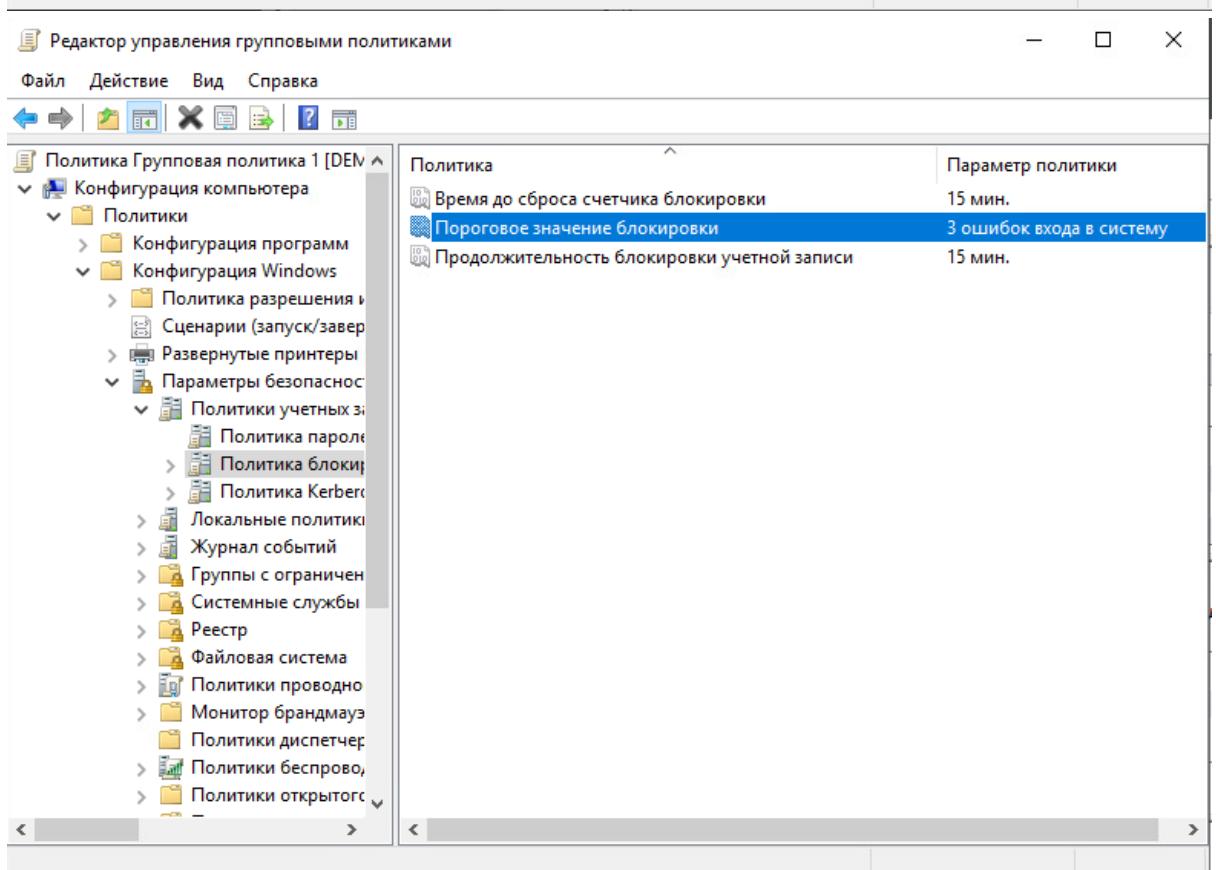
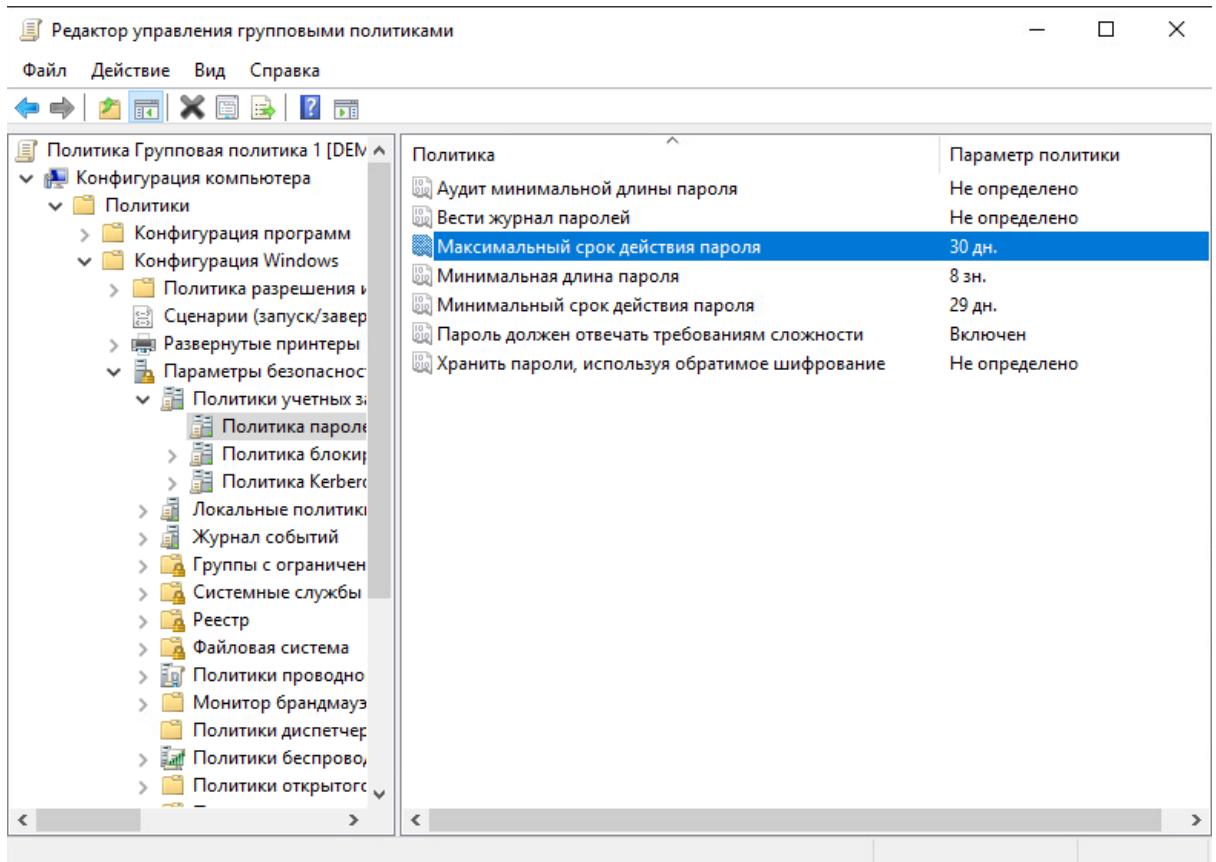
Групповые политики домена

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).

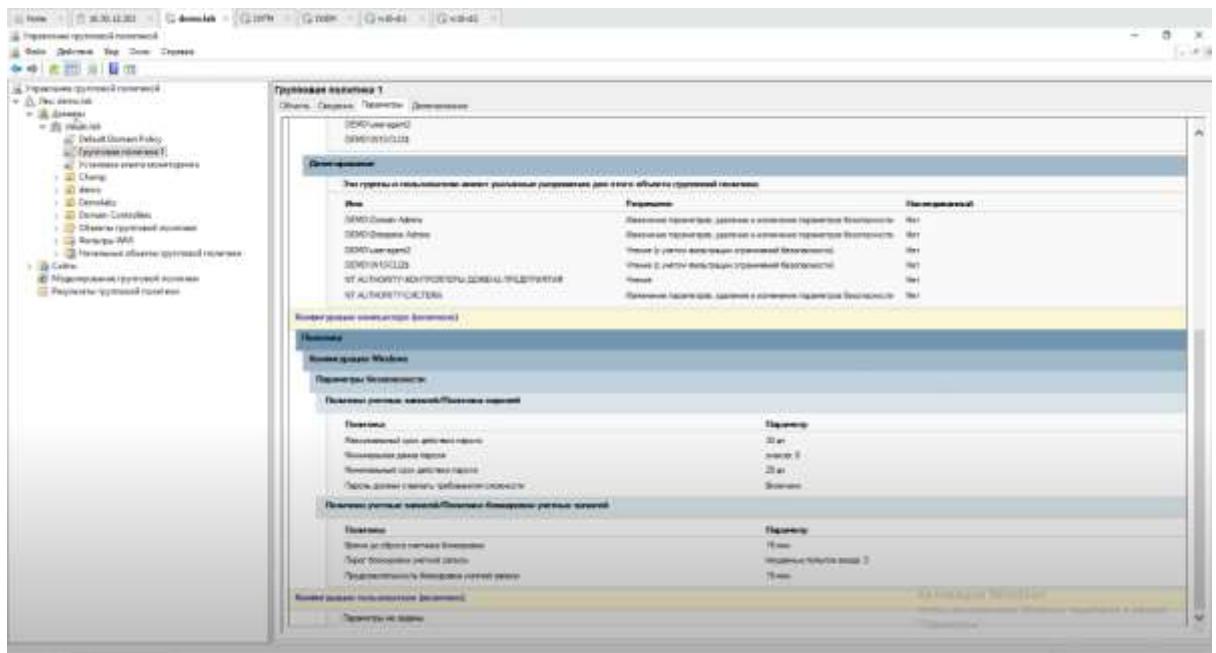
Групповая политика 1

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.



Скриншот



Задокументировать настройки политики скриншотами.

