

ДЕМОЭКЗАМЕН

Описание модуля 1:

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:

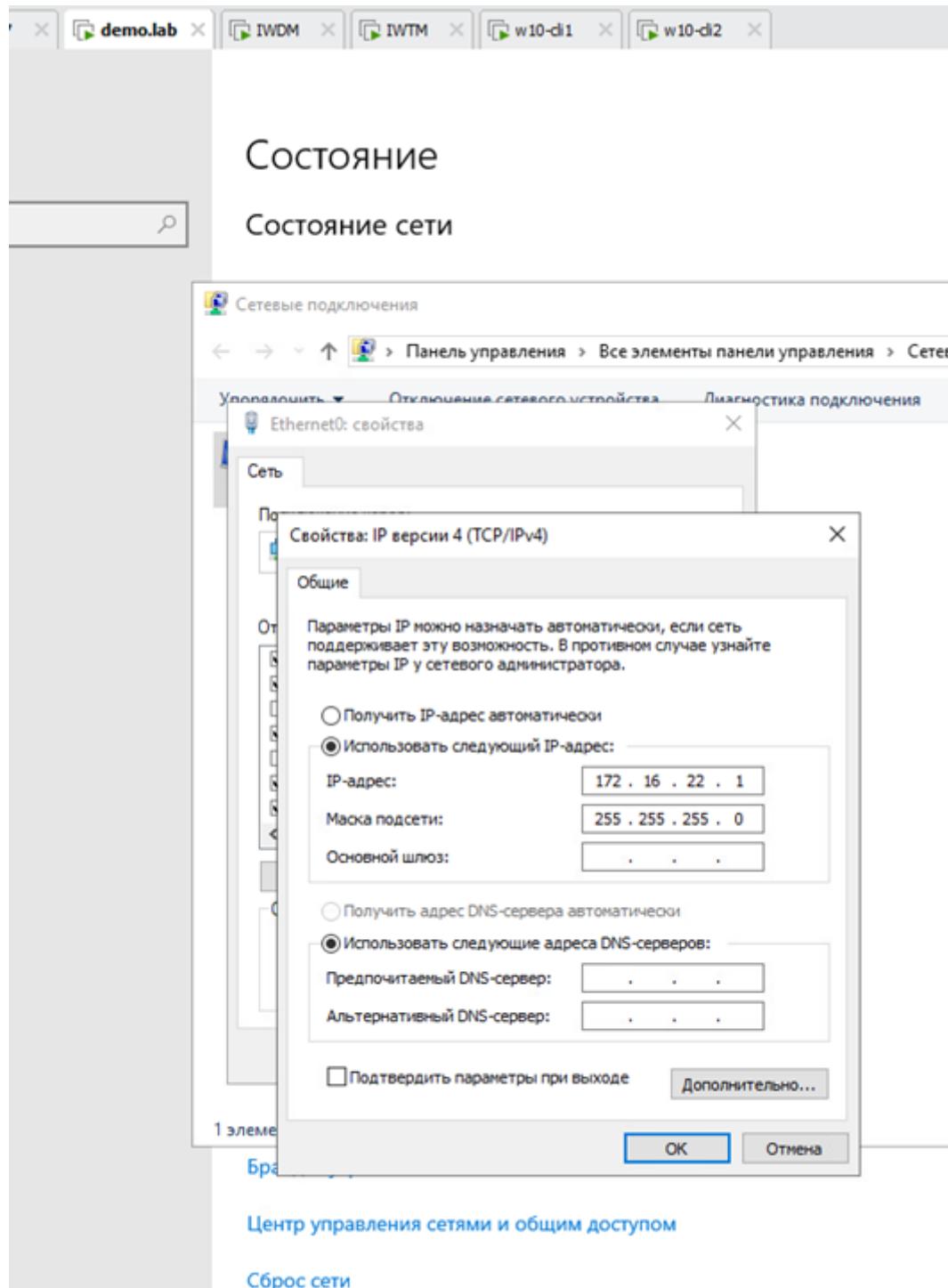
Логин: user-agent1, пароль: xxXX1234, права пользователя домена

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

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

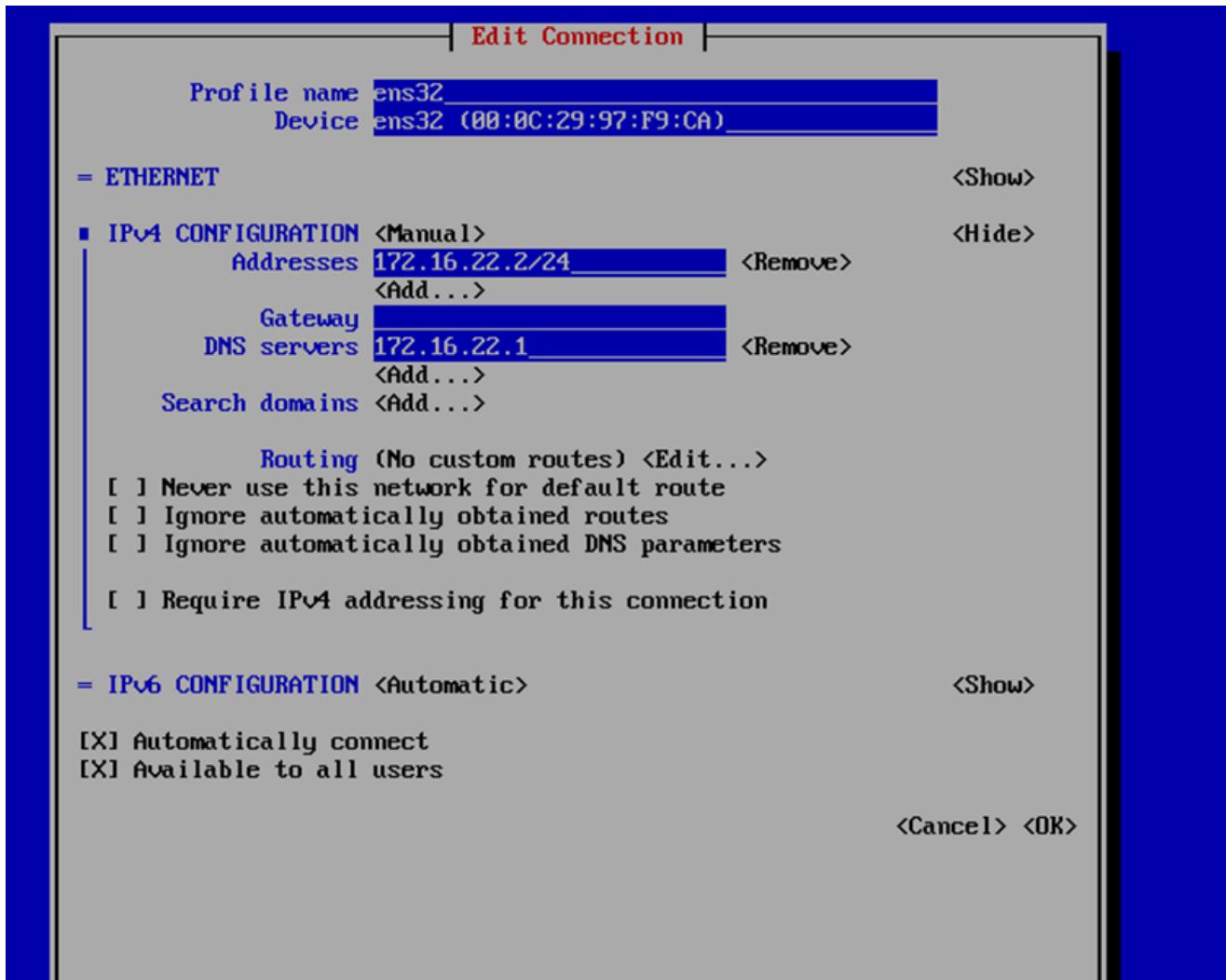
Логин: iwtm-officer, пароль: xxXX1234, права пользователя домена

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



Далее переходим на IWTM.

Прописываем – nmtui. Там также проверяем сетевую настройку (действуем по тому же принципу, главное наличие DNS (для дальнейшей работы с краулером)). После этого можно пропинговать для проверки (или зайти в браузер>инфовоч., чтобы убедится в том что все работает)

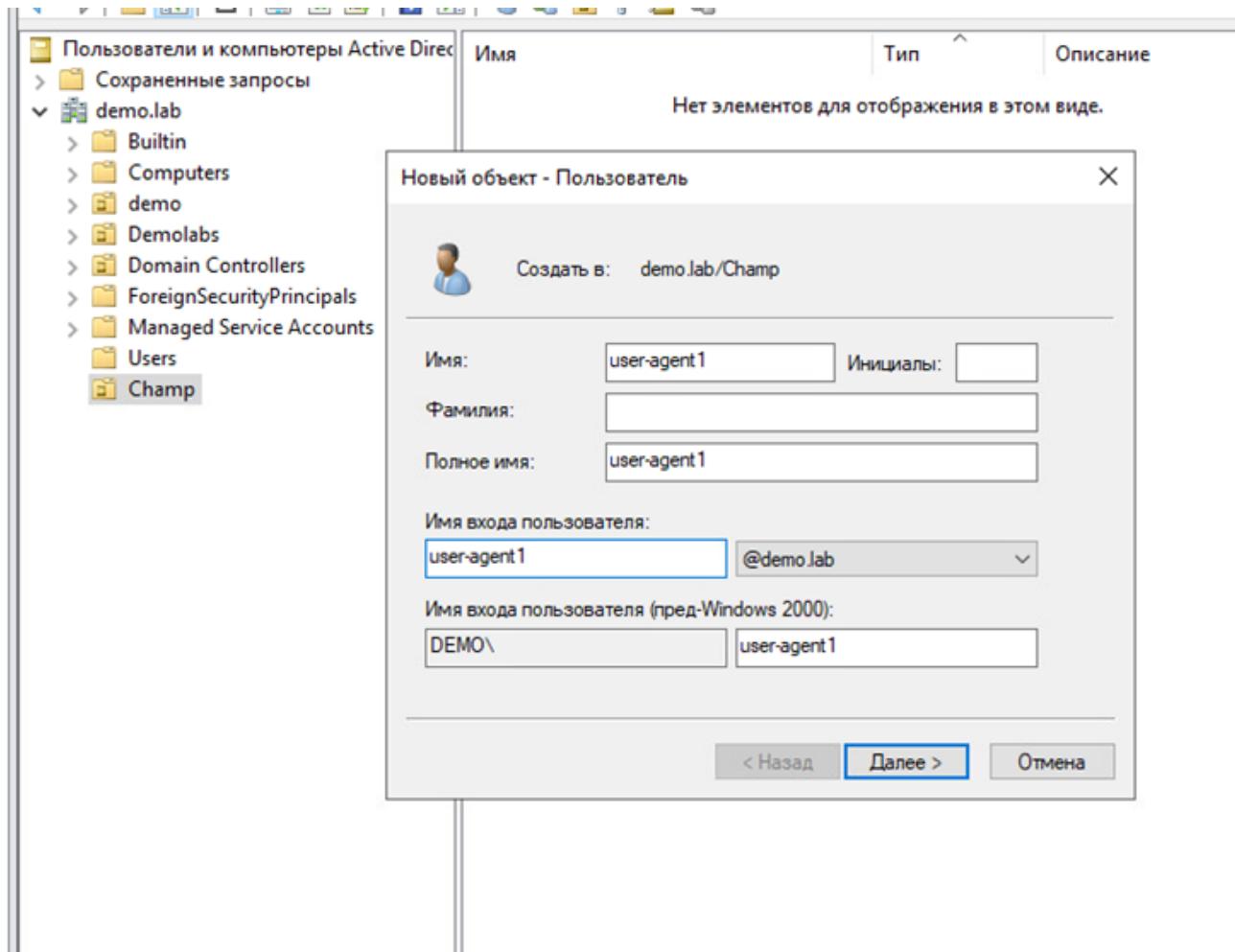


```
[root@iwtm ~]# ping 172.16.22.1
PING 172.16.22.1 (172.16.22.1) 56(84) bytes of data.
64 bytes from 172.16.22.1: icmp_seq=1 ttl=128 time=1.93 ms
64 bytes from 172.16.22.1: icmp_seq=2 ttl=128 time=0.454 ms
64 bytes from 172.16.22.1: icmp_seq=3 ttl=128 time=1.11 ms
^C
--- 172.16.22.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.454/1.165/1.931/0.604 ms
[root@iwtm ~]#
```

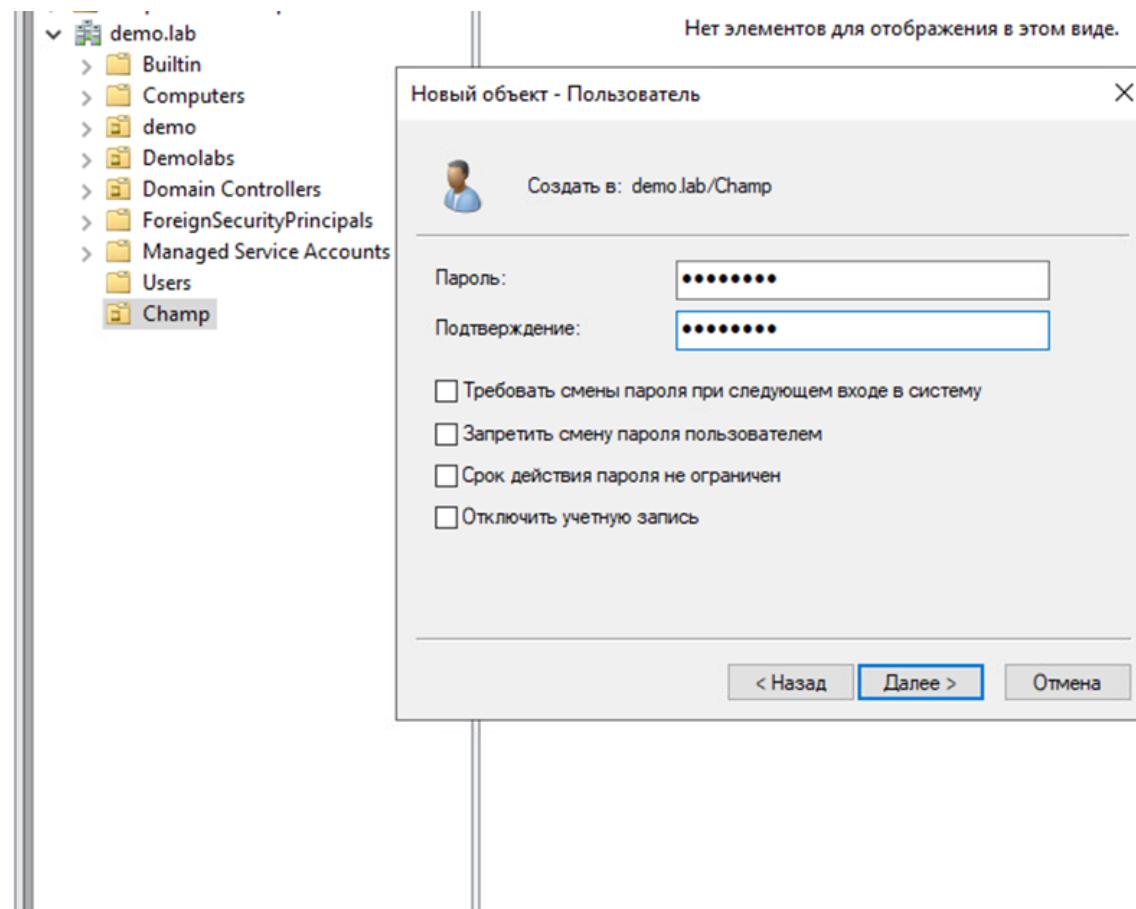
Или же зайти в браузер на demo.lab и там ввести ip iwtm (то есть зайти на инфовоч)

The screenshot shows the Windows Active Directory Users and Computers snap-in. On the left, the navigation pane displays the structure: Пользователи и компьютеры Active Direct... > Сохраненные запросы > demo.lab > База данных > Computers > demo > Demolabs > Domain Controllers > ForeignSecurityPrincipals > Managed Service Accounts > Users. A context menu is open over the 'demo' container, with the 'Создать подразделение...' option highlighted. A modal dialog box titled 'Новый объект - Подразделение' (New object - Department) is displayed in the center. It contains a 'Создать в:' dropdown set to 'demo.lab/' and a 'Имя:' input field containing 'Champ'. Below the input field is a checkbox labeled 'Заштитить контейнер от случайного удаления' (Protect container from accidental deletion), which is checked. At the bottom of the dialog are 'OK', 'Отмена' (Cancel), and 'Справка' (Help) buttons.