Групповая политика 2

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

Задокументировать 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

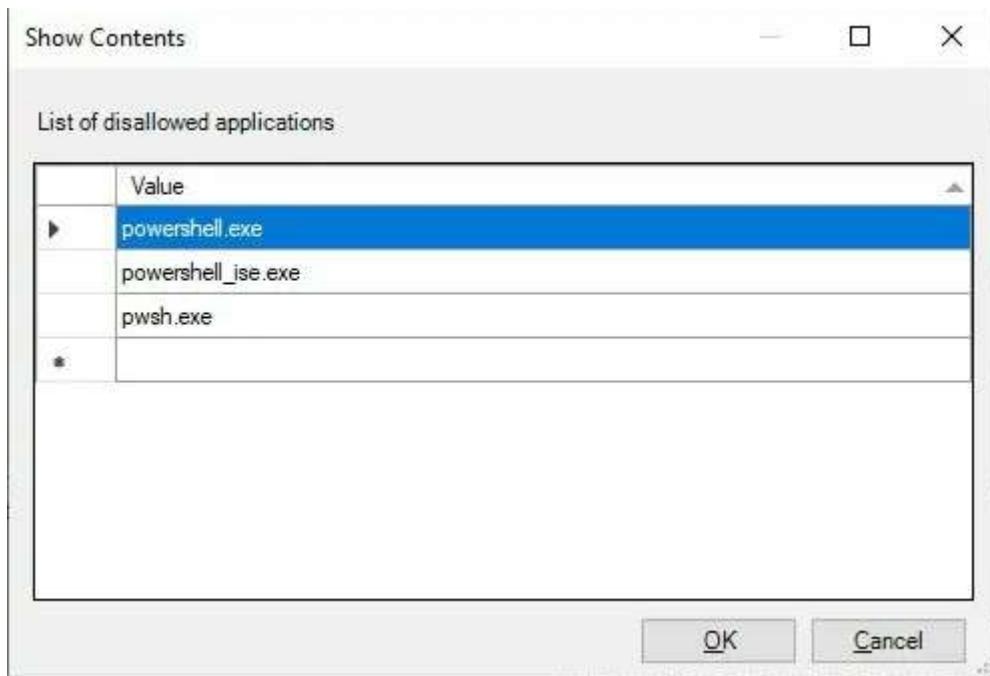
Options:

List of disallowed applications Show...

Help:

Prevents Windows from running applications listed in the policy setting.
If you enable this policy setting, Windows prevents users from running applications listed in the list of disallowed applications.

Нажимаем кнопку → Показать и вводим список команд, запускающих PowerShell

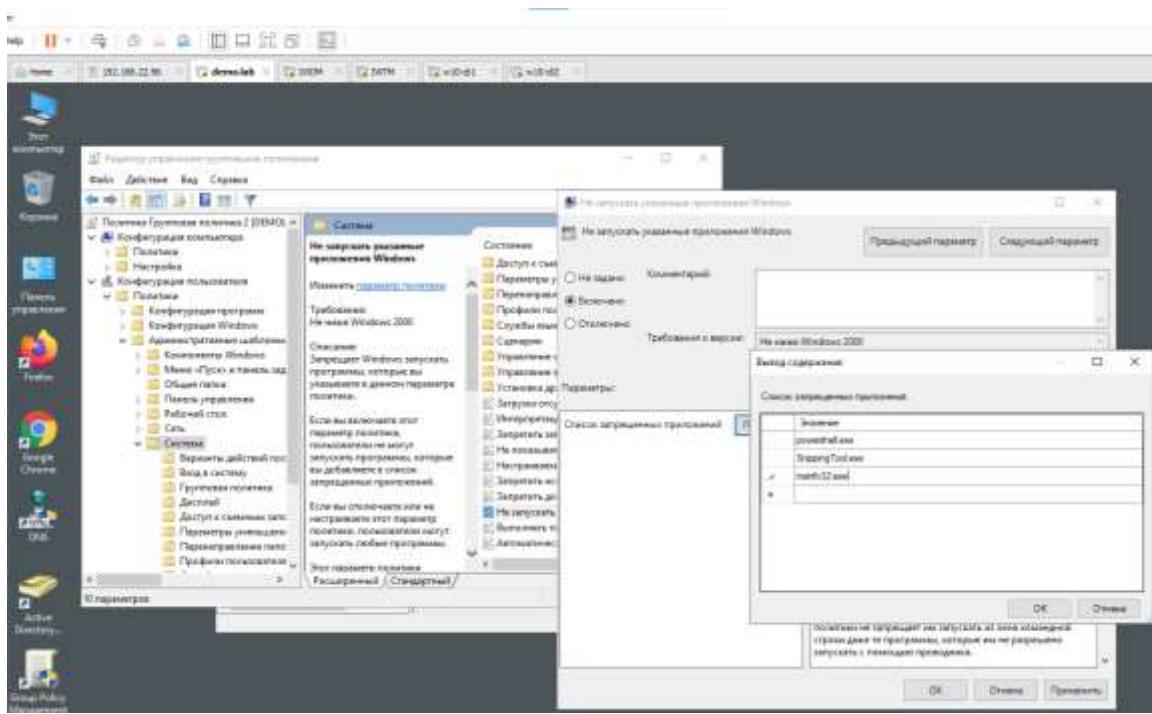


Также вводим ножницы

SnippingTool.exe

И сведения о системе

msinfo32.exe



Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 3

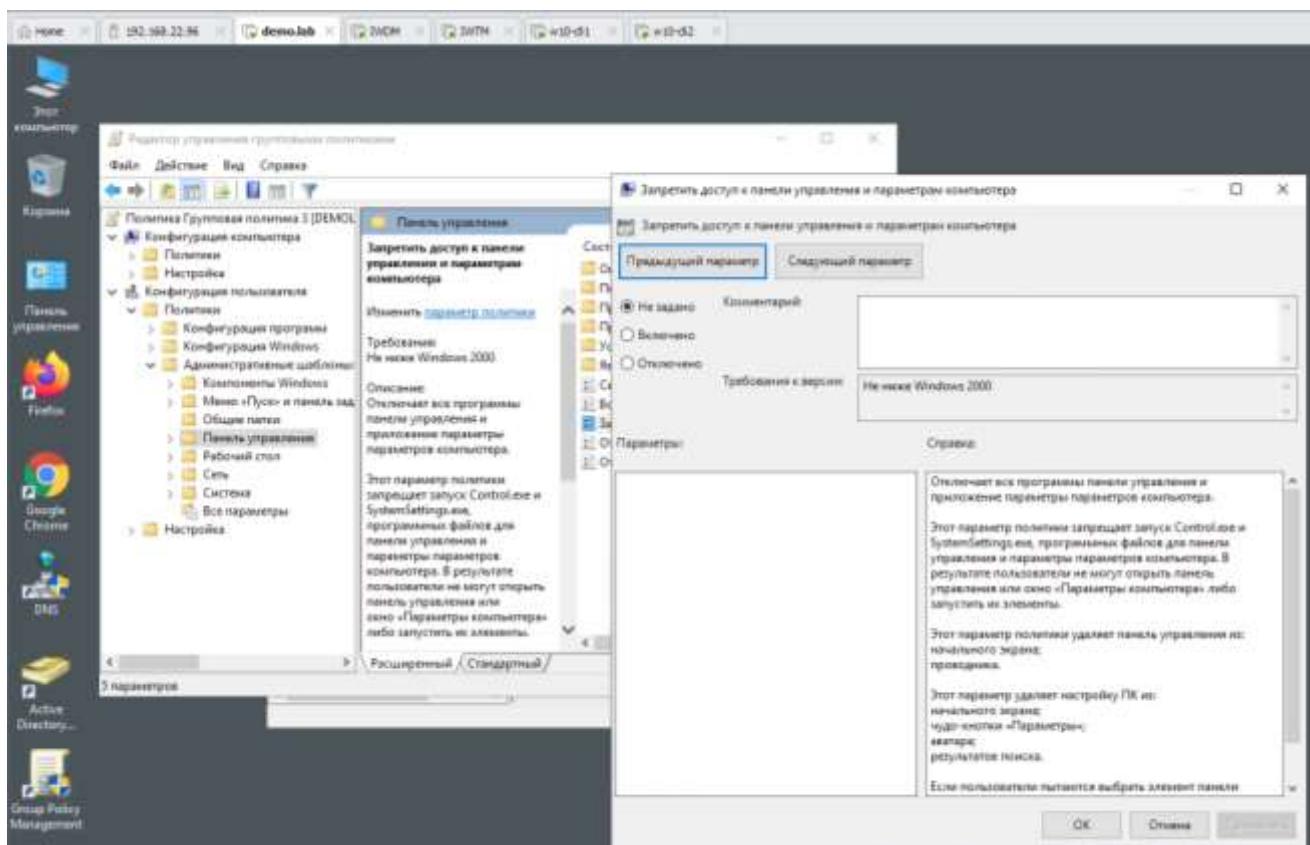
Запретить использование панели управления стандартными политиками.

Задокументировать 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”



Задокументировать настройки политики и выполнение скриншотами.