В нашем случае изменяется название подразделение – QualExam (и лучше убрать галочку «Заштитить контейнер от случайного удаления»)



Далее создаем необходимых пользователей (необходимо заполнить как показано в этом примере «имя» и «имя входа пользователя»)



192.168.22.7

- demo.lab
- IWDM
- IWTM
- w10-cli1
- w10-cli2

Имя	Тип	Описание
user-agent1	Пользователь	
user-agent2	Пользователь	
iw-admin	Пользователь	
iwtm-officer	Пользователь	
ldap-sync	Пользователь	

(не забываем, что конечный результат будет отличаться в зависимости от задания)

Выбор: "Группы"

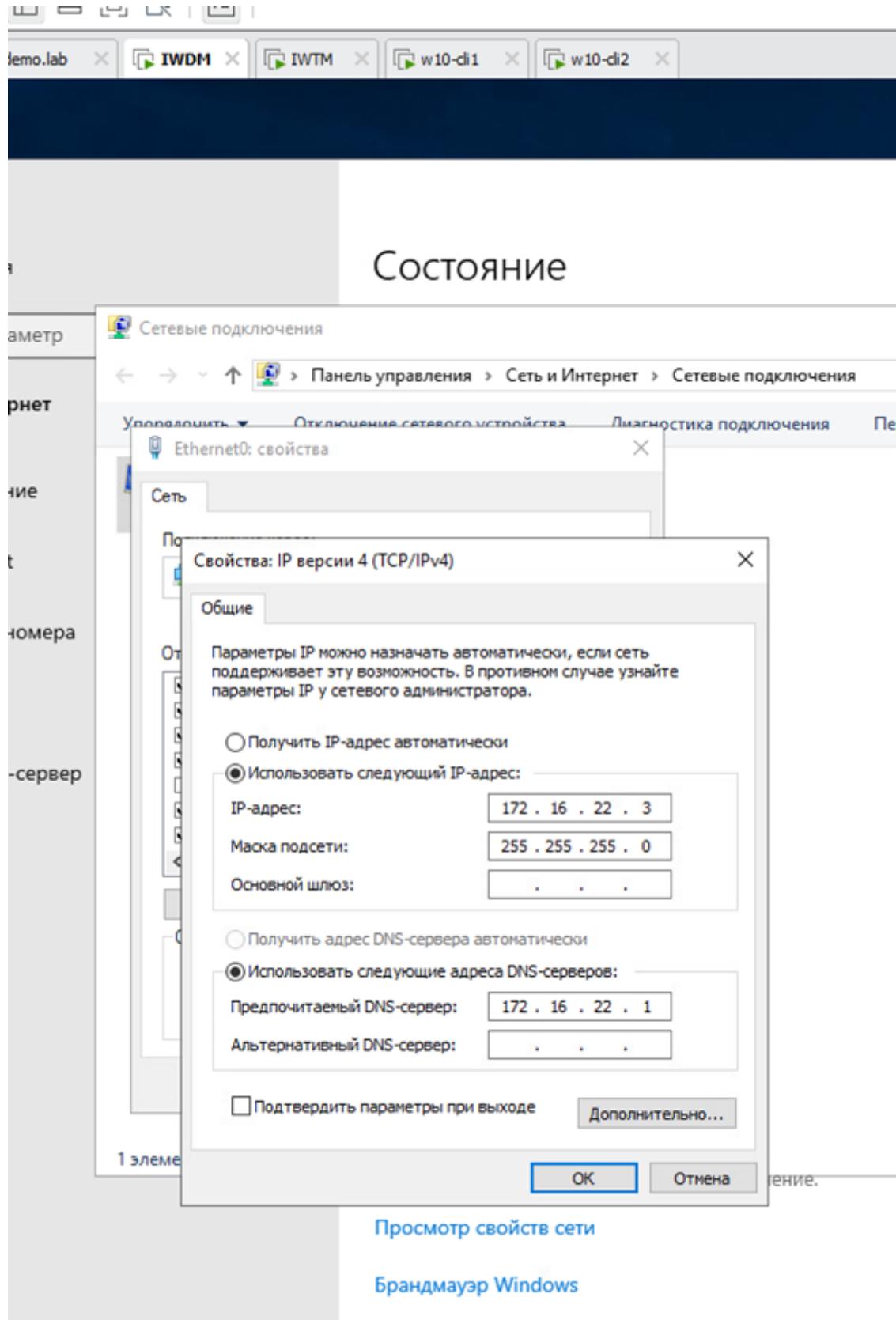
Выберите тип объекта:
"Группы" или "Встроенные субъекты безопасности"

В следующем месте:

Введите имена выбираемых объектов ([примеры](#)):

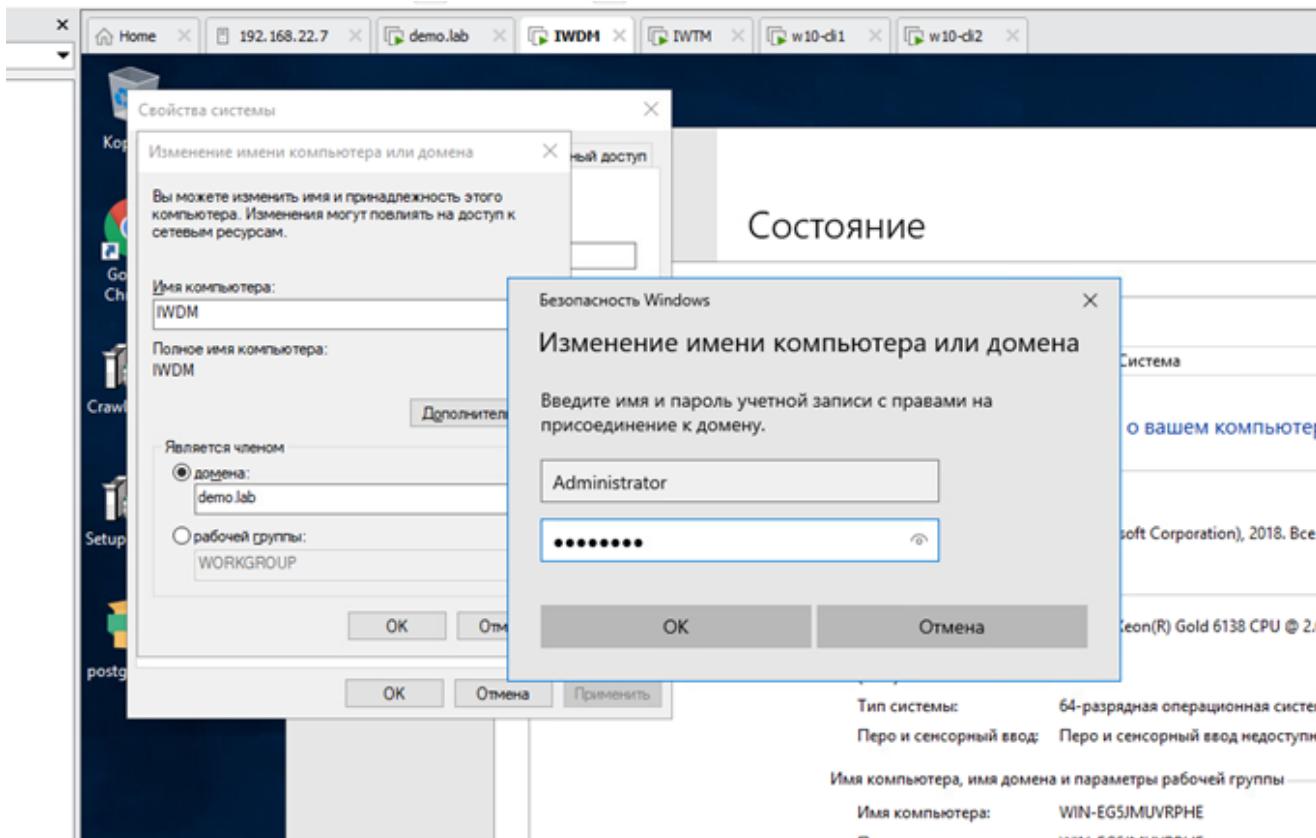
Права администратора для iw-admin (зайти в его свойства > группы)

Далее проверяем сетевые настройки на IWDM.



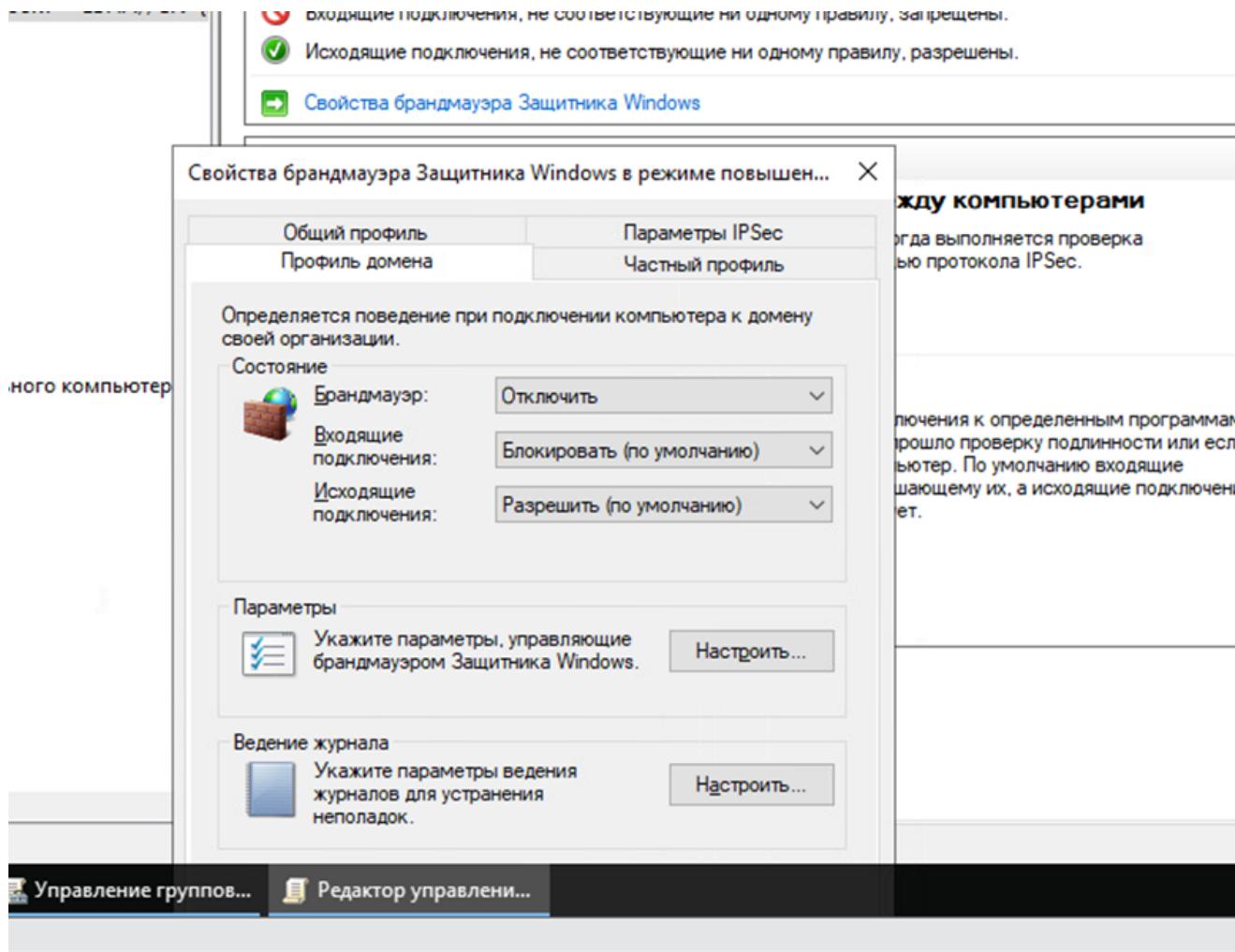
Просмотр свойств сети

Брандмаэр Windows



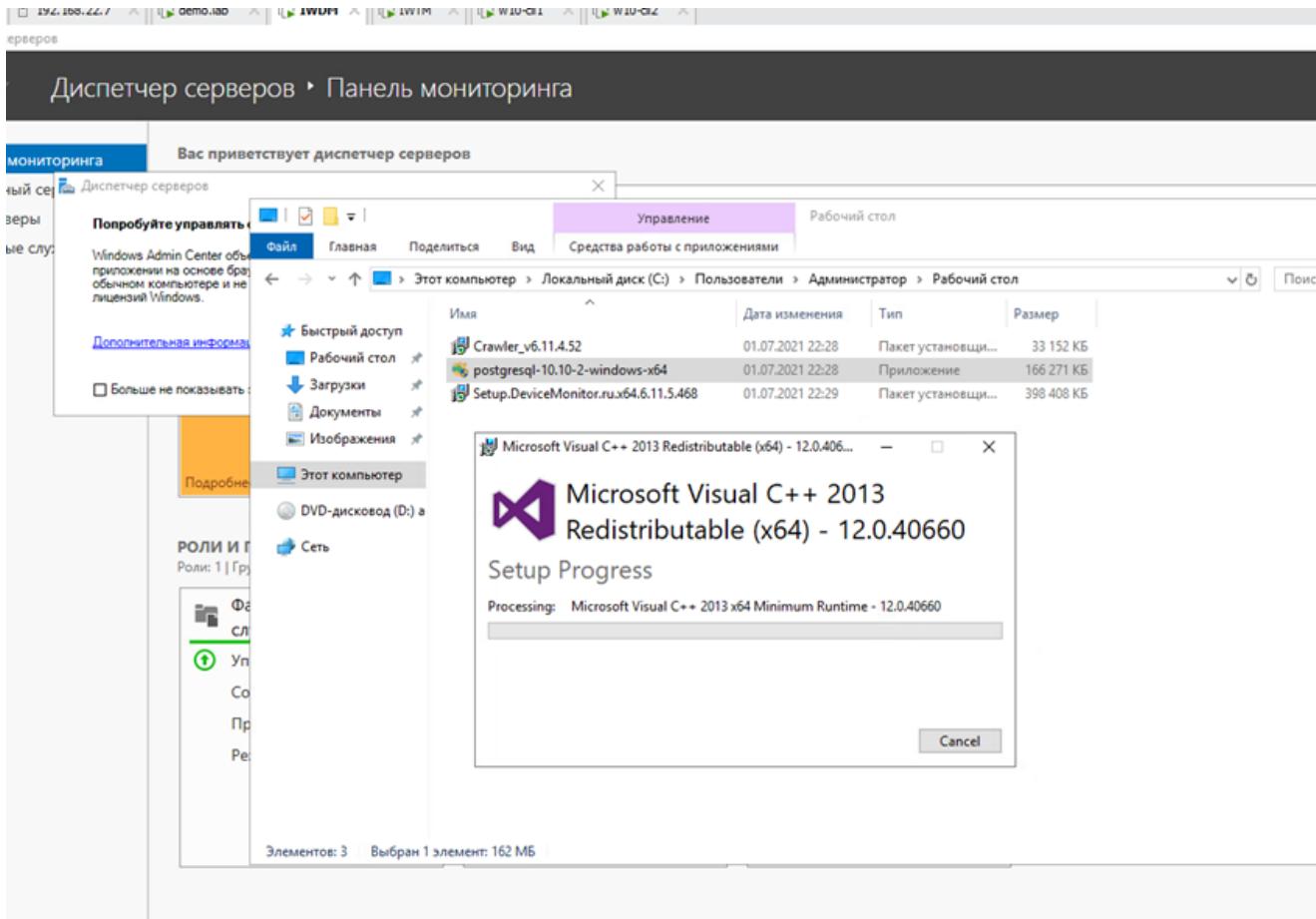
Меняем ИМЯ и ВНОСИМ в домен.

Чтобы сюда попасть нужно нажать правой кнопкой мыши на Default Domain Policy (нажать изменить)



Отключаем брандмауэр

Далее переходим на IWDM – вход от лица ранее созданного пользователя
(iw-admin)



(При установке оставляем все без изменения, кроме пароля)

Устанавливаем базу (в случае возникновения ошибки при установке необходимо заново попробовать установить. В случае если появится синий слон – убрать галочку в этом окне).

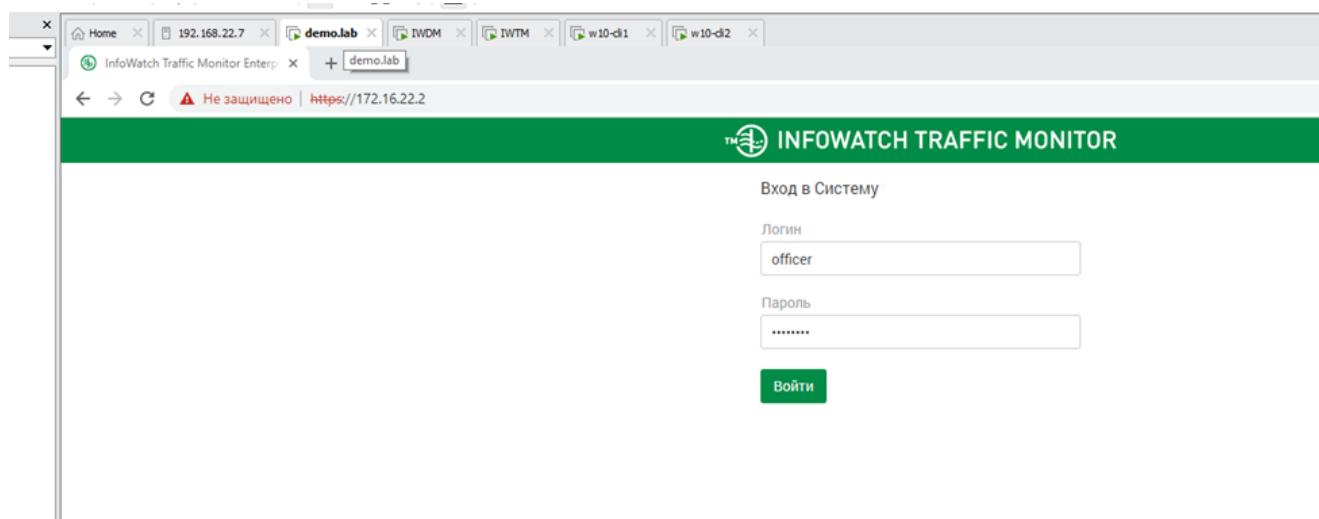
Откройте установщик правой кнопкой мыши от имени админа. Уберите галочку с **Stack Bulder**, при вводе пароля необходимо убедиться, что язык выбран англ.