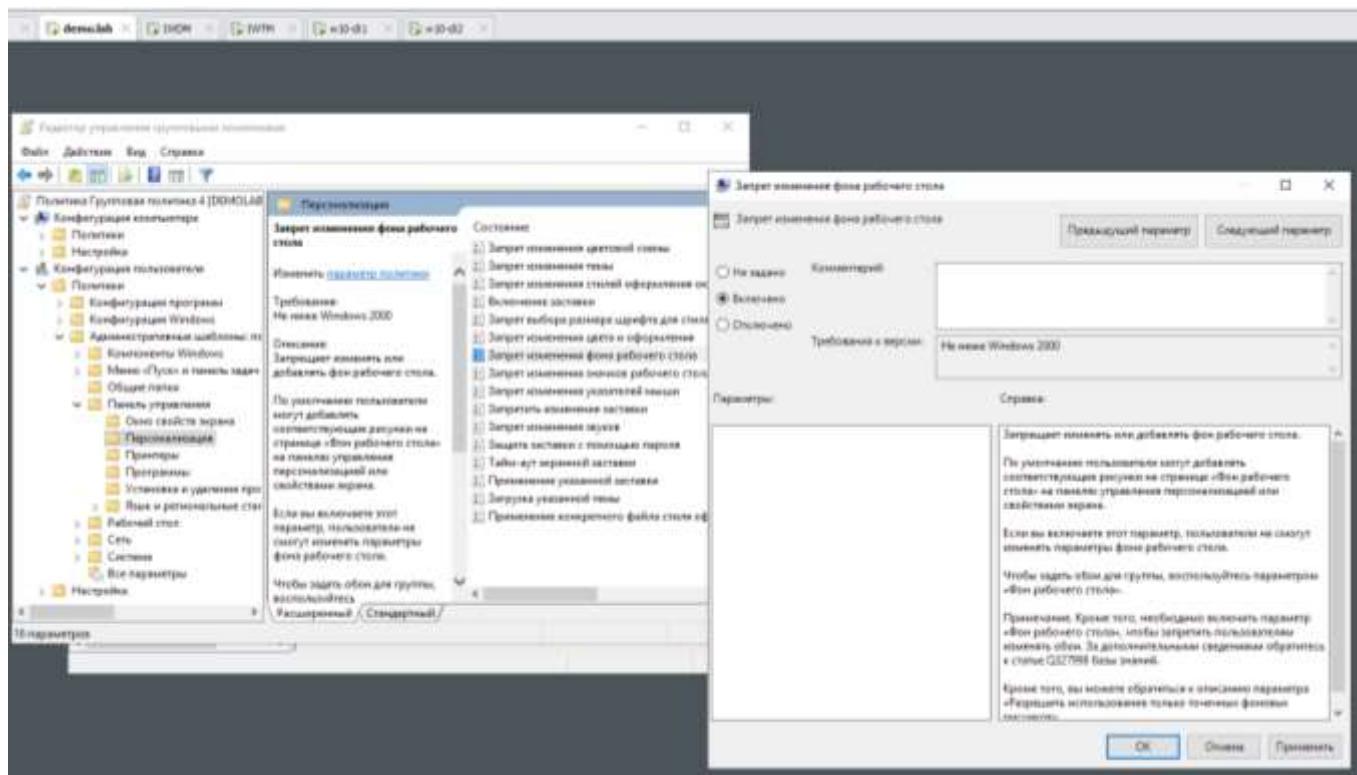
Групповая политика 4

Запретить пользователю самостоятельно менять обои рабочего стола.

Задокументировать настройки политики и выполнение скриншотами.

Конфигурация пользователя → Административные шаблоны – Панель управления – Персонализация.

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



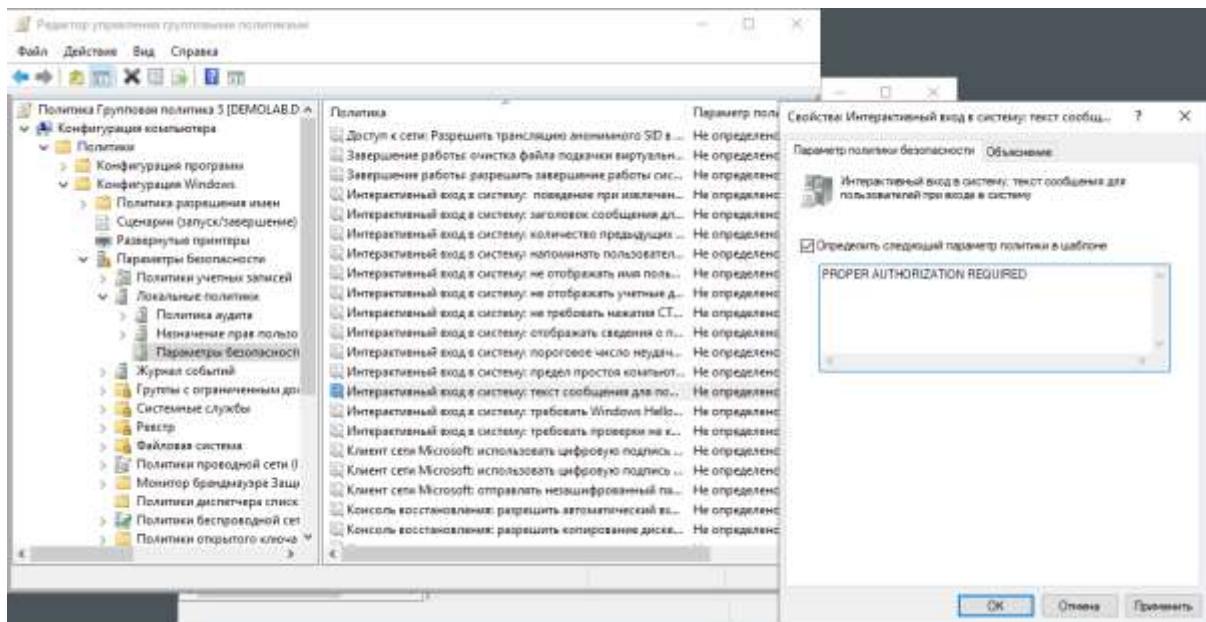
Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 5

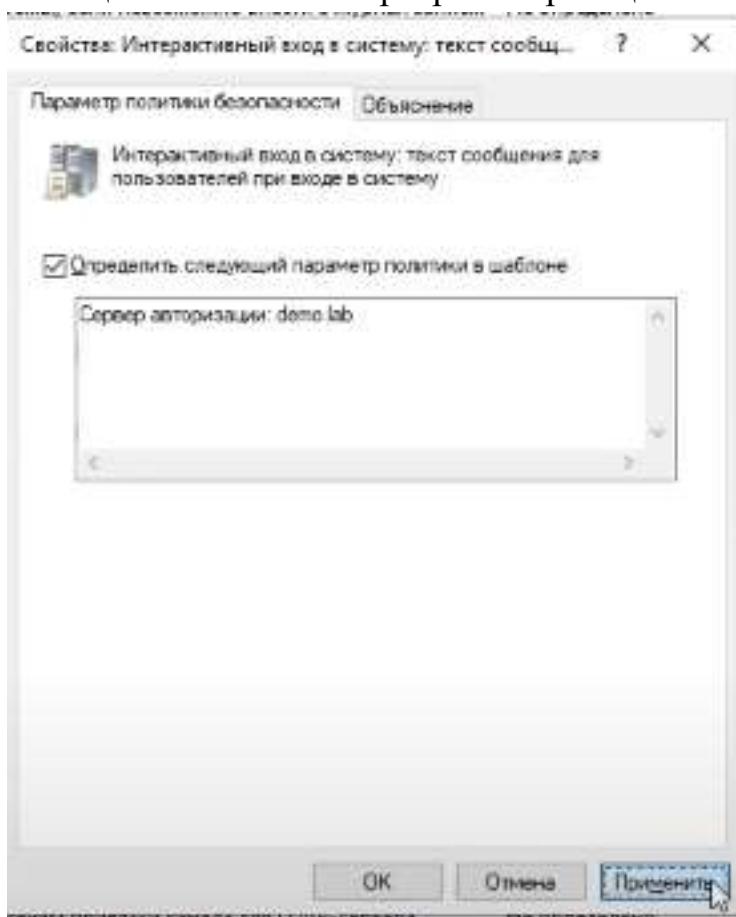
Настроить дополнительные параметры системы, согласно которым при входе на компьютер 2 отображается сообщение с именем сервера авторизации.

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

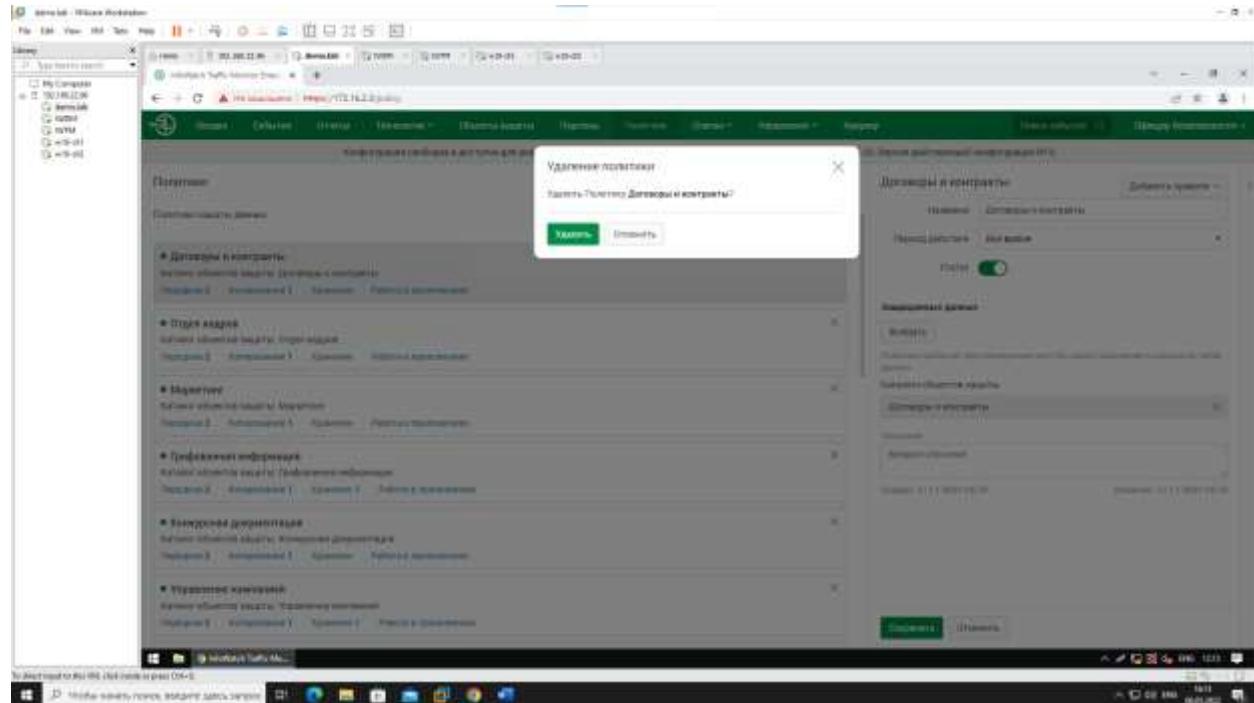


Зафиксировать настройки политики и выполнение скриншотами.