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 **Idap-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.



The screenshot shows the main dashboard of the InfoWatch Traffic Monitor Enterprise. At the top, there is a navigation bar with tabs: 'Политики', 'Списки', 'Управление', 'Краулер', and a search bar 'Поиск событий'. Below the navigation bar, there is a sidebar with a date selector '2022 - 02.03.2022' and a dropdown menu titled 'Топ нарушений' (Top violations) which is currently set to 'Без учета' (Without consideration). The main content area has a heading 'LDAP-синхронизация' (LDAP synchronization) and a list of management options: 'Лицензии' (Licenses), 'Управление доступом' (Access management), 'Состояние Системы' (System status), 'Аудит' (Audit), 'Контроль целостности' (Integrity control), 'Службы' (Services), 'Плагины' (Plugins), 'Почтовый сервер' (Email server), and 'Почтовые уведомления' (Email notifications). A message at the bottom states: 'Выбранного периода данные отсутствуют' (Data for the selected period are absent). On the right side of the dashboard, there is a small box with a chart icon and the number '24'.

Сводка События Отчеты Технологии ▾ Объекты защиты Персоны Политики Списки ▾ Управление ▾ Краулер

LDAP-серверы

+ ✎ × ▼

Нет элементов

Добавление LDAP-сервера

Имя сервера

Тип сервера

Синхронизация Автоматическая Ручная

Период синхронизации

Повторение минут

Настройки соединения

LDAP-сервер

Использовать протокол Kerberos

Глобальный LDAP-порт

LDAP-порт

Использовать глобальный каталог

LDAP-запрос

Анонимный доступ

Логин

Пароль

Сохранить Проверить соединение Отменить

Не защищено | <https://172.16.22.2/settings/ldap>

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

LDAP-серверы

+ ✎ × ▼

Нет элементов

Тип сервера

Синхронизация Автоматическая Ручная

Период синхронизации

Повторение минут

Настройки соединения

LDAP-сервер

Использовать протокол Kerberos

Глобальный LDAP-порт

LDAP-порт

Использовать глобальный каталог

LDAP-запрос

Анонимный доступ

Логин

Пароль

Сохранить Проверить соединение Отменить

✓ LDAP-синхронизация
Проверка соединения прошла успешно

Управление доступом

Пользователи

Выберите пользователя из LDAP

LDAP-сервер для поиска: demo.lab

Поиск: iwtm

Пользователь	Доменний аккаунт	Адрес сервера	Департамент
<input checked="" type="checkbox"/> iwtm-officer	iwtm-officer@demo.lab	172.16.22.1	

Сохранить Отменить

Не выбираем vip.

Пользователи

Логин	Название	Email	Роли	Области видимости	Описание
<input checked="" type="checkbox"/> iwtm-officer	iwtm-officer				
<input type="checkbox"/> administrator	Администратор		Администратор	Предустановлен	
<input type="checkbox"/> officer	Офицер безопасности		Администратор	Полный доступ Предустановлен	

Редактирование пользователя

Логин: iwtm-officer

Статус: Активен

Email: iwtm-officer@demo.lab

Полное имя: iwtm-officer

Роли: Офицер безопасности, Администратор

Области видимости: Полный доступ, VIP

Описание: Описание

Создано: 02.03.2022, 13:27 — Изменено: 02.03.2022, 13:27

Сохранить Отменить

← → C ⚠ Не защищено | <https://172.16.22.2/login>

INFOWATCH TRAFFIC MONITOR

Вход в систему

Логин: iwtm-officer

Пароль: *****

Войти

(Все должно быть также как в обычном офицере)

После этого не забыть создать документ с скриншотами.

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 “QualExam” на домене.

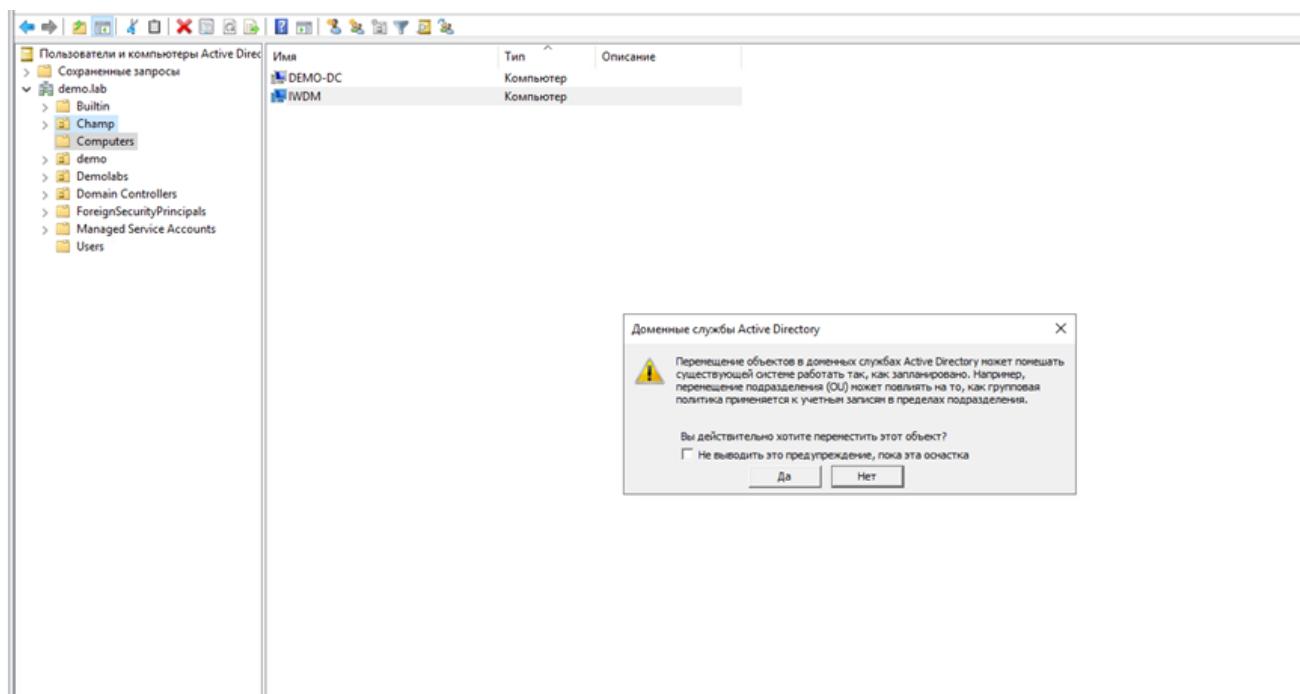
Установить базу данных PostgreSQL с паролем суперпользователя xxXX1234.

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.

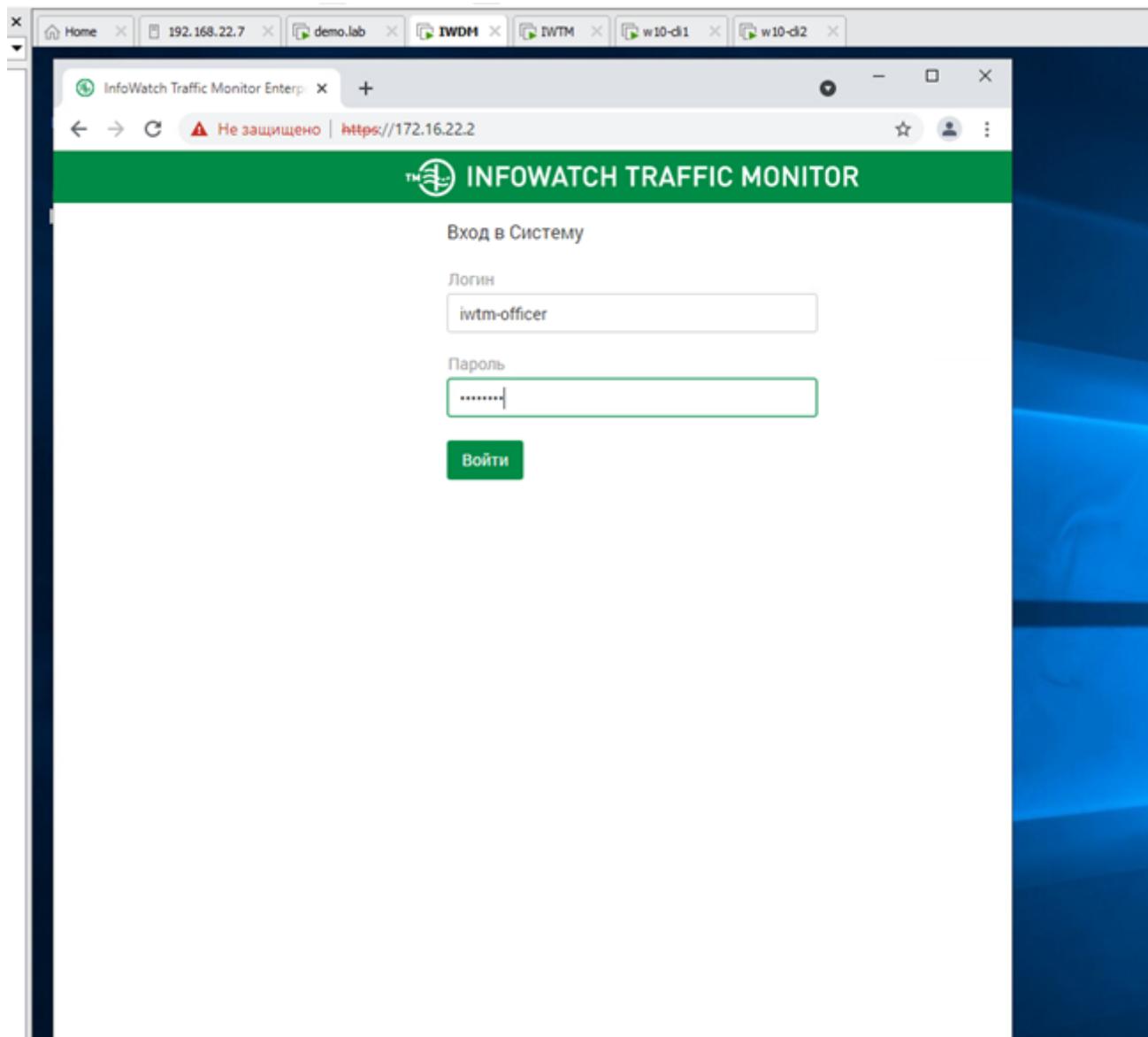


Подразделение будет отличаться, но принцип такой же (перетащить с папки где компьютеры в созданное ранее подразделение)

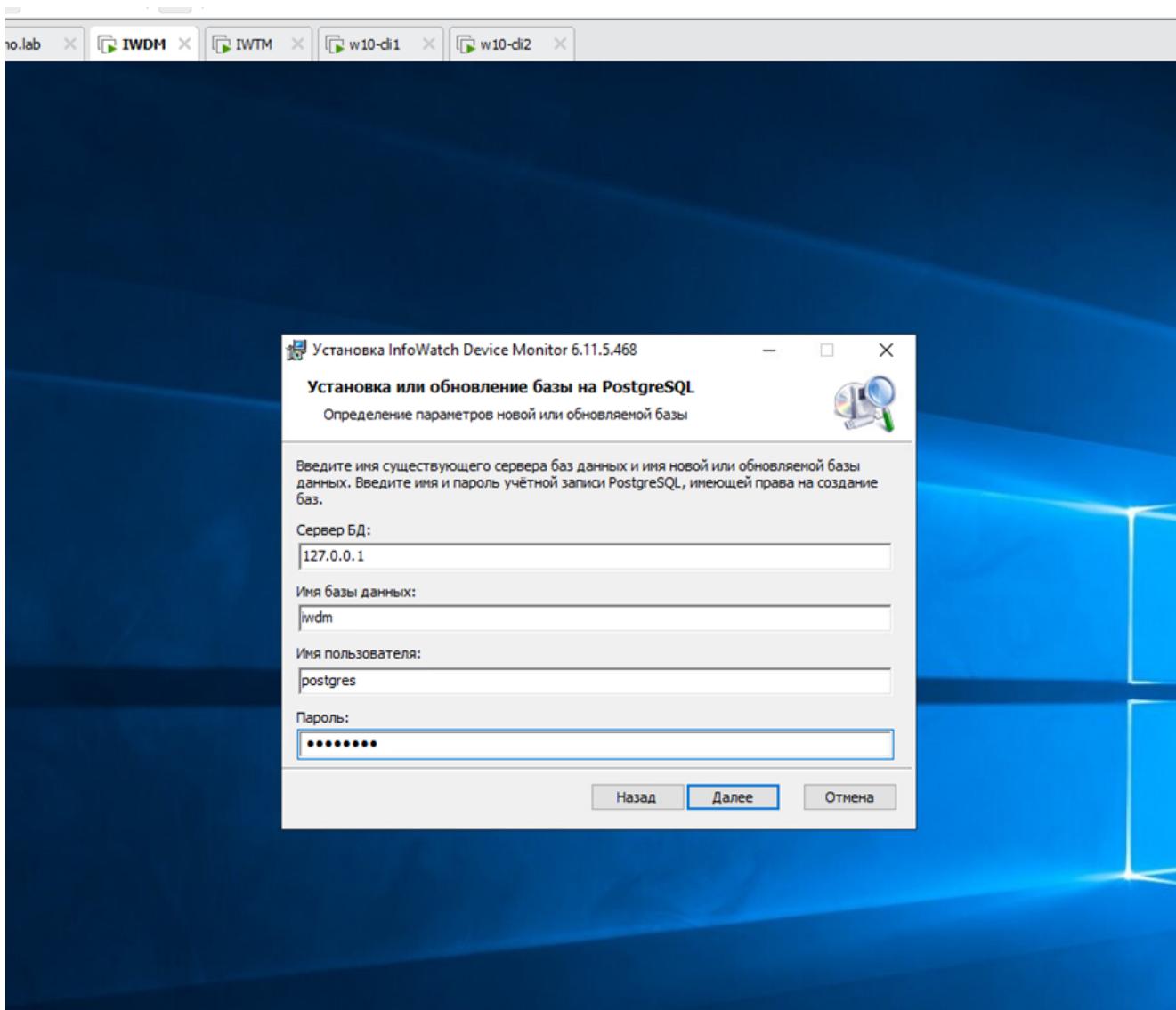
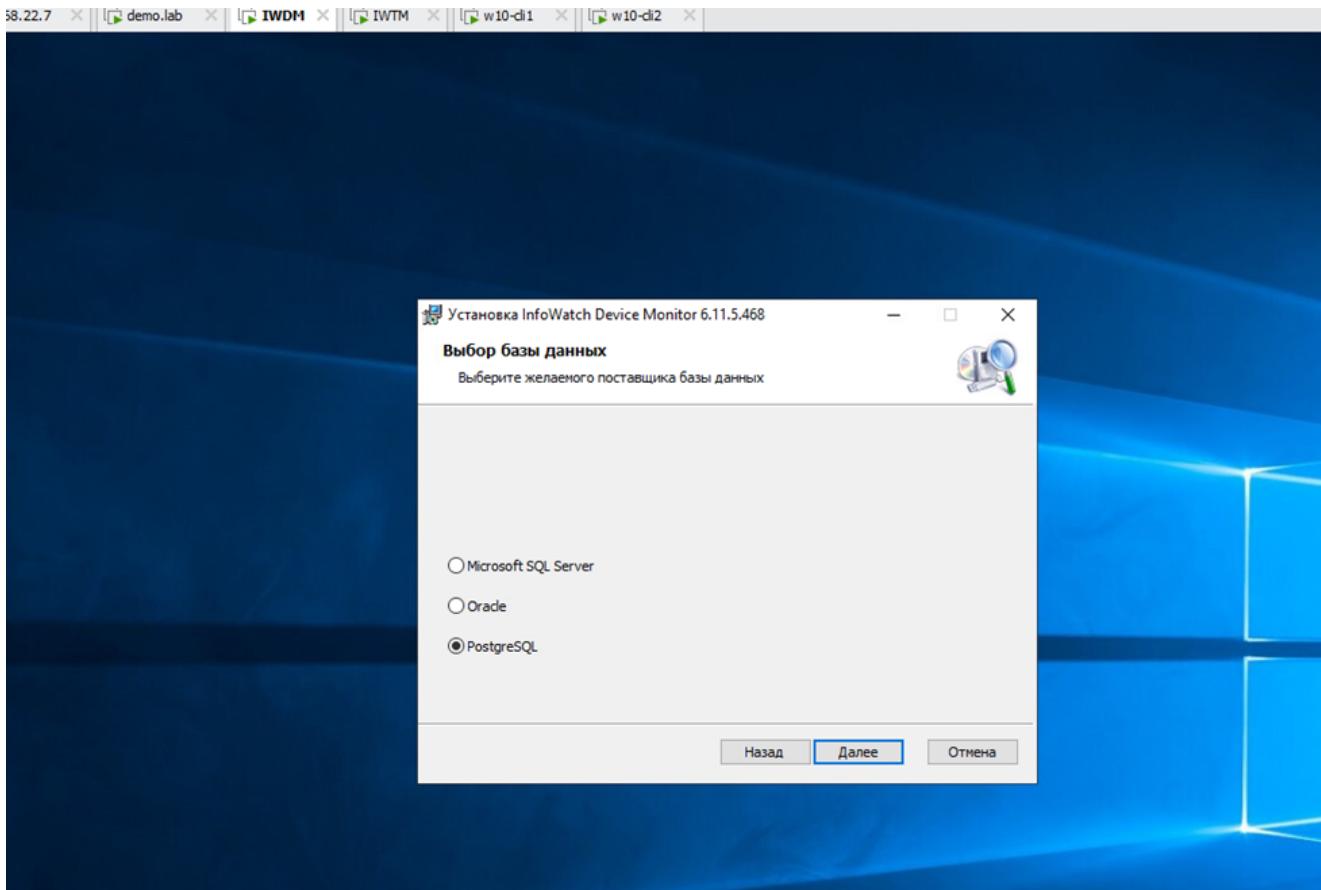
Имя	Тип	Описание
IWDM	Компьютер	
iw-admin	Пользователь	
iwtm-officer	Пользователь	
ldap-sync	Пользователь	
user-agent1	Пользователь	
user-agent2	Пользователь	