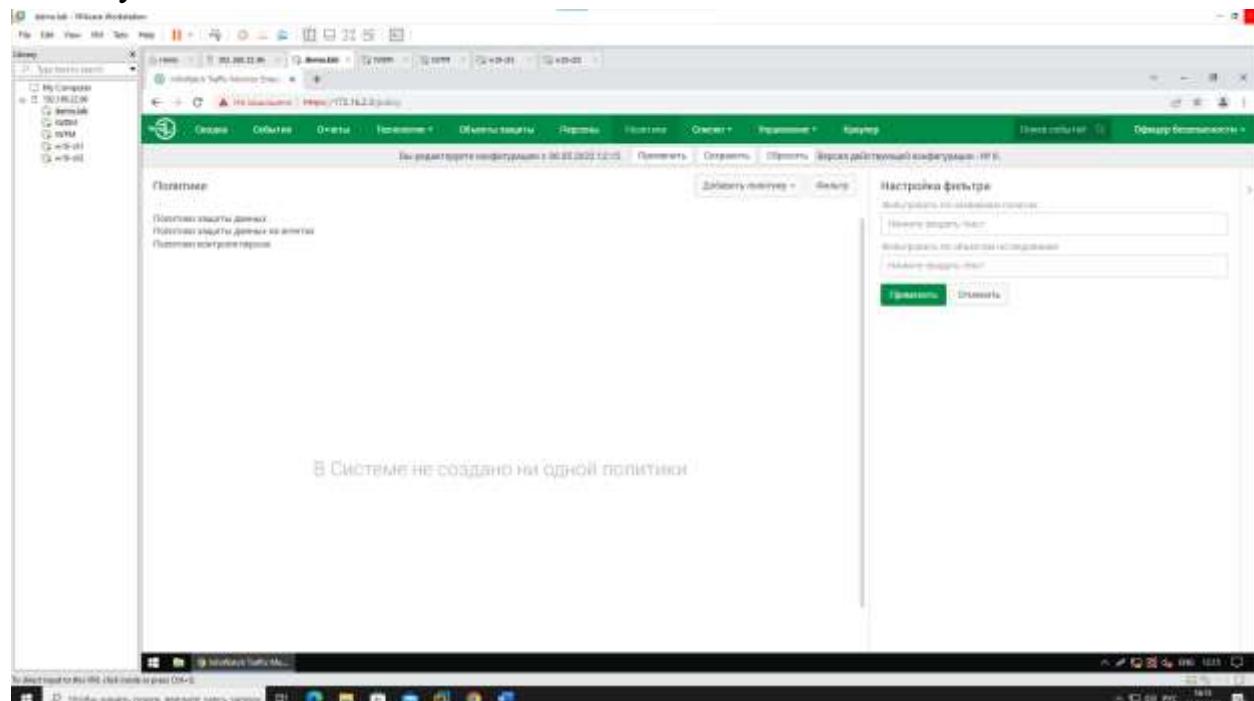
После всего этого применяем групповые политики через cmd → gpupdate /force и смотрим результат: запускаем панель управления на агенте2 и фиксируем работу политики

Модуль 3

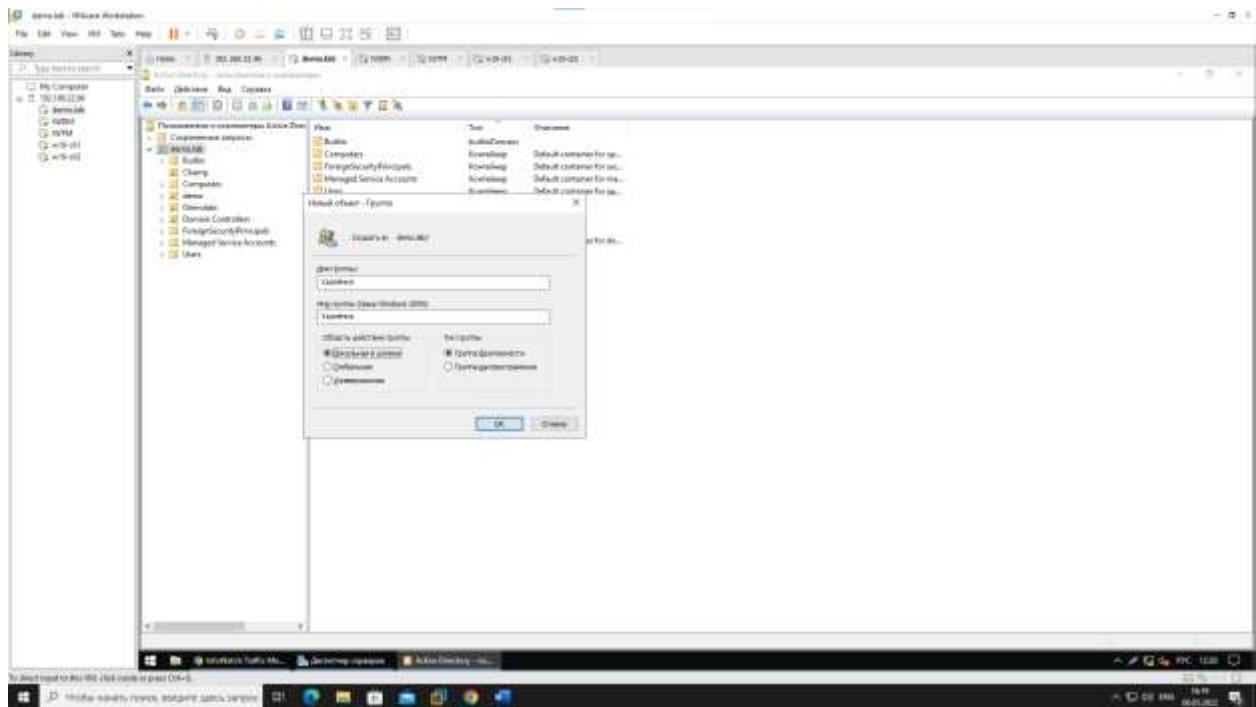
Удаляем все стандартные политики



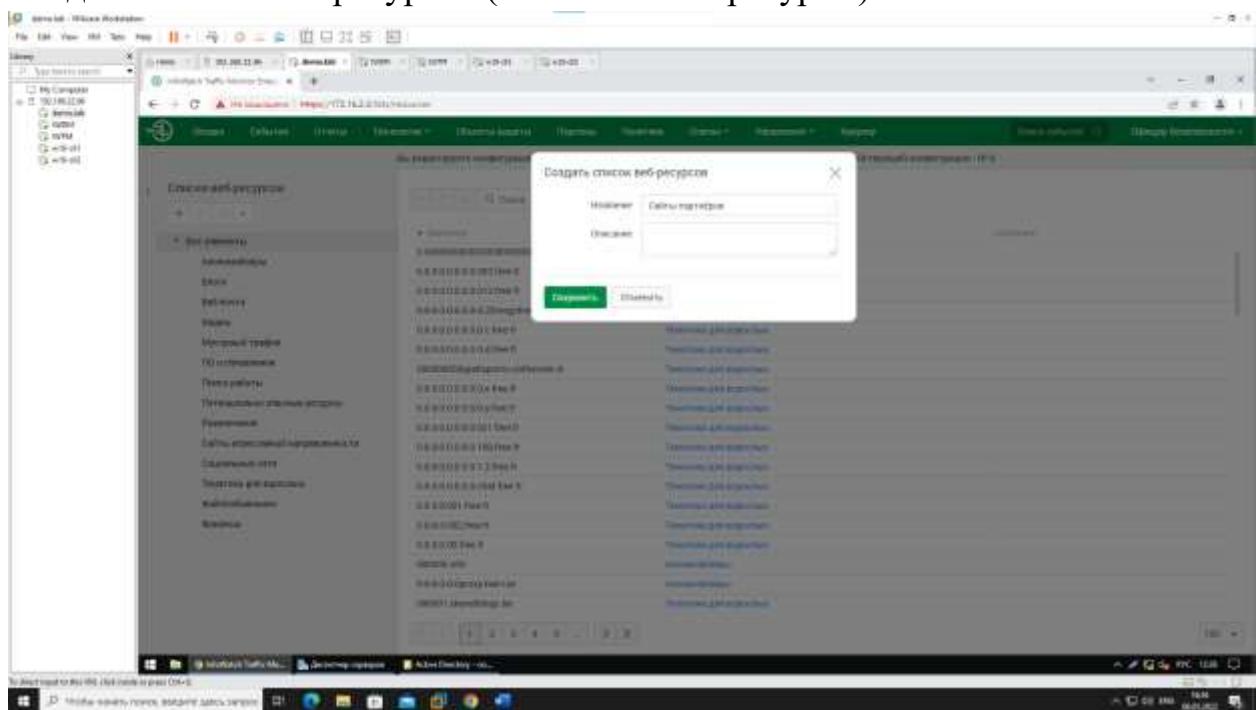
После удаления выглядит вот так



Создаем локальную группу с название – удалёнка



Создаем список веб ресурсов (Списки – Веб-ресурсы)



Добавляем веб-ресурсы

The screenshot shows the Yandex Direct interface. In the foreground, a modal window titled 'Добавить веб-ресурс' (Add website resource) is open, prompting for a 'Название' (Name) and a 'Адресс' (Address). Below this, the main 'Списки веб-ресурсов' (Website resource lists) page is visible. On the left, a sidebar lists various categories under 'Все элементы' (All elements), including 'Лендинг-страницы', 'Блоги', 'Бафф-сайты', 'Медиа', 'Мусорный трафик', 'По изображениям', 'Поиск работы', 'Потенциальные новые ресурсы', 'Радиошоу', and 'Сайты агрессивной направленности'. The main area displays a table titled 'Сайты партнёров' (Partnership websites) with columns for 'Сайт' (Site), 'Статус' (Status), and 'Последнее обновление' (Last update). The table lists three sites: 'infoteleco.ru' (Status: Проверено), 'ITAP' (Status: Проверено), and 'vennare.com' (Status: Проверено).

Задание 4

Периметр компании

InfoWatch Traffic Monitor Enterprise

← → ⌂ □ Не защищено | https://172.16.2.3/lists/perimeters/0B08E6E5DCF826A7ED533D003C0A403100000000

Сводка События Отчеты Технологии Объекты защиты Персоны Политики Списки Управление Краупер

Вы редактируете конфигурацию с 06.05.2022 12:15. Применить Сохранить Сбросить Версия действ.

Периметры Редактирование

+ ×

Исключить из перехвата

Компания

Название: Компания

Почтовый домен: demo.lab

Список веб-ресурсов: Сайты партнёров

Группа персон: Удалёнка

Использовать только рабочие контакты

Добавить

Описание: Персоны и компьютеры компании. Используется для контроля информации, передаваемой за периметр компании.

Создан: 17.11.2021 05:29 Изменен: 17.11.2021 05:29

Сохранить Отменить

Исключение из перехвата

InfoWatch Traffic Monitor Enterprise

← → ⌂ □ Не защищено | https://172.16.2.3/lists/perimeters/0B08E6E5DCF826A7ED533D003C0A403200000000

Сводка События Отчеты Технологии Объекты защиты Персоны Политики Списки Управление Краупер

Вы редактируете конфигурацию с 06.05.2022 12:15. Применить Сохранить Сбросить Версия действ.

Периметры Редактирование

+ ×

Исключить из перехвата

Компания

Название: Исключить из перехвата

Персона: Komilov V. Fedosej

Использовать только рабочие контакты

Добавить

Описание: Если включена политика 'Исключить из перехвата', то почтовые сообщения, отправленные входящими в данный периметр персонами,

Создан: 17.11.2021 05:29 Изменен: 17.11.2021 05:29

Сохранить Отменить

В ПОСЛЕДНЮЮ ОЧЕРЕДЬ

Политика 3

Технологии – Эталонные документы, создаем политику в эталонных документах

The screenshot shows the InfoWatch Traffic Monitor Enterprise web interface. In the top navigation bar, the URL is https://172.16.2.3/analysis/fingerprint/C22CCFBA68D92C239A058860E56021EC00000000. The main menu includes 'Сводка', 'События', 'Отчеты', 'Технологии', 'Объекты защиты', 'Персоны', 'Политики', 'Список', 'Управление', and 'Краудр'. A modal window titled 'Создать' (Create) is open, prompting for a name ('Название') which is set to 'Политика 3'. It also contains settings for 'Порог цитируемости для текстовых данных' (Text data citation threshold) at 10% and 'Порог цитируемости для бинарных данных' (Binary data citation threshold) at 50%. There is a note 'Добавить описание' (Add description) and two buttons at the bottom: 'Создать' (Create) and 'Отменить' (Cancel).

На основе всех типов данных

The screenshot shows the InfoWatch Traffic Monitor Enterprise web interface. The URL is https://172.16.2.3/analysis/fingerprint/C5AE72383BB242BEA47AE8. The main menu is identical to the previous screenshot. A modal window titled 'Вы редактируете конфигурацию с 06.0' (You are editing configuration 06.0) is open, showing the configuration for 'Политика 3'. The configuration details are: 'На основе текстовых данных' (Based on textual data) and 'На основе всех типов данных' (Based on all data types). The left sidebar shows 'Каталоги эталонных документов' (Catalogs of reference documents) with a search bar and a list of elements: 'Все элементы' (All elements), 'Автоматические эталонные документы...' (Automatic reference documents...), and 'Эталонные документы' (Reference documents). The element 'Политика 3' is currently selected.

Добавляем картинку котика

Сводка События Отчеты Технологии + Объекты защиты Персоны Политики Списки + Управление Краткое меню Помощь Помощь Справка + История + Краткое меню Поиск системы Официр Безопасности

Вы редактируете конфигурацию с 06.05.2023 12:15 - Применить Сохранить Отменить Версия действующей конфигурации - IP 9.

Каталоги эталонных документов

Политика 3

+ - Q. Показать

Название Текущий район Несущий район Ранее район Дата создания Источник

Название Название района Несущий район Ранее район Дата создания Источник

Название Название района Несущий район Ранее район Дата создания Источник

Политика 3

Все элементы

автоматически загруженные документы

эталонные документы

Политика 3

Загрузка технологий

Стандартные документы

Каталог ✓ Сохранено

Добавляем объекты защиты

Сводка События Отчеты Технологии + Объекты защиты Персоны Политики Списки + Управление Краткое меню Помощь Помощь Справка + История + Краткое меню Поиск системы Официр Безопасности

Вы редактируете конфигурацию с 06.05.2023 12:15 - Применить Сохранить Отменить Версия действующей конфигурации - IP 9.

Каталоги объектов защиты

Создать

Название: Политика 3

Статус: вкл.

Описание:

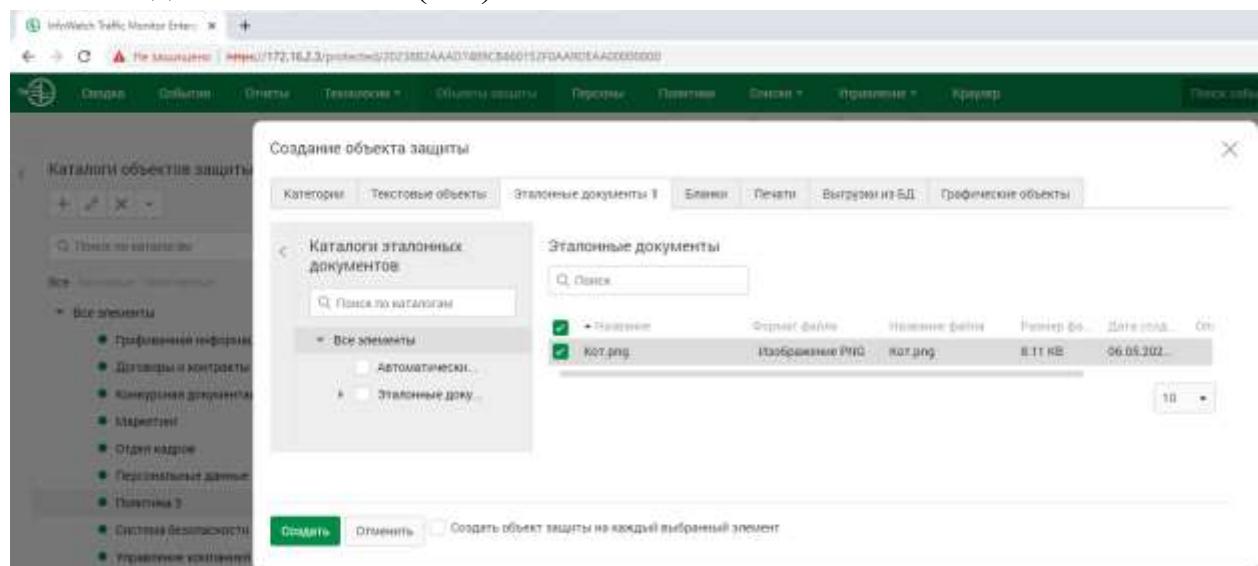
Создать Отменить

Все элементы

Название

- Активы и бюджетированное управление
- Базы данных
- Бухгалтерская отчетность
- Графы конфиденциальности
- Графы секретности
- Документы

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



Условием – выбираем кортику Кота

The screenshot shows the 'Create Protection Object' dialog box for 'Policy 3'. It includes sections for 'Name' (Polityka 3), 'Status' (Enabled), 'Technology Elements' (selected), 'Detection Conditions' (empty), 'Add Condition' button, 'Condition' dialog (showing 'Kot.rpd' selected), 'Description' field (empty), and 'Create' and 'Cancel' buttons.

Вот так

Вы редактируете конфигурацию с 06.03.2022 12:15. Редактировать Сохранить Обратить в версию действующей конфигурации - IP 9.

Каталог объектов защиты

Политика З

Название	Описание (текущий)	Дата создания	Дата изменения	Управление
Софт Клиент	Хотят	06.03.2022 12:07	06.03.2022 12:07	
Софт Клиент 2	Хотят	06.03.2022 12:07	06.03.2022 12:07	

+ Все

Софт Клиент
Софт Клиент 2

Все элементы

- Графическая информация
- Документы и контракты
- Конфиденциальная документация
- Маркетинг
- Отдел кадров
- Персональные данные
- Политики

Списки – Теги, создаем новый тег

InfoWatch Traffic Monitor Enterprise x +

← → G ▲ Не защищено | https://172.16.23/lists/tag

Сводка События Отчеты Технологии Объекты защиты Персоны Политики Списки Управление Краткое

Вы редактируете конфигурацию с 06.03.2022 12:15. Редактировать Сохранить Обратить в версию действующей конфигурации - IP 9.

Управление тегами

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

+

Назначение VIP На рассмотрение

Создать тег

Название Политика З Цвет

Описание

Сохранить Отменить

Переходим в политики, создаем политику защиты данных

Вы редактируете конфигурацию с 06.03.2022 12:15. Редактировать Сохранить Обратить в версию действующей конфигурации - IP 9.