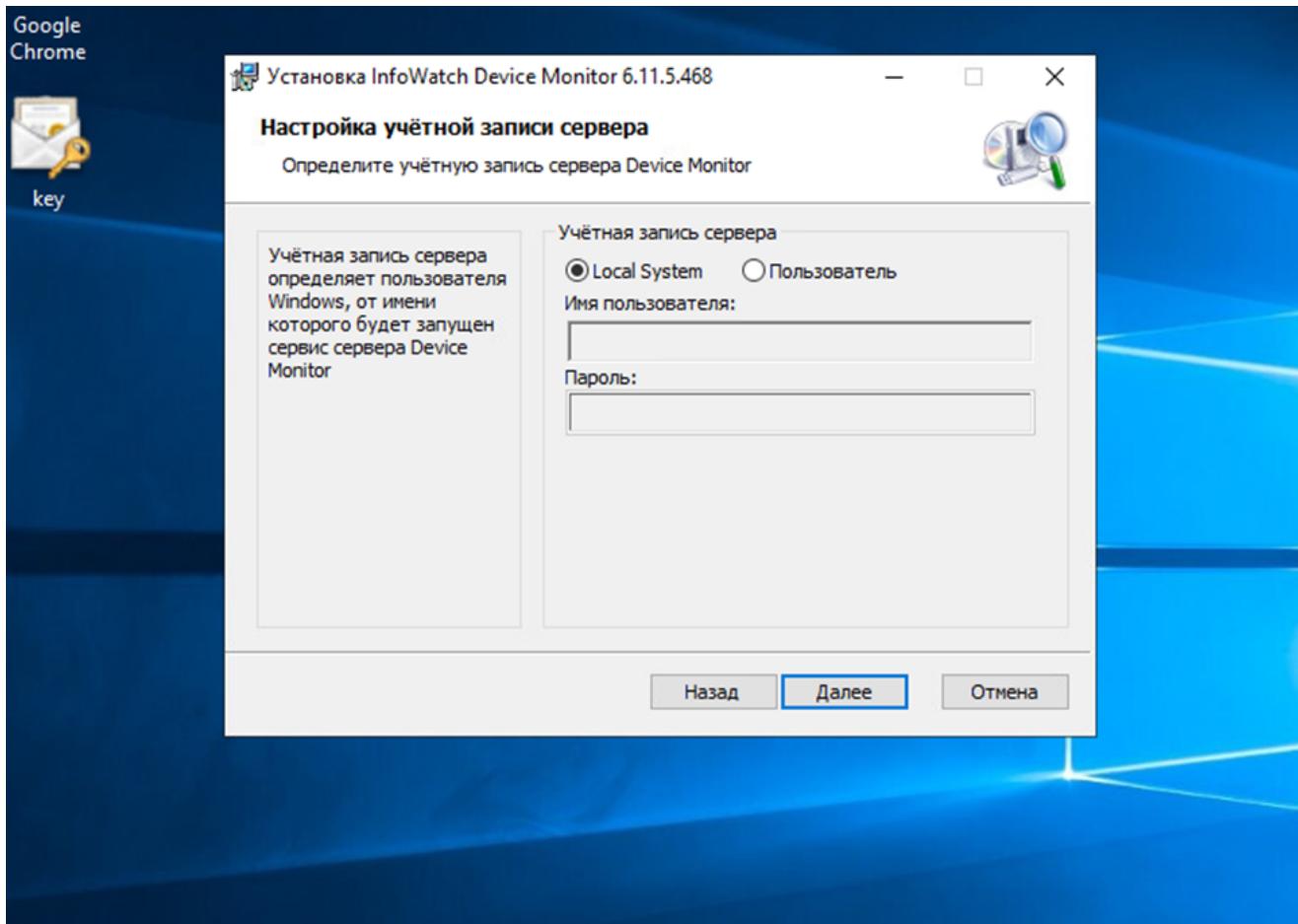
Имя	Дата изменения	Тип	Размер
Crawler_v6.11.4.52	01.07.2021 22:28	Пакет установщи...	33 152 КБ
postgresql-10.10-2-windows-x64	01.07.2021 22:28	Приложение	166 271 КБ
Setup.DeviceMonitor.ru.x64.6.11.5.468	01.07.2021 22:29	Пакет установщи...	398 408 КБ

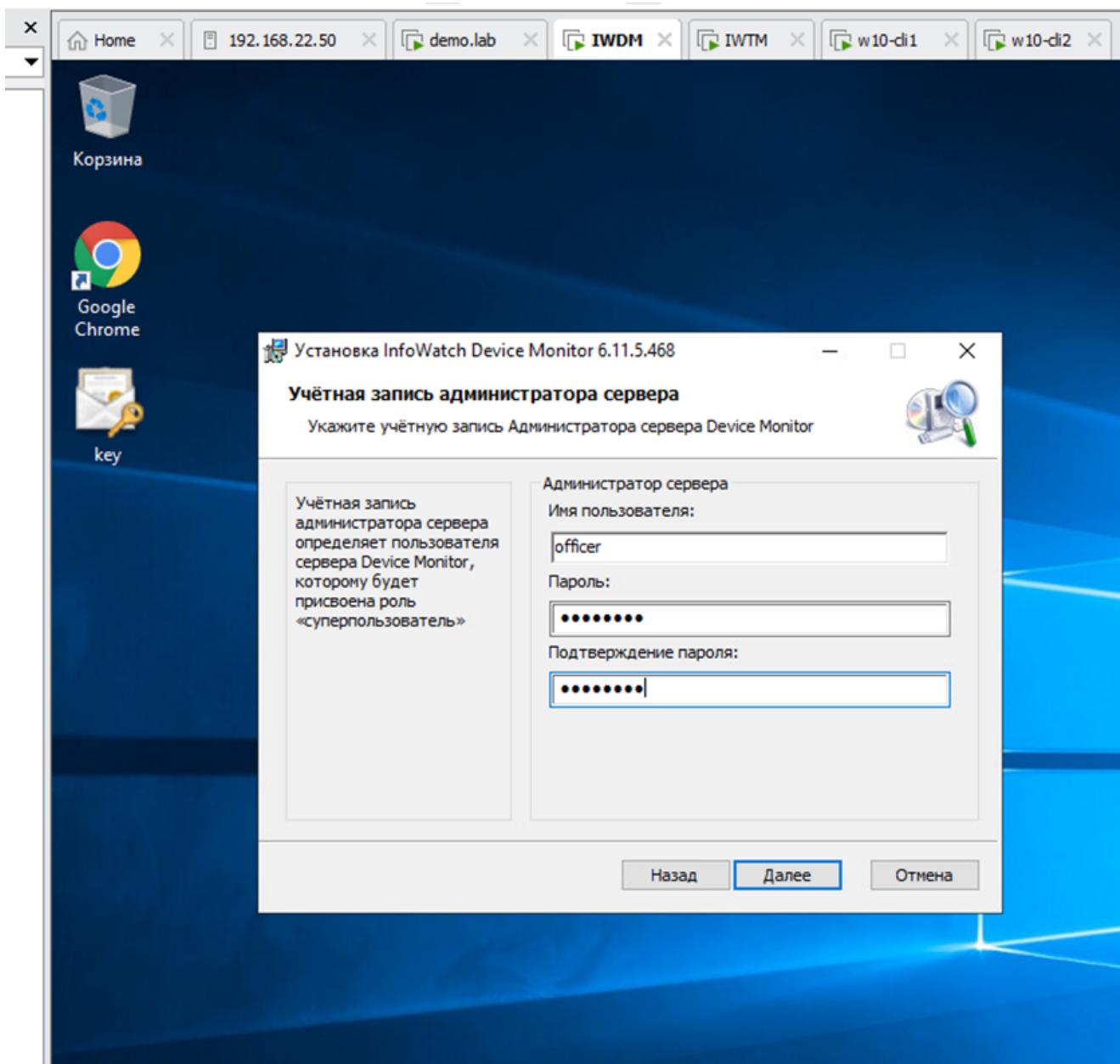
Далее снова переходим на iwdm и начинаем установку (скриншоты только где происходи изменение)



The screenshot shows a web browser window for 'InfoWatch Traffic Monitor Enterprise' at the URL <https://172.16.22.2/settings/plugins>. The page title is 'Плагины' (Plugins). On the left, there's a sidebar with 'Плагины' (Plugins), 'InfoWatch Crawler', and 'InfoWatch Device Monitor'. The main content area shows 'InfoWatch Device Monitor' details: 'InfoWatch Device Monitor', 'Производитель: IW', 'Версия 6.11.5'. Below this is a table with columns: Статус (Status), Имя (Name), Содержание (Content), and Описание (Description). One row is selected with the status 'Активный' (Active), name 'Token-3', content '9bq0vugoxkuej3frw166h', and no description. A blue tooltip 'Токены' (Tokens) is displayed above the table, stating 'Токен скопирован в буфер обмена' (Token copied to clipboard).







The screenshot shows the InfoWatch Traffic Monitor Enterprise web interface. The top navigation bar includes links for Home, demo.lab, IWDM, IWTM, w10-cl1, w10-cl2, and a placeholder for a plugin. A warning message 'Не защищено' (Not protected) is displayed at the top. The main menu has tabs for Сводка, События, Отчеты, Технологии, Объекты защиты, Персоны, Политики, Списки, and Управление.

In the left sidebar, under 'Плагины', the 'InfoWatch Device Monitor' tab is selected. It displays the following details:

- InfoWatch Device Monitor
- Производитель: IW
- Версия 6.11.5

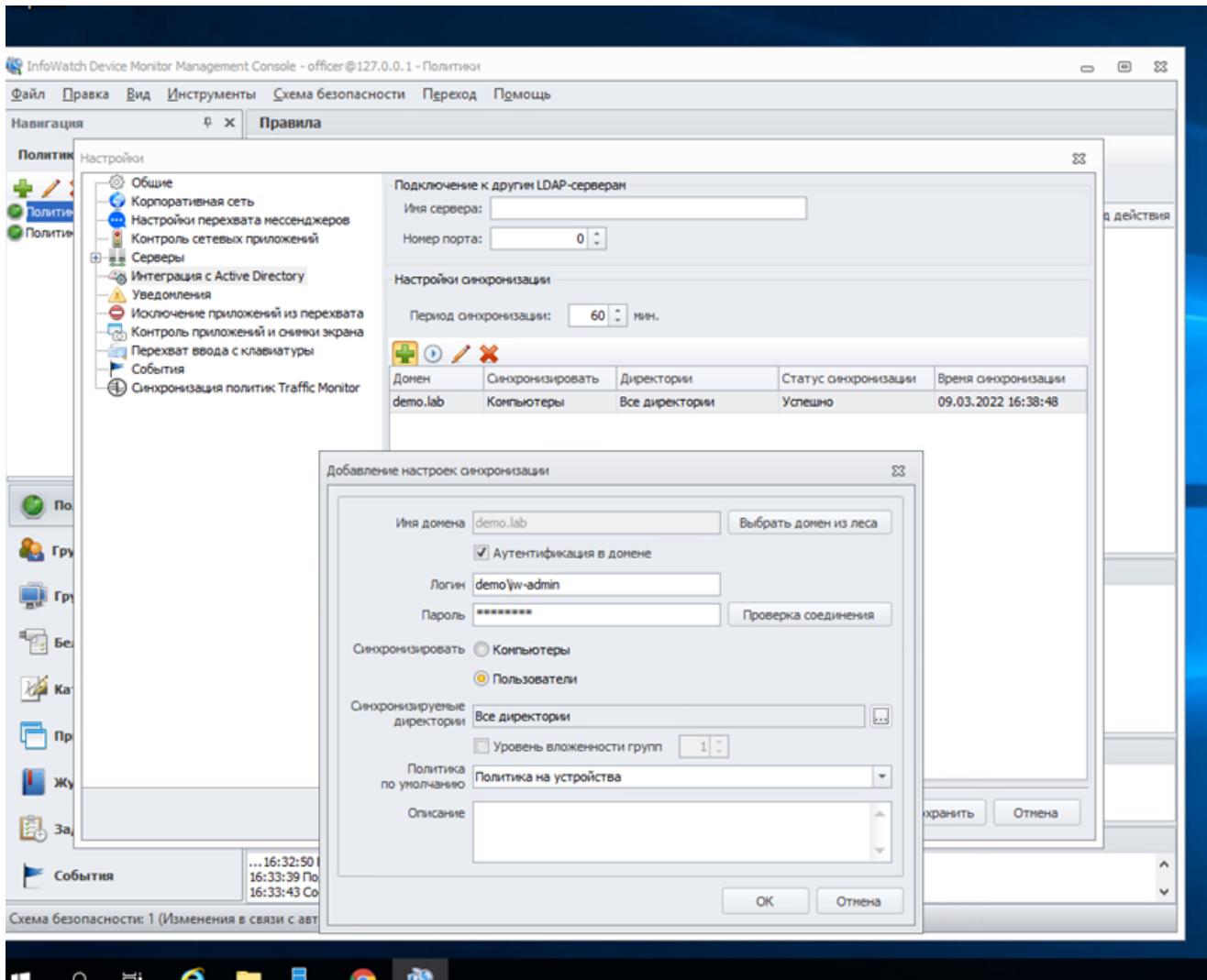
Below this, there are tabs for Плагины, Лицензии, and Токены, with 'Плагины' currently selected. There are also buttons for adding (+), deleting (X), and managing (refresh, edit).

A modal window titled 'Установка InfoWatch Device Monitor 6.11.5.468' is open, showing the 'Настройка соединения с Traffic Monitor' (Connection setup with Traffic Monitor) step. The configuration fields include:

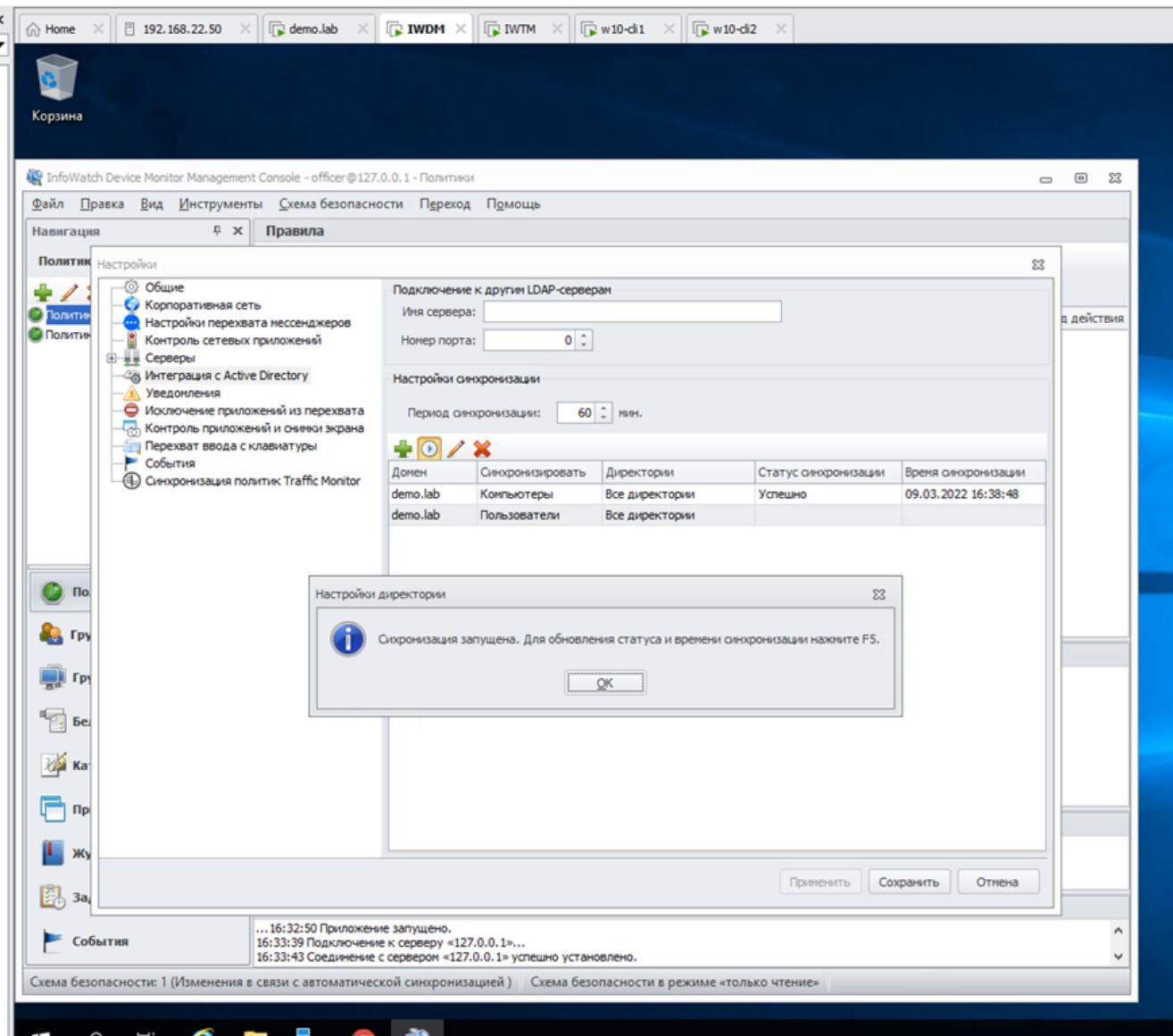
- Адрес соединения с ТМ должен иметь вид: host или host:port
- Адрес сервера ТМ: 172.16.22.2
- Количество соединений: 4
- Токен авторизации: 9bq0vugxxkuej3fw166h
- Checkboxes for 'Работать в автономном режиме' and 'Сохранять теневые копии'

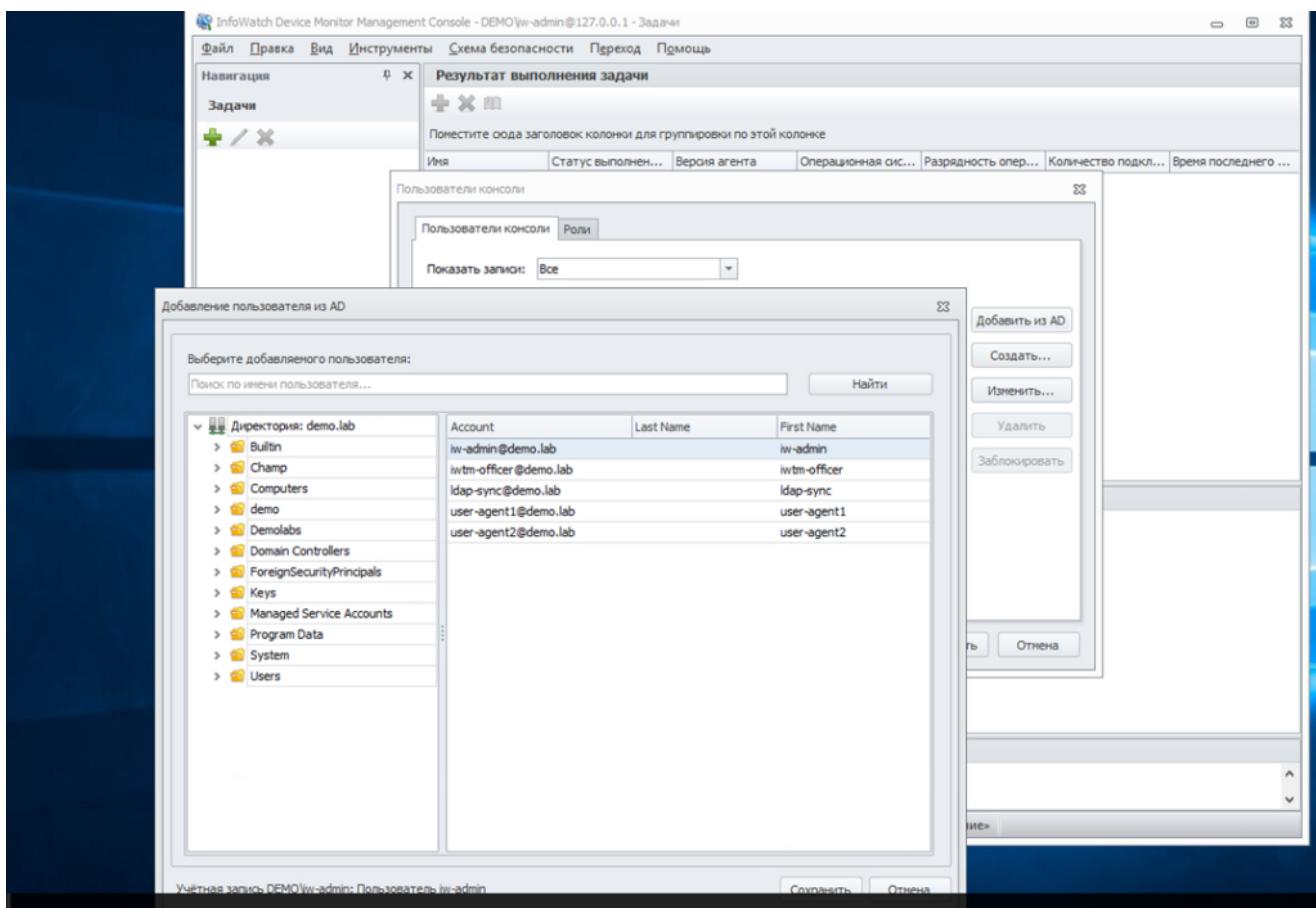
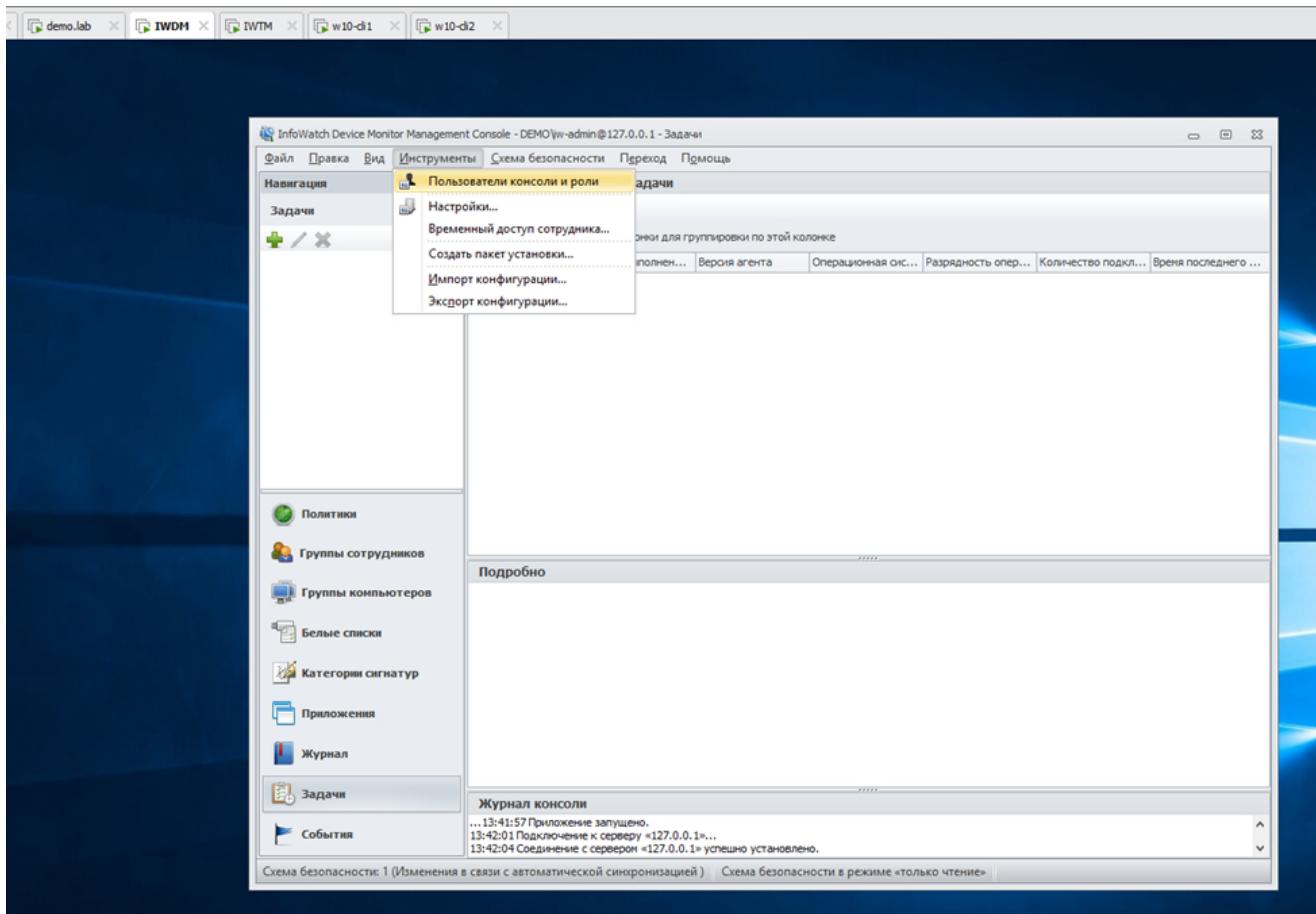
At the bottom of the modal are buttons for Назад (Back), Далее (Next), and Отмена (Cancel). The 'Далее' button is highlighted in blue.

Далее вход в консоль на рабочем столе



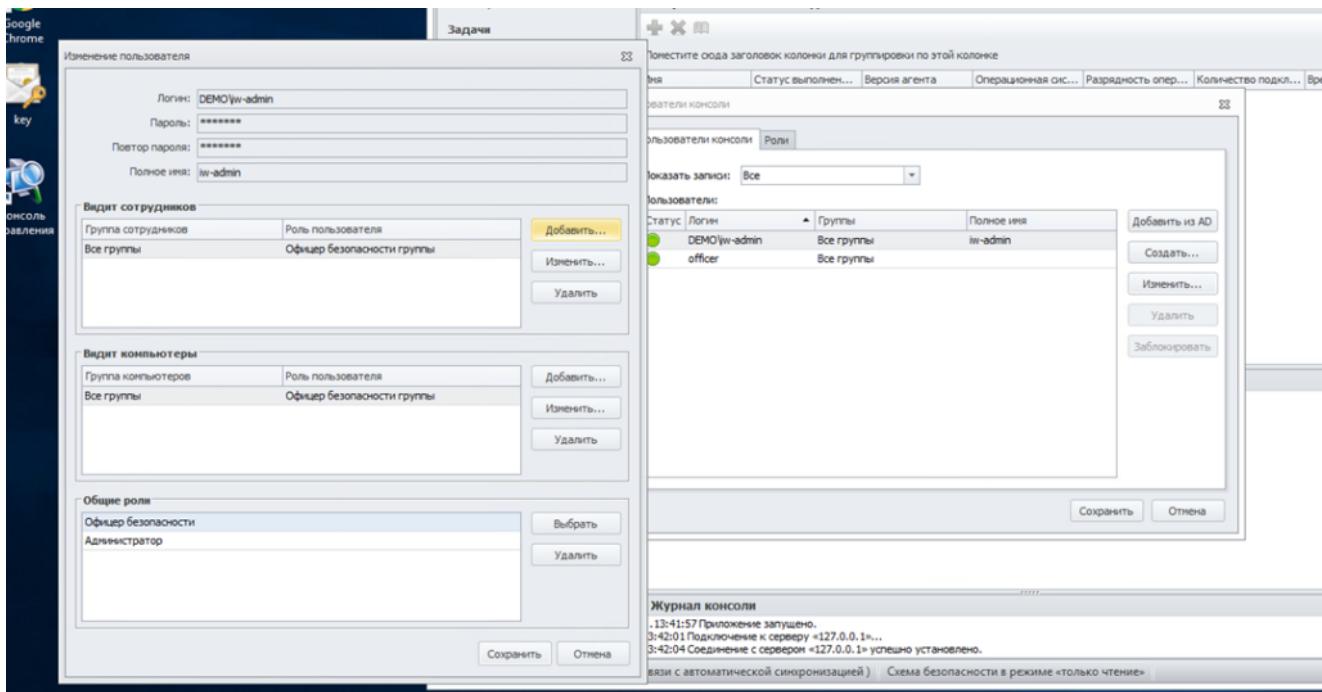
Не забыть седлать тоже самое с ПК



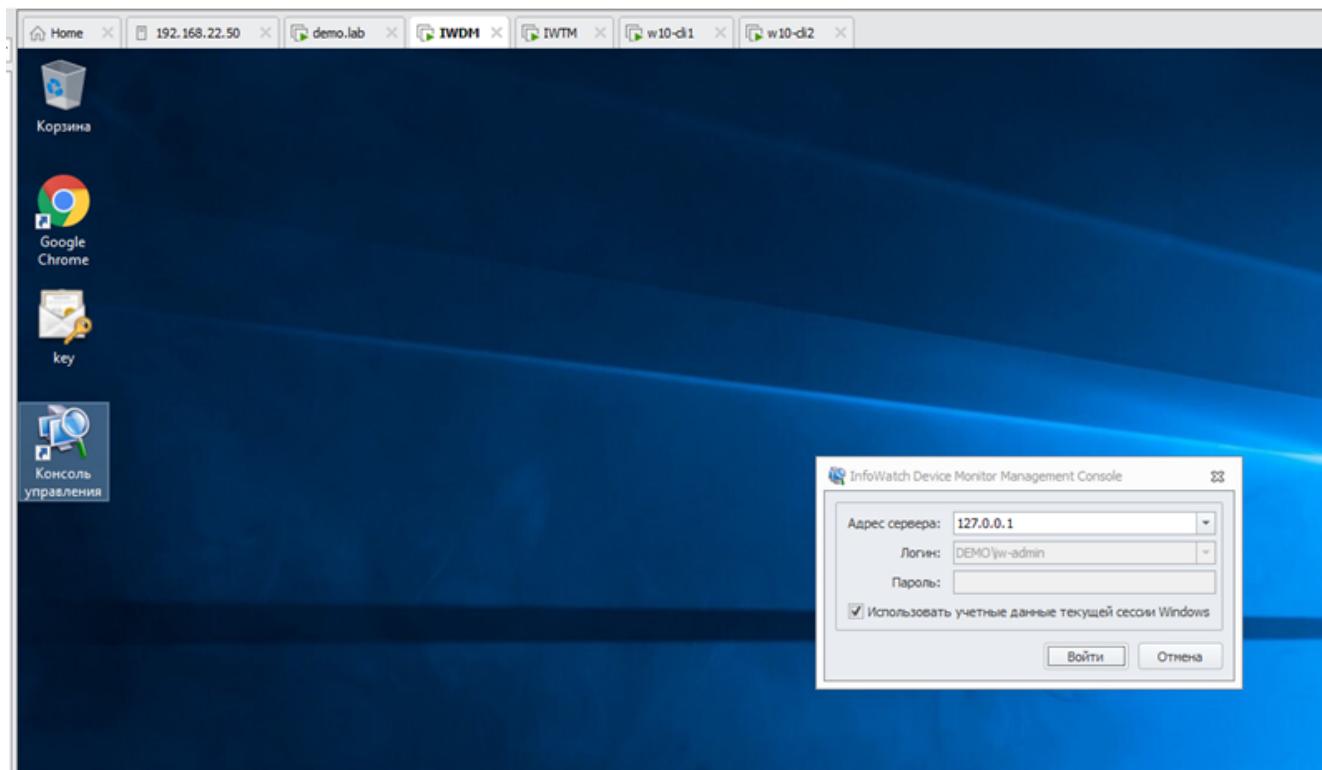


Выбираем добавить из AD

Далее из ранее созданного подразделения – iw-admin и жмем сохранить



Далее выбираем DEMO\iw-admin и жмем изменить, добавляем видит сотрудников, видит компьютеры, общие роли.



Теперь проверяем вход без пороля

Задание 4: Установка агента мониторинга на машине нарушителя

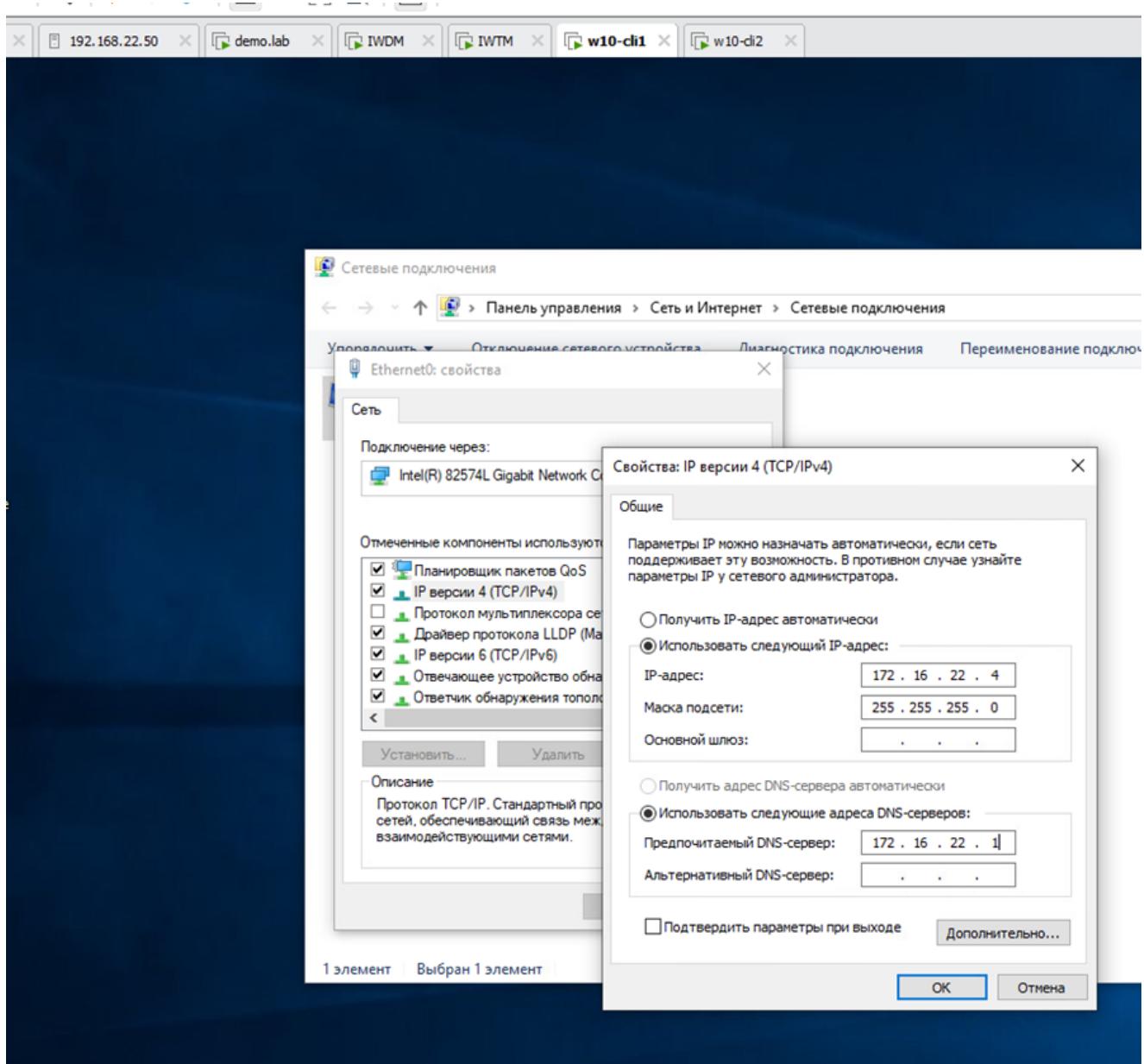
Необходимо ввести клиентскую машину 1 в домен, после перезагрузки войти в систему от ранее созданного пользователя user-agent1.