Политики

Политики защиты данных

Политика защиты данных

Политика защиты данных

Добавить политику | Фильтр | Политика защиты данных

Название Политика защиты данных

Период действия Всё время

Статус

Заданные данные

Выбрать Политика действует на выбранные данные пока не сделан выбор

Создан 06.03.2022 12:02 Изменен 06.03.2022 12:10

Сохранить Отменить

Добавляем правило передачи

Правило передачи

Правила защиты данных

• Политика защиты данных

Политика на основе данных

Передача изображения звуковая работа и приватная

Добавить правило

Отправитель: Любой отправитель

Напечатано наружу: Нет

Удалить: Да

Изменить: Да

Работа с правами: Да

Добавить правило: Да

Действия по получению: Да

Правило передачи

Компьютеры: СЕРВИС X, КЛИЕНТ X, КЛИЕНТ X, DEMO-00 X, DEMO-01 X, DEMO-02 X, DEMO-03 X

Файл: Отправить сообщение

Сообщение: Установить конфиденциальность

Действие: Установить конфиденциальность

Действие для срабатывания правила:

Отправить сообщение: Установить конфиденциальность

Напечатать сообщение: Нет

Установить конфиденциальность: Нет

Изменить сообщение: Нет

Установить конфиденциальность: Правила З-К

Напечатать сообщение: Выбрать статус

Удалить сообщение: Выбрать статус

Создать

Закрыть

Политика 5

Переходим в объекты защиты и создаем новый объект защиты

Вы редактируете конфигурацию

Каталоги объектов защиты

+ -

Поиск по каталогам

Все: Активы и бюджетирование

• Все элементы

- Финансы
- Управление компаний
- Грифованная информация

Создать

Название: Политика 5

Статус: Активен

Описание:

Создать

Отменить

Добавляем

Создание объекта защиты

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

🔍 Поиск

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

🔍 Поиск по каталогам

Все элементы Текстовые объе...

Текстовые объекты

🔍 Поиск

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

К < 1 2 3 4 > >>

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

10

Создать Отменить Создать объект защиты на каждый выбранный элемент.

Вот так выглядит

Вы редактируете конфигурацию с 05.01.2023 12:16. Примите Сохраните Отменить (Берет действующий инфопакет, ID: 6)

Политика S

Название	Элементы текущей	Создано	Обновлено
Графический объект: кредитная карта	кредитная карта	06.05.2022 12:16	06.05.2023 12:16
Текстовый объект: Номер кредитной карты	Номер кредитной карты	06.05.2022 12:16	06.05.2023 12:16
Текстовый объект: Номер кредитной карты (16 цифр)	Номер кредитной карты (16 цифр)	06.05.2022 12:16	06.05.2023 12:16

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 'Policy' configuration screen in a software application. At the top, there are tabs for 'Справка', 'События', 'Очаги', 'Текущие', 'Объекты мониторинга', 'Переводы', 'Планы', 'Окна', 'Управление', 'Кратко', 'Линк событий', and 'Офицер безопасности'. The main area displays two policy configurations:

- Политика защиты данных:** A window titled 'Политика защиты данных №1' with tabs for 'Предмет', 'Использование', 'Правила', and 'Работа с приложениями'. It contains sections for 'Правило передачи' (Delivery rule) and 'Правило защиты данных' (Data protection rule).
- Правило защиты данных №1:** A detailed view of the data protection rule, showing conditions like 'Любой отправитель' (Any sender) and 'Любой получатель' (Any recipient), and actions like 'Напечатать' (Print).

On the right side, there is a 'Заданные данные' (Defined data) section with a 'Выбрать' (Select) button, and a 'Правило передачи' (Delivery rule) section with a 'Создано' (Created) field showing '03.05.2022 10:18' and an 'Изменено' (Modified) field showing '03.05.2022 10:18'. At the bottom are 'Сохранить' (Save) and 'Отменить' (Cancel) buttons.

Правило передачи

The screenshot shows the 'Delivery Rule' configuration screen in the same software application. The top tabs are identical to the previous screen. The main area displays the 'Правило передачи' (Delivery rule) configuration:

- Правило передачи:** A window titled 'Правило передачи' with tabs for 'Направление', 'Тема события', 'Компьютеры', 'Отправители', 'Получатели', 'Дни действия правила', and 'Часы действия правила'. It includes fields for 'Направление' (Direction) set to 'В одну сторону' (One-way), 'Тема события' (Event topic) set to 'Тема', 'Компьютеры' (Computers) showing 'CLIENT1' and 'CLIENT2', and 'Отправители' (Senders) and 'Получатели' (Recipients) both set to 'Напечатать текст' (Print text).
- Действия при срабатывании правила:** A table showing actions triggered by the rule:

Исправить текстовую информацию	Напечатать текст
<input checked="" type="checkbox"/> Напечатать	<input checked="" type="checkbox"/> Разрешить
<input checked="" type="checkbox"/> Напечатать события (если есть)	<input checked="" type="checkbox"/> Скрыть
<input checked="" type="checkbox"/> Напечатать обобщенное ТБ	<input checked="" type="checkbox"/> Пометка №1
<input checked="" type="checkbox"/> Назначить отправителю статус	<input checked="" type="checkbox"/> Выберите статус

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

Вот так должно получиться

The screenshot shows the InfoWatch Traffic Monitor Enterprise interface. The main window displays two policy configurations: 'Политика 5' and 'Политика 2'. Policy 5 is selected and expanded, showing rules for traffic from 'Любой отправитель' to 'Любой получатель' through ports 'CLIENT1' and 'CLIENT2'. Policy 2 is also listed. On the right side of the interface, there is a detailed view of a 'Правило передачи' (Forwarding rule) with fields for 'Направление' (Direction), 'Тип действия' (Action type), 'Компьютеры' (Computers), 'Отправители' (Senders), 'Получатели' (Recipients), 'Длительность правила' (Rule duration), and 'Часы действия правила' (Rule hours). Below this, a section titled 'Действия при срабатывании правила' (Actions on rule trigger) lists actions like 'Начните передачу трафика' (Start traffic transmission), 'Разрешить' (Allow), 'Запретить' (Ban), and 'Сбросить' (Reset). At the bottom right are 'Создать' (Create) and 'Отменить' (Cancel) buttons.

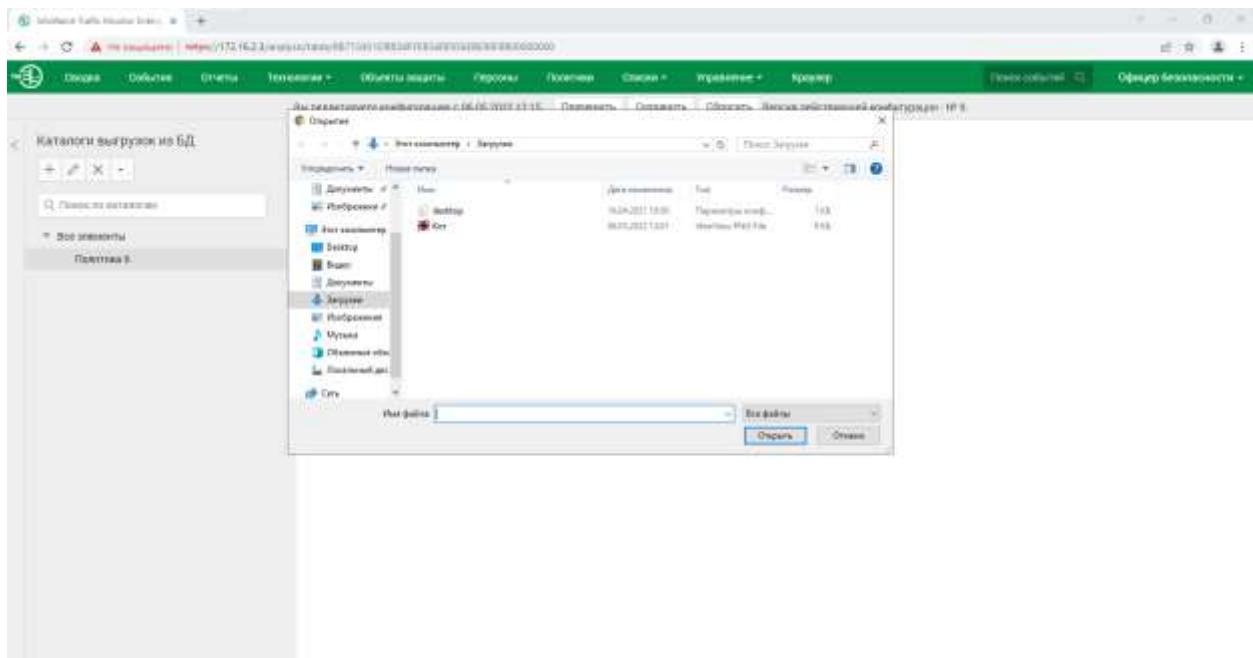
Политика 6

Переходим, технологии – выгрузки из бд

Создаем каталог

The screenshot shows the 'Catalogs' section of the InfoWatch Traffic Monitor Enterprise interface. On the left, a sidebar lists 'Каталоги выгрузок из БД' (Export catalogs from DB) and a search bar. The main area shows a 'Создать' (Create) dialog box for a new catalog. The dialog has fields for 'Название' (Name) set to 'Политика 6', 'Описание' (Description) with placeholder 'Добавить описание' (Add description), and 'Создать' (Create) and 'Отменить' (Cancel) buttons at the bottom. The background shows a list of 'Все элементы' (All elements).

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

+ / -	Условие по зада...	Правило	Минимальное ко...
	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.