Необходимо ввести клиентскую машину 2 в домен, после перезагрузки войти в систему от ранее созданного пользователя user-agent2.

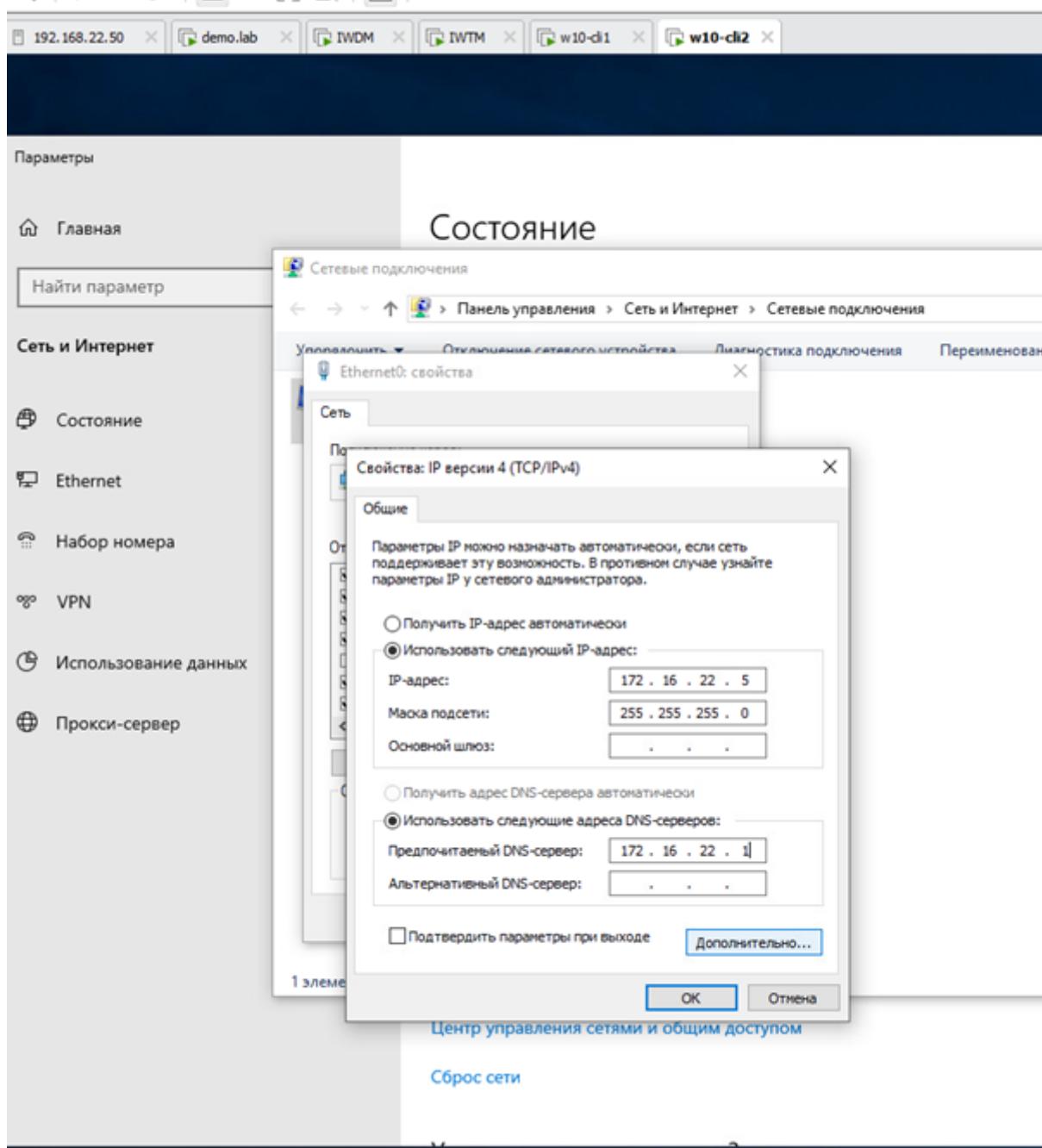
После входа в систему необходимо переместить веденные в домен компьютеры в ранее созданное подразделение “Champ” на домене.

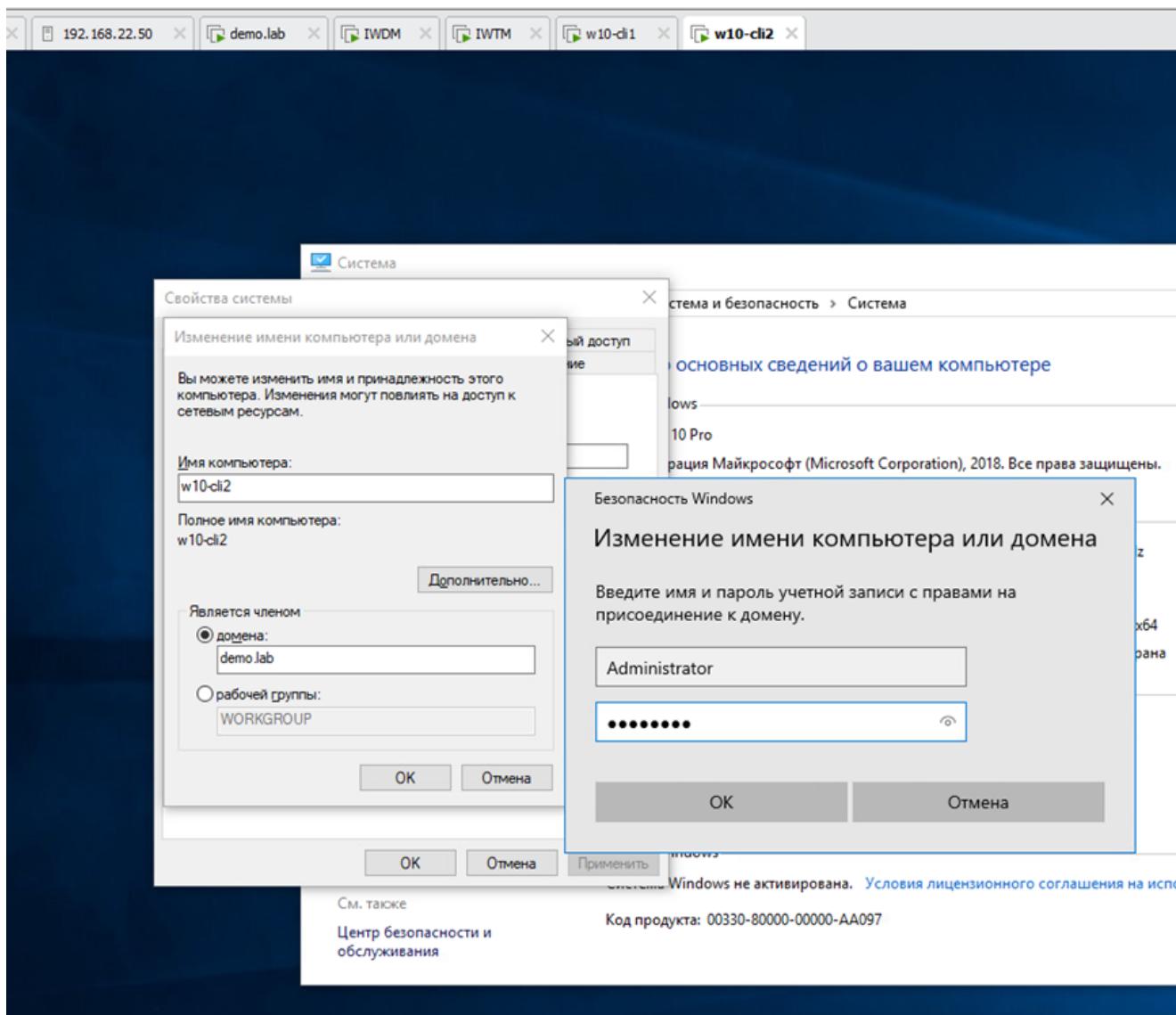
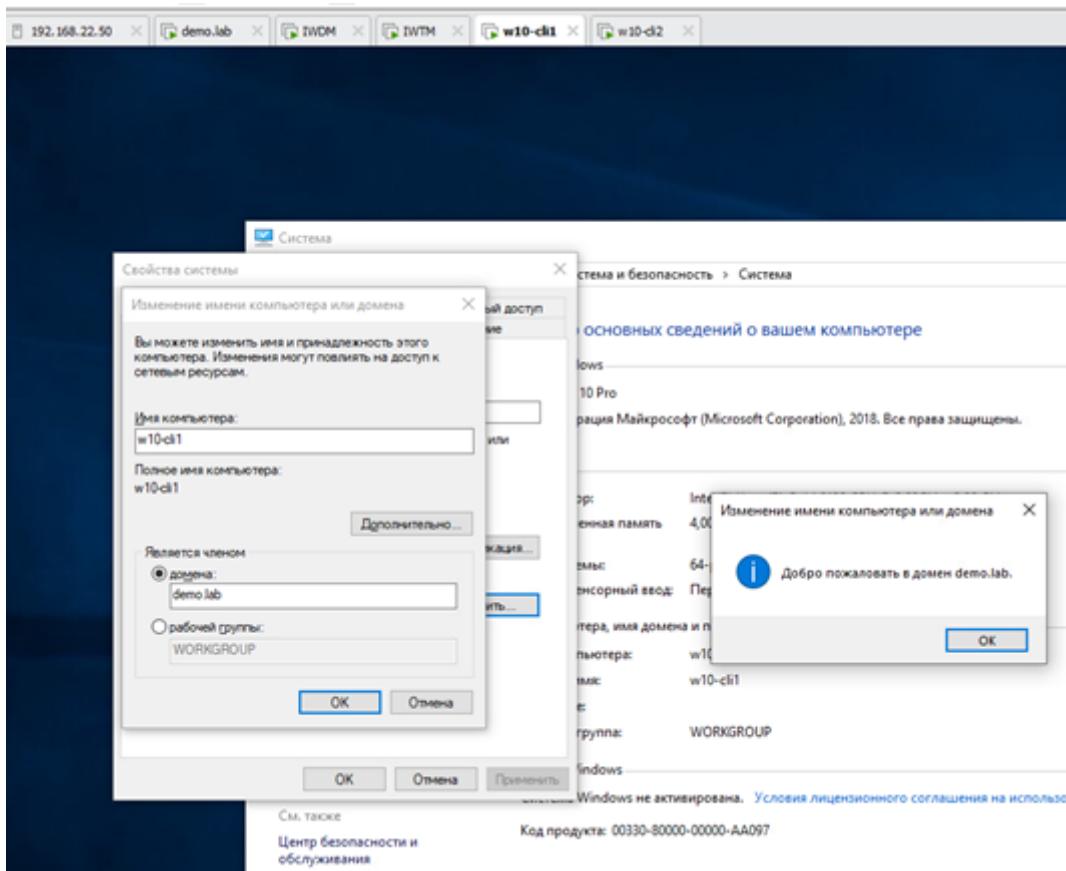
Установить агент мониторинга: На машину 1 с помощью задачи первичного распространения с сервера агентского мониторинга. На машину 2 с помощью групповых политик домена. Необходимо создавать отдельные объекты групповых политик на каждое задание и делать снимки экрана для подтверждения создания и выполнения

политик. Ручная установка с помощью переноса на машину нарушителя пакета установки является некорректным выполнением задания



На клиенте проверяем сетевую настройку.





Меняем имя и вносим в домен

Active Directory - пользователи и компьютеры

Имя	Тип	Описание
IWDM	Компьютер	
W10-CLI1	Компьютер	
W10-CLI2	Компьютер	
iw-admin	Пользователь	
ivtm-officer	Пользователь	
ldap-sync	Пользователь	
user-agent1	Пользователь	
user-agent2	Пользователь	

Просто перетаскиваем пк клиента с Computers в подразделение

InfoWatch Device Monitor Management Console - officer @127.0.0.1 - Задачи

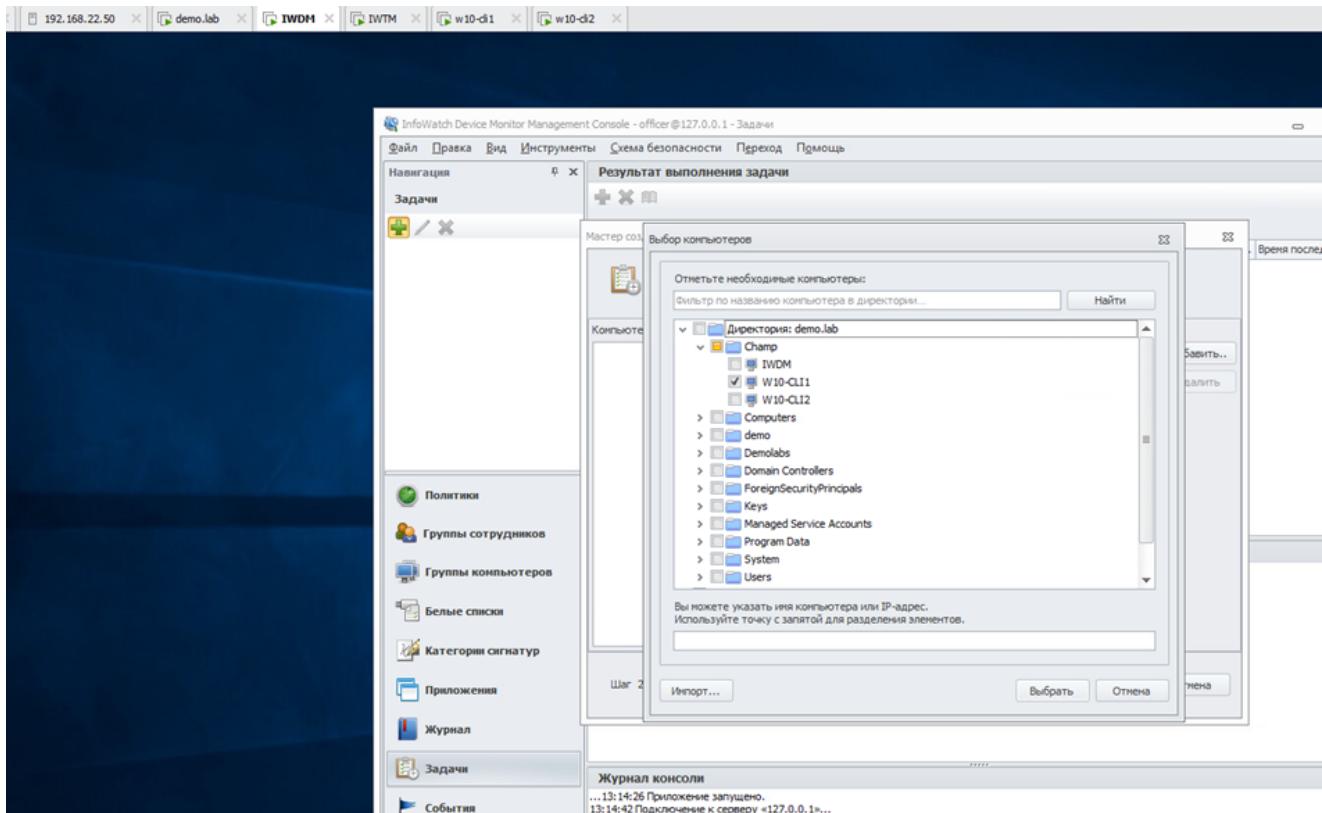
Мастер создания задачи

Шаг 1 из 7

Далее > Отмена

Журнал консоли

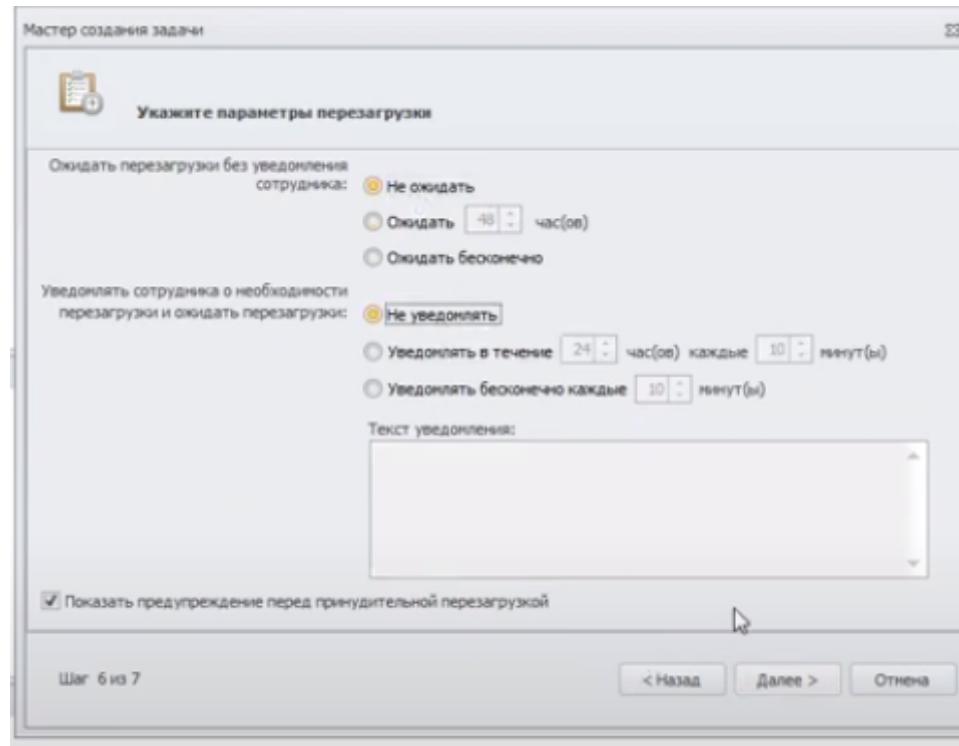
Схема безопасности: 1 (Изменения в связи с автоматической синхронизацией) Схема безопасности в режиме «только чтение»



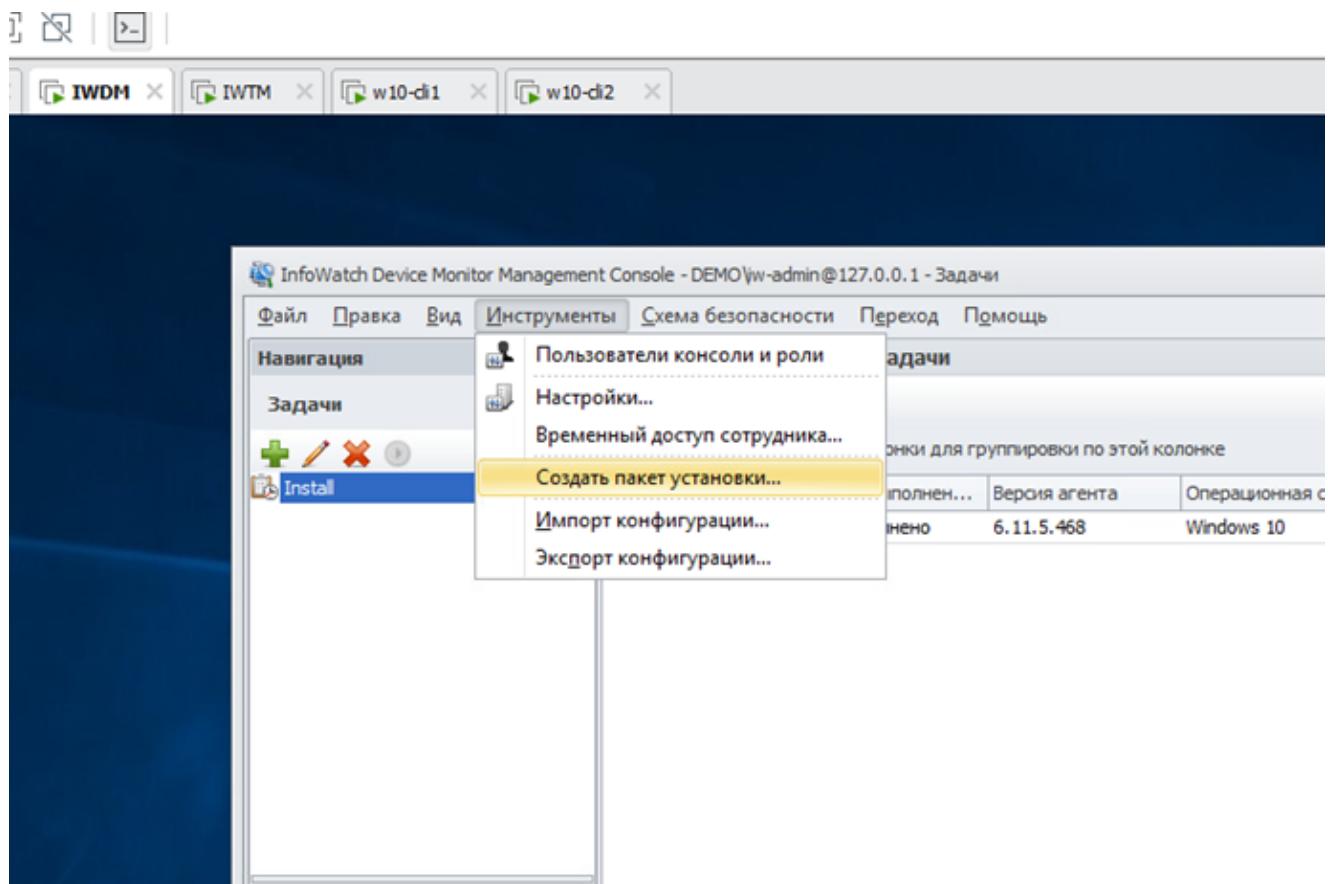
Имя	Статус выполнения задачи	Версия агента	Операционная система	Разрядность опер. системы
W10-CLI1.DEMO.LAB	В процессе		Windows 10	x64

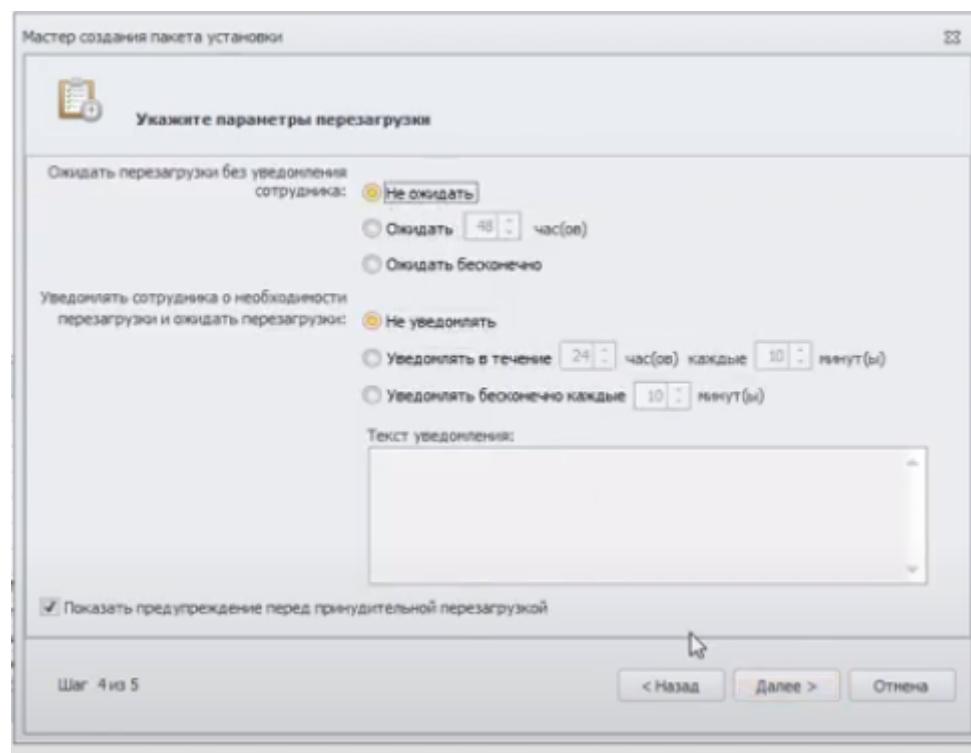
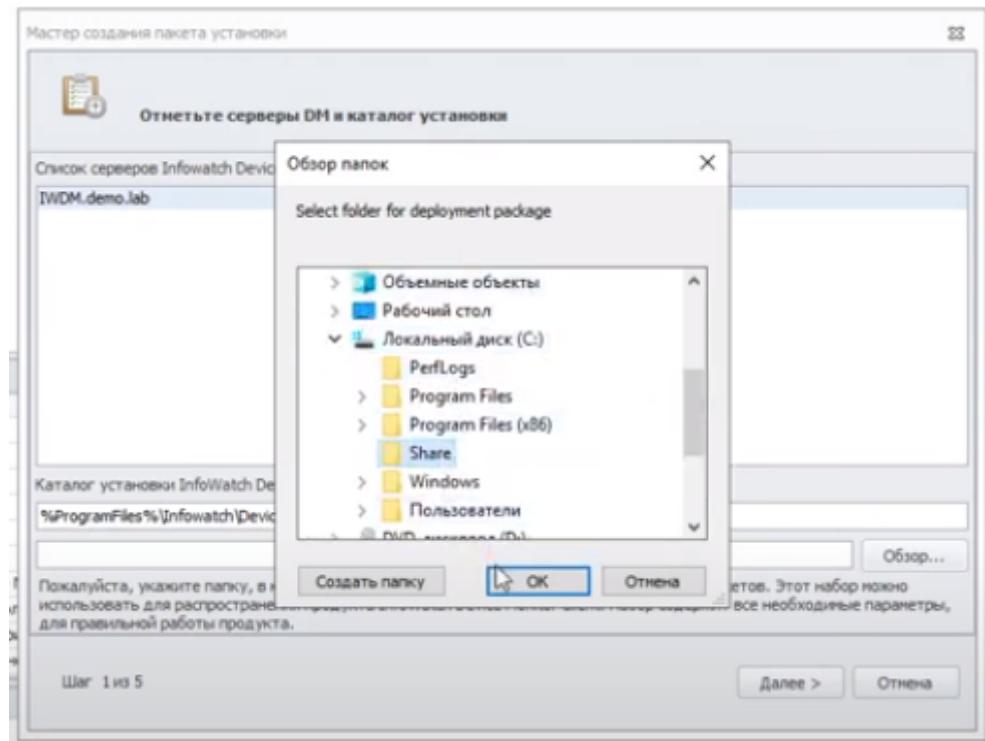
Далее запускаем созданную задачу (после завершения нужно перезагрузить ПК и проверить на клиенте агента – сделать скринь установки и результата на

агенте – загрузить их в созданный документ на рабочем столе iwdm (создать самому!)



2 агент





The screenshot shows the Windows Group Policy Management (GPM) interface. The left pane displays a tree structure under 'Лес: demo.lab / Домены / demo.lab'. The right pane shows the 'Состояние' tab for the 'demo.lab' domain. A modal dialog box titled 'Новый объект групповой политики' (New Group Policy Object) is open, prompting for a name ('Имя:' - Agent) and source ('Исходный объект групповой политики:' - [нет]). Below it, another window titled 'Связи' (Associations) lists 'demo.lab' with 'Путь' (Path) 'demo.lab'. A warning dialog box 'Управление групповой политикой' (Group Policy Management) asks if the user wants to delete delegation rights, with 'OK' and 'Отмена' (Cancel) buttons.

(Удалить – фильтр безопасности)

С GPO связаны следующие сайты, домены и подразделения:

Размещение	Принудительный	Связь задействована	Путь
demo.lab	Нет	Да	demo.lab

Фильтры безопасности
Параметры данного объекта групповой политики определяют, каким образом будут применяться параметры GPO к следующих групп, пользователей и компьютеров:

Имя

Выбор: "Пользователь", "Компьютер" или "Группа"

Выберите тип объекта:
"Пользователь", "Группа" или "Встроенный субъект безопасности"

В следующем месте:
demo.lab

Введите имена выбираемых объектов (примеры):
user-agent2 (user-agent2@demo.lab)

Фильтр WMI
Объект GPO связан со следующим фильтром WMI:
<отсутствует>

(добавить)

Размещение	Принудительный	Связь задействована	Путь
demo.lab	Нет	Да	demo.lab

Фильтры безопасности
Параметры данного объекта групповой политики определяют, каким образом будут применяться параметры GPO к следующих групп, пользователей и компьютеров:

Имя

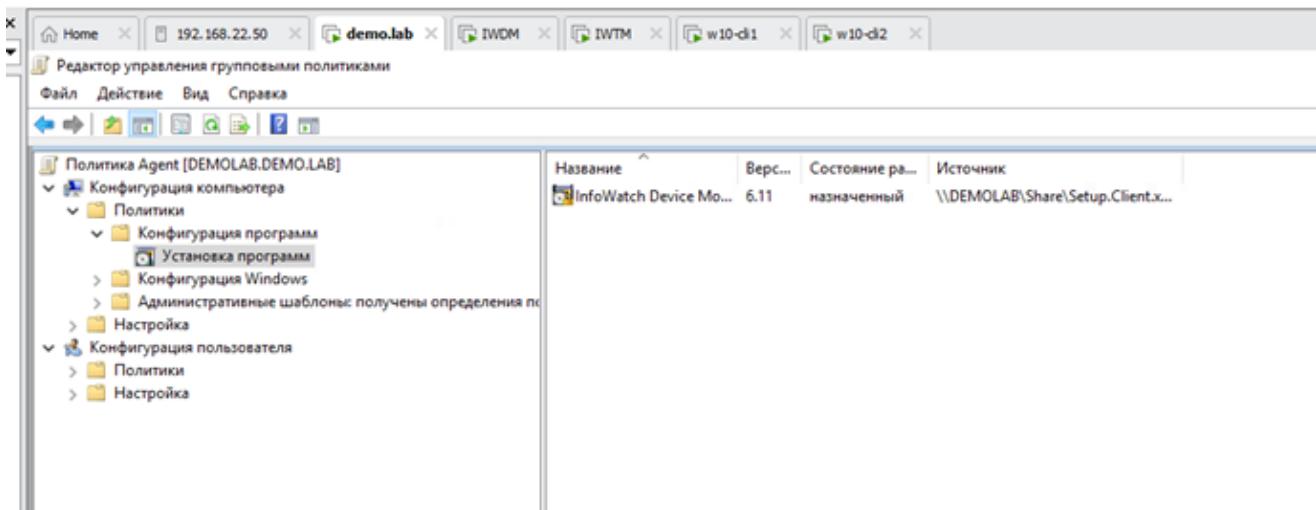
Выбор: "Пользователь", "Компьютер" или "Группа"

Выберите тип объекта:
"Пользователь", "Компьютер", "Группа" или "Встроенный субъект"

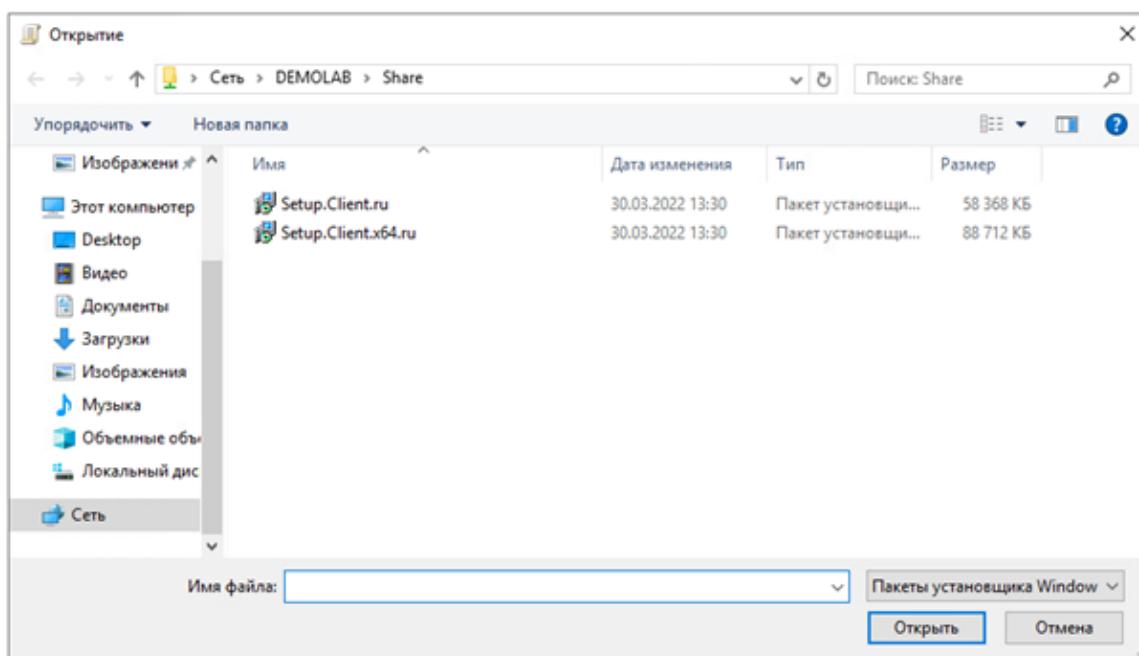
В следующем месте:
demo.lab

Введите имена выбираемых объектов (примеры):
W10-CLI2

Убедитесь, что в типах объекта добавлены компьютеры



Необходимо создать пакет (нажатие правой кнопки мыши)



Выбрать второй (x64)