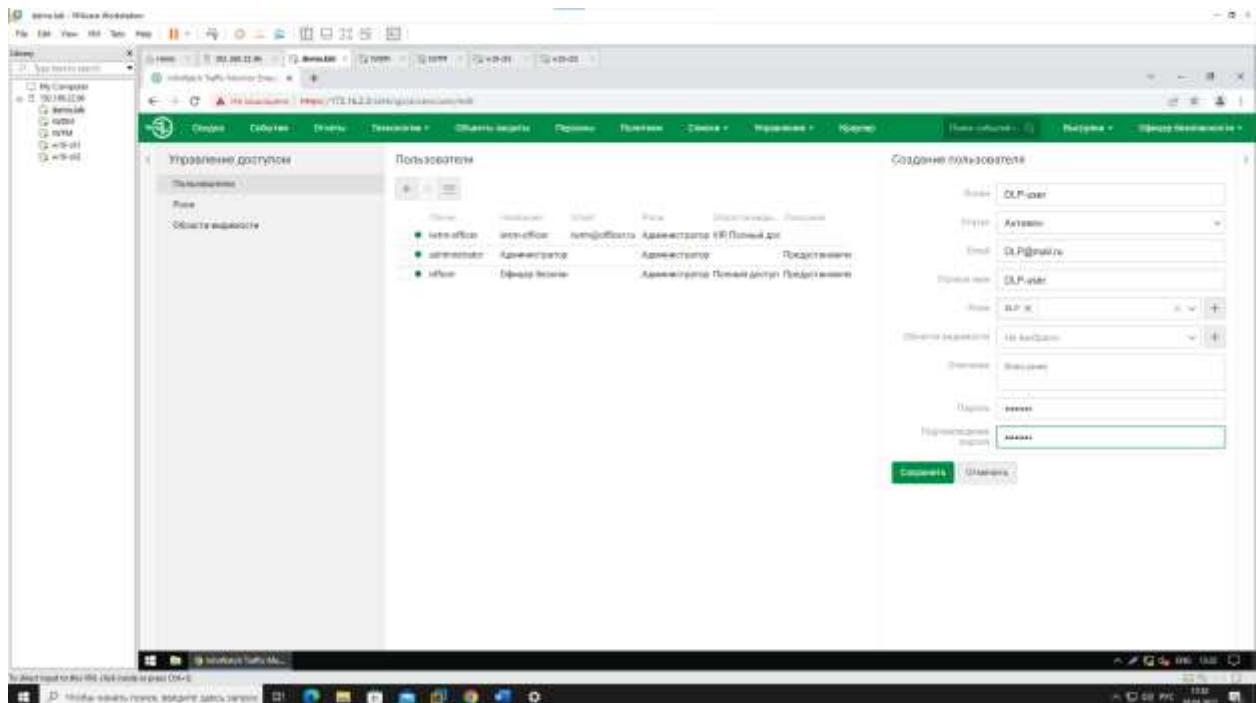
Правило передачи	
Направление маршрута	→ В одну сторону ↳ В оба направления
Тип события	Тип <input type="button" value="▼"/>
Компьютеры	Начните вводить текст <input type="text"/> <input type="button" value="+"/>
Отправители	= <input type="button" value="▼"/> Начните вводить текст <input type="text"/> <input type="button" value="+"/>
Получатели	= <input type="button" value="▼"/> Начните вводить текст <input type="text"/> <input type="button" value="+"/>
Дни действия правила	Любой день недели <input type="button" value="▼"/>
Часы действия правила	0:00 <input type="button" value="⌚"/> - 0:00 <input type="button" value="⌚"/>
Действия при срабатывании правила	
Отправить почтовое уведомление	Начните вводить текст <input type="text"/> <input type="button" value="+"/>
Назначить событию вердикт	<input checked="" type="checkbox"/> Разрешить <input type="button" value="▼"/>
Назначить событию уровень нарушения	<input checked="" type="radio"/> Низкий <input type="button" value="▼"/>
Назначить событию теги	Политика 3 <input type="text"/> <input type="button" value="+"/>
Назначить отправителю статус	Выберите статус <input type="button" value="▼"/>
Удалить событие <input type="button" value="Toggle"/>	

Рисунок 86 – «Правило передачи политики 3»

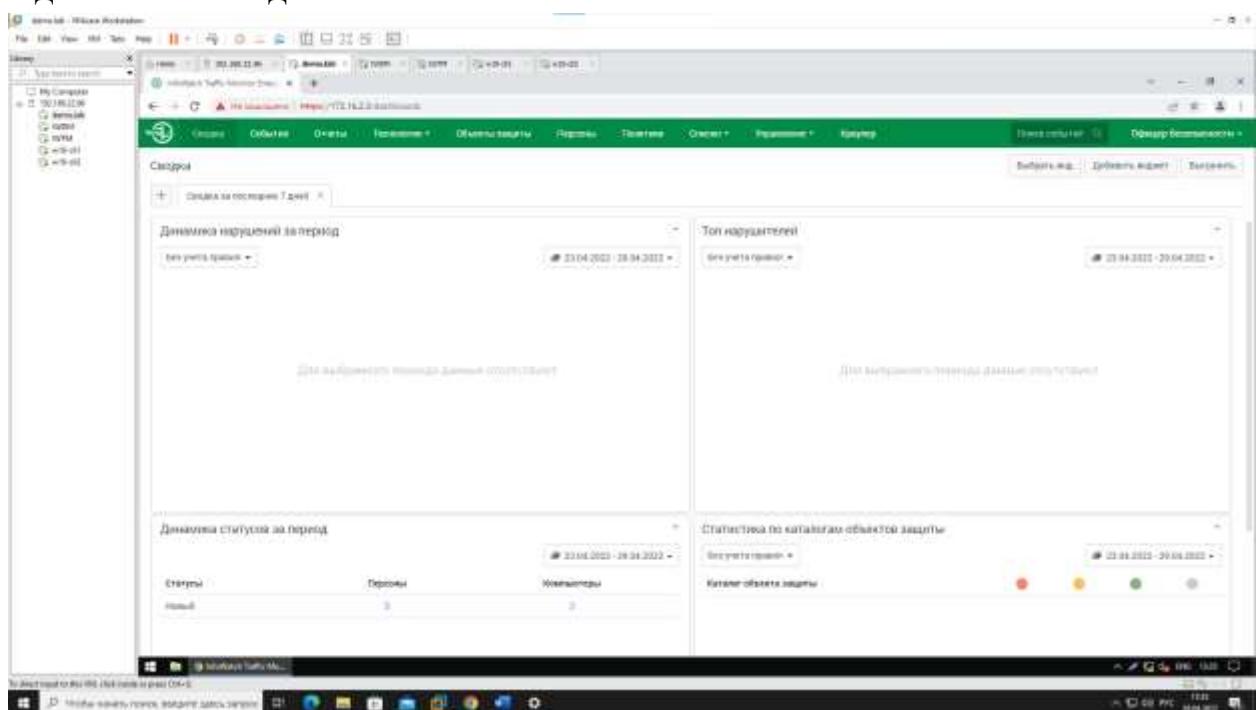
Модуль 4

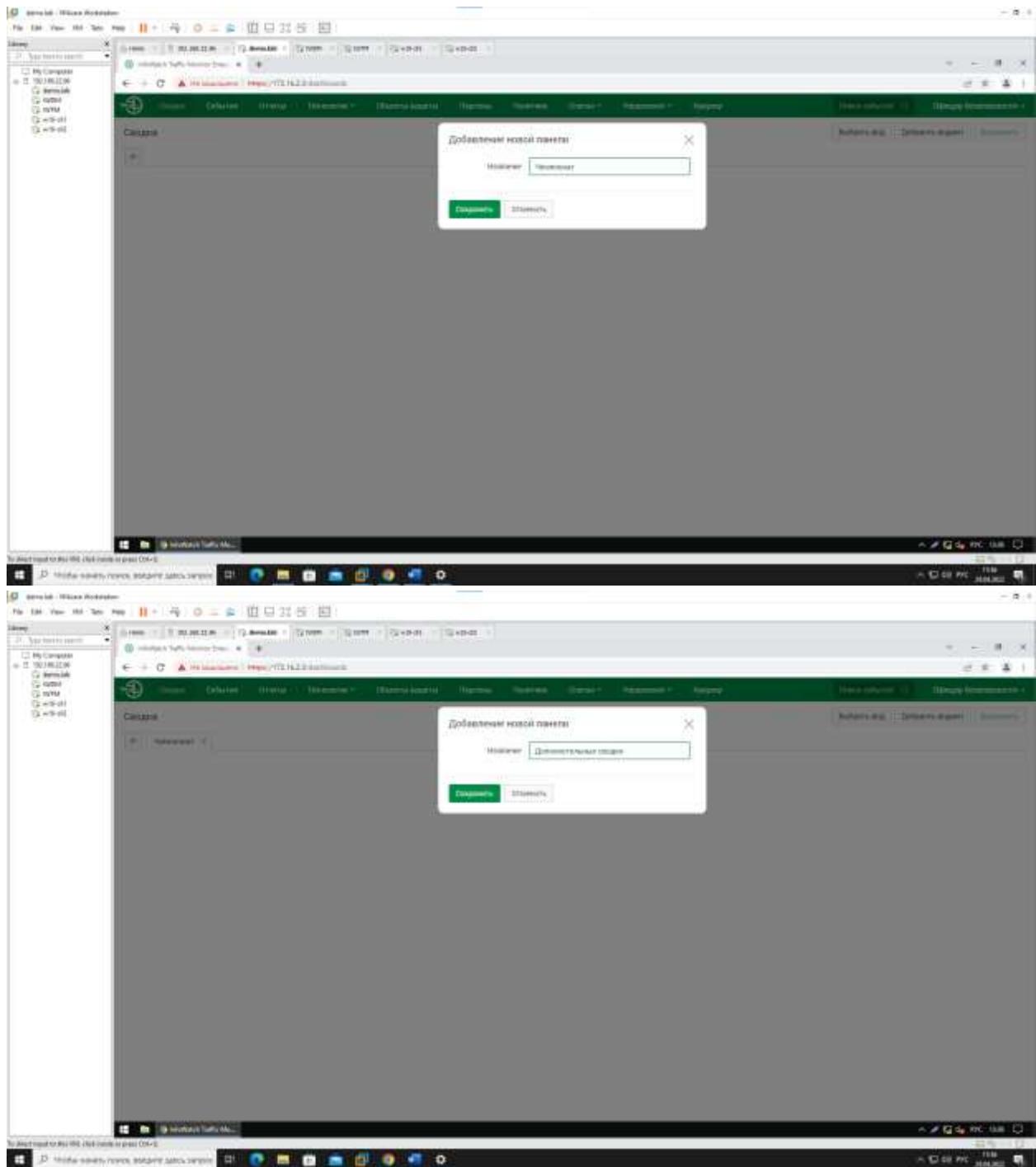
Создание пользователя и роль для него

The screenshot shows a Windows desktop environment with three overlapping application windows. The top window is titled 'Создание роли' (Role Creation) and displays a list of roles with checkboxes. The 'DLR' role is selected, and its details are shown in the right pane. The middle window is titled 'Создание пользователя' (User Creation) and shows a list of users with checkboxes. The 'Администратор' user is selected, and its details are shown in the right pane. A modal dialog box titled 'Выбор роли (1)' (Role Selection (1)) is open, listing the 'DLR' role with a checked checkbox. At the bottom of the dialog are two buttons: 'Сохранить' (Save) and 'Отмена' (Cancel).



Удаляем все сводки





Добавляем подборку

Скриншоты демонстрируют процесс настройки отчета в Microsoft Power BI Desktop.

На первом снимке видно диалоговое окно "Выберите тип статистики", предлагающее различные типы диаграмм для отображения данных. Пользователь может выбрать один из предложенных вариантов или нажать "Добавить изображение".

На втором снимке показано окно "Подборка", где можно настроить параметры отчета. Видны фильтры для "СтартаДата" и "Тип нарушений".

На третьем снимке отображается окончательный вид отчета, готовый к публикации.

The screenshot shows the InfoWatch Traffic Monitor Enterprise web interface. The main window displays a sidebar with navigation links like 'Сводка', 'События', 'Отчеты', 'Технологии', 'Объекты защиты', 'Персоны', 'Политики', 'Списки', 'Управление', and 'Краулер'. A sub-menu under 'Запросы' is open, listing options such as 'Создать обычный запрос', 'Создать расширенный запрос', 'Создать папку запросов', and several event-based filters like 'События в карантине за текущую неделю...', 'События за последние 7 дней', 'События за текущий день', and 'События сотрудников под наблюдением...'. The central area contains the message 'Выберите или создайте запрос' (Select or create a query). Below this, a detailed 'Редактирование запроса' (Edit query) dialog is open, showing fields for 'Название' (Name: Краулер), 'Описание' (Description), and tabs for 'Запрос' (Request), 'Образцы' (Samples), and 'Детали' (Details). Under 'Запрос', there are dropdowns for 'Тип запроса' (Query type: Общежайт), 'Для журнала' (For log: Последние 3 дня), and 'Параметры' (Parameters: Старт). At the bottom of the dialog are buttons for 'Сохранить в библиотеке' (Save to library), 'Сохранить' (Save), and 'Отмена' (Cancel).

Добавляем условие – технологии

Скриншоты демонстрации работы с базой данных в Microsoft SQL Server Management Studio.

Верхний скриншот: Выбор результата анализа.

Окно диалога "Выбор результата анализа" (Select Result Set for Analysis). Виджет "Категории" (Categories) показывает папку "Проверка" с подкаталогом "Кредитная карта". Виджет "Результаты" (Results) отображает три записи:

Название	Дата создания	Описание
Кредитная карта	12.11.2021 05:29	Система сравнивает количество карт в группе с...
Паспорт гражданина РФ	17.11.2021 05:29	Система сравнивает количество паспортов граждани...

Нижний скриншот: Создание запроса.

Окно диалога "Создание запроса" (New Query). Виджет "Запрос" (Query) содержит:

- Название: Новый запрос;
- Текущий: Текущий
- Запрос: Текущий
- Фильтр: Паспорт 7 дней
- Логика: Кредитная карта > Паспорт гражданина РФ

Виджет "Создать в базе данных" (Create in Database) имеет активную кнопку "Создать" (Create).

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

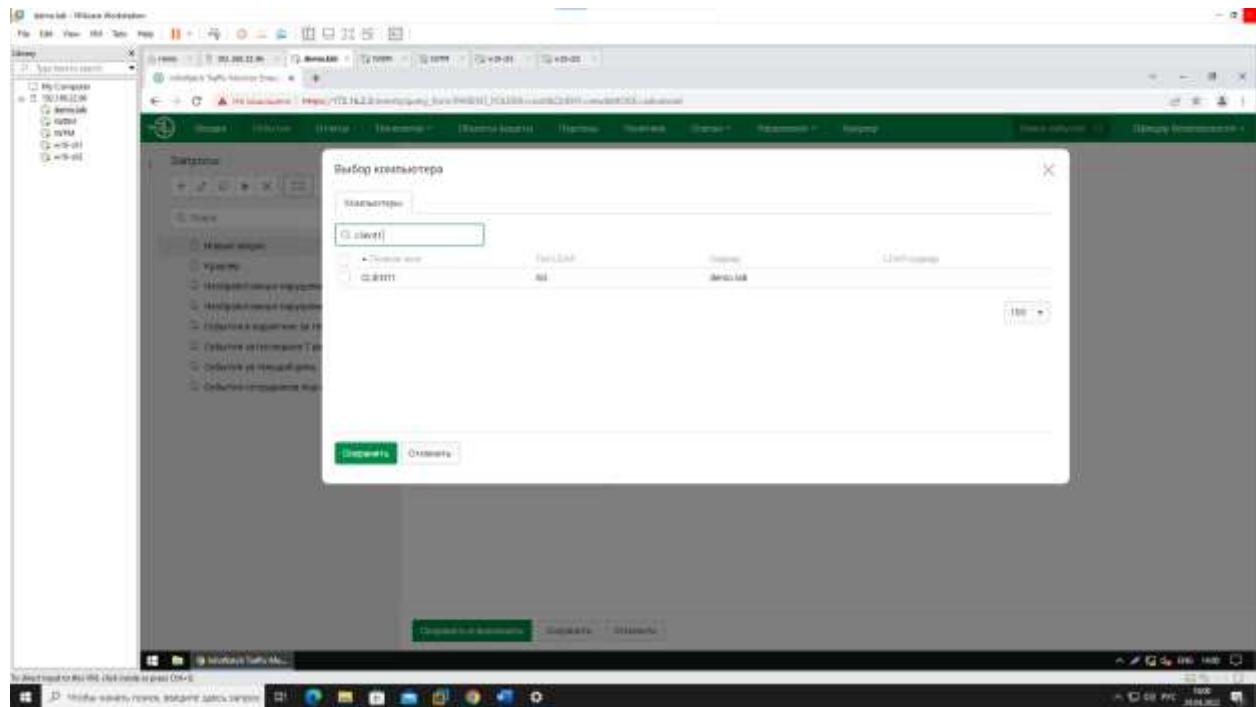
Название:	Статистика по политикам
Интервал обновления:	Не обновлять ▾
Период:	Текущий месяц ▾
Политики	Начните вводить текст <input type="text"/> +
<button>Сохранить</button> <button>Отменить</button>	

Общие настройки виджета

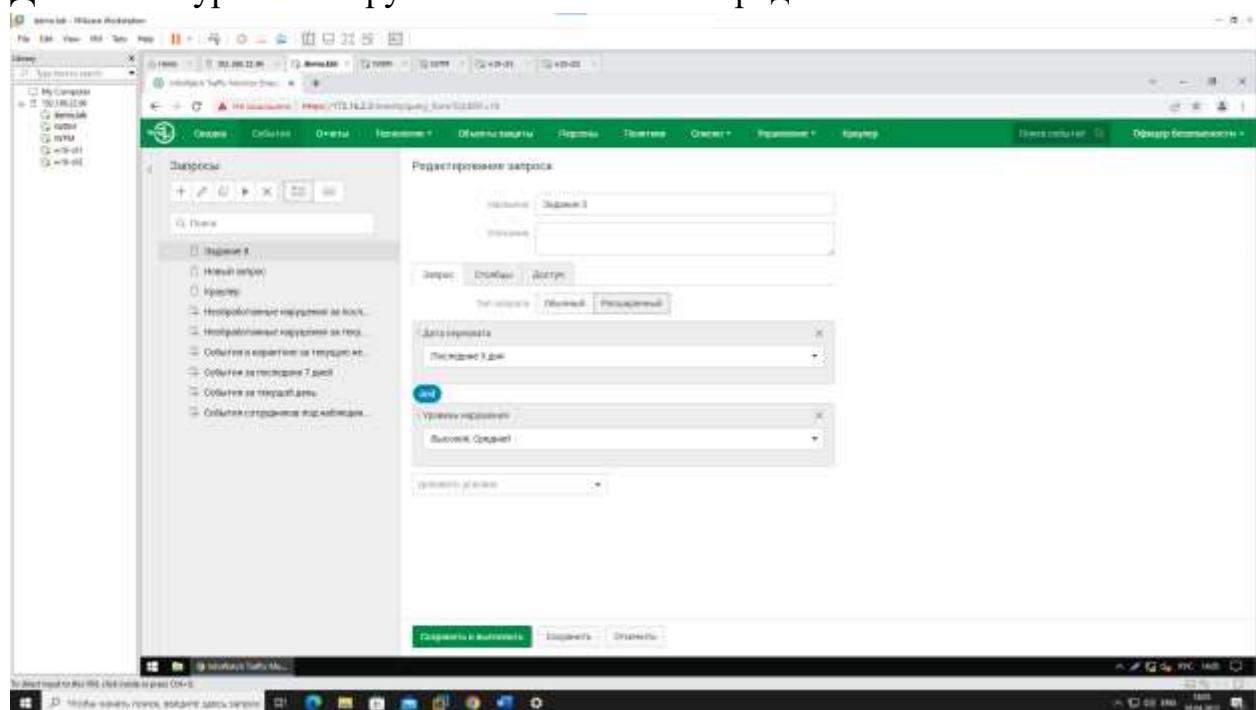
Название:	Топ нарушителей
Интервал обновления:	Не обновлять ▾
Период:	Последние 30 дней ▾
Количество нарушителей	10 ▾
Группы	Введите название группы <input type="text"/> +
Статусы	Выберите статус <input type="text"/> +
<button>Сохранить</button> <button>Отменить</button>	

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