Необходимо зайти на 2 машину клиента и зайти в командную строку.

```
C:\Windows\system32\cmd.exe - gpupdate /force
Microsoft Windows [Version 10.0.17763.107]
(c) Корпорация Майкрософт (Microsoft Corporation), 2018. Все права защищены.

C:\Users\user-agent2>gpupdate /force
Выполняется обновление политики...

Обновление политики для компьютера успешно завершено.

При обработке политики компьютера возвращены следующие предупреждения:

Клиентскому расширению "Software Installation" групповой политики не удалось применить один или несколько параметров, поскольку эти изменения должны обрабатываться до запуска системы или до входа пользователя. Завершение обработки групповой политики будет выполнено перед следующим запуском системы или входом этого пользователя, что может вызвать замедление загрузки и запуска системы.

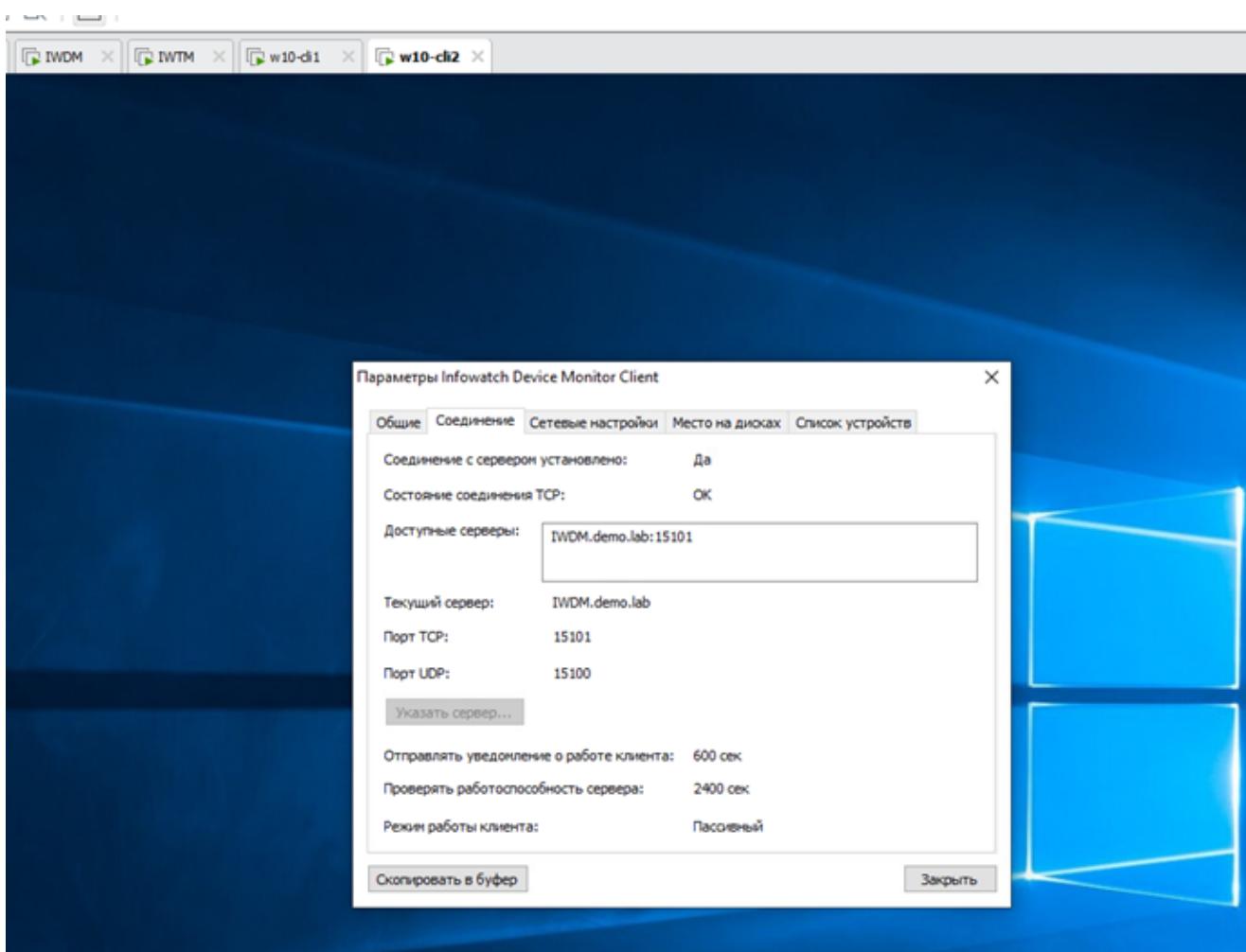
Обновление политики пользователя завершено успешно.

Чтобы получить дополнительные сведения, просмотрите журнал событий или запустите GPRESULT /H GPRReport.html из командной строки для просмотра сведений о результатах групповой политики.

Включены некоторые политики компьютера, выполняющиеся только при загрузке компьютера.

Перезагрузить компьютер? (Y(Да)/N(Нет))y
```

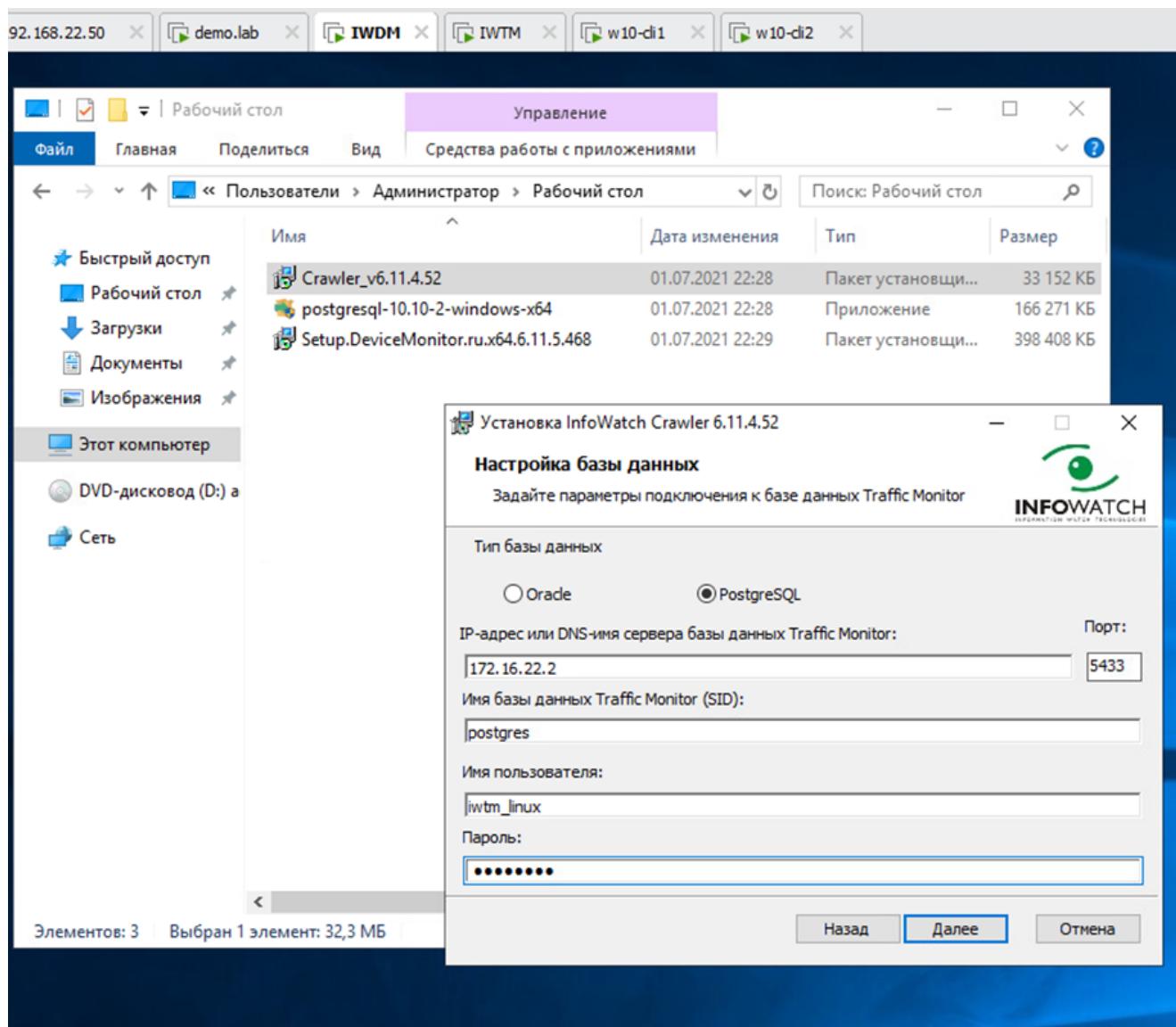
gpupdate /force



Должен появится агент

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).



Далее с iwmd необходимо зайти в командную строку для получения информации о Consul

```
C:\Users\iw-admin>ssh root@172.16.22.2
The authenticity of host '172.16.22.2 (172.16.22.2)' can't be established.
ECDSA key fingerprint is SHA256:/tyqpVxfDBHW7MKssKvQ1ZQiixxpaHkbx8nGXGongNI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.16.22.2' (ECDSA) to the list of known hosts.
root@172.16.22.2's password:
Last login: Wed Mar 23 16:58:10 2022
[root@iwtm ~]#
```

```
[root@iwtm ~]# cat /opt/iw/tm5/etc/consul/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 ~]#
```

Установка InfoWatch Crawler 6.11.4.52

Настройка Traffic Monitor

Задайте параметры подключения агента Consul:

IP-адрес или DNS-имя сервера Traffic Monitor с установленным Consul:
172.16.22.2

Имя центра обработки данных, в котором работает Consul:
iwtm

Секретный ключ для шифрования сетевого трафика Consul:
4RTZ5ttYY6RwIYX28XWNPw==

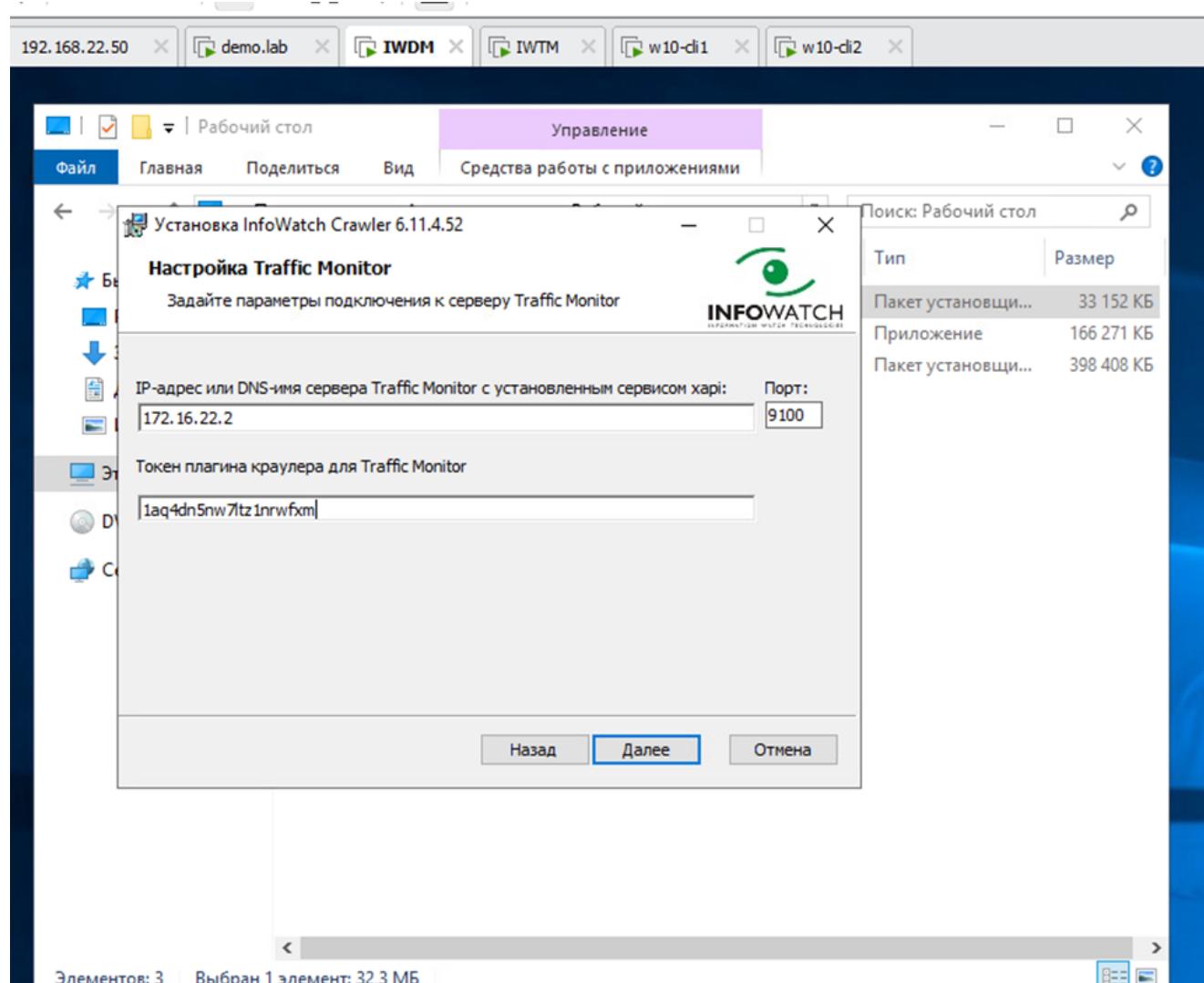
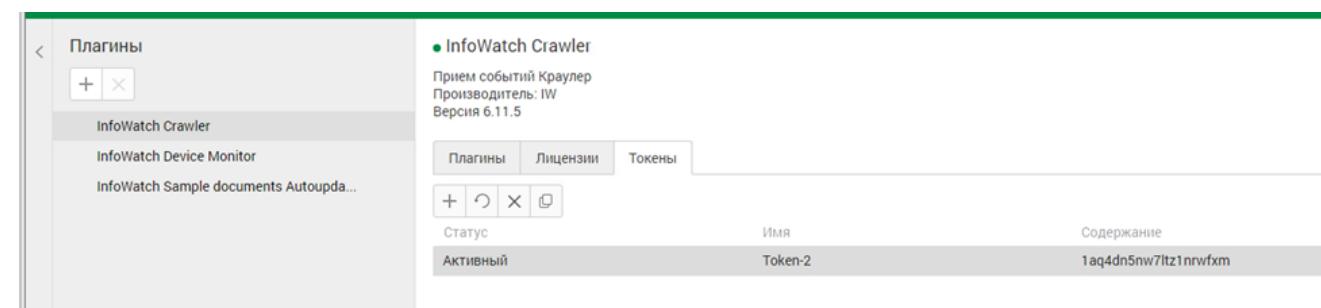
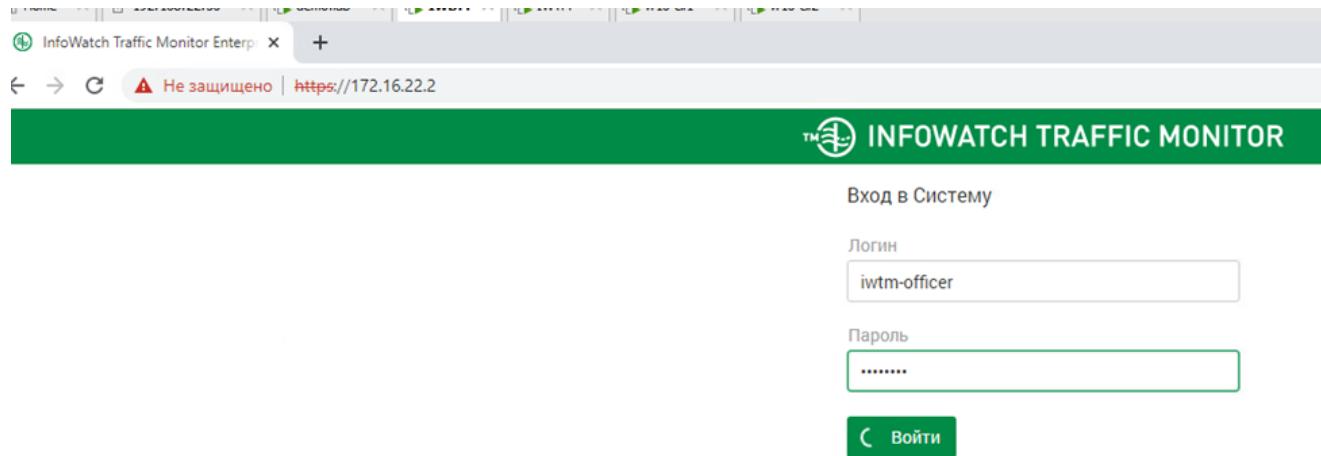
Локальный IP адрес.
Это IP-адрес, который должен быть доступен всем остальным узлам кластера Consul:
172.16.22.3

Назад Далее Отмена

ПОКАРУЧИИ СЛОГИ

Тип	Размер
Пакет установщики...	33 152 КБ
Приложение	166 271 КБ

```
C:\Users\iw-admin>ssh root@172.16.22.2
The authenticity of host '172.16.22.2 (172.16.22.2)' can't be established.
ECDSA key fingerprint is SHA256:/tyqpVxfDBHW7MKssKvQ1ZQiixxpaHkbx8nGXGongNI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.16.22.2' (ECDSA) to the list of known hosts.
root@172.16.22.2's password:
Last login: Wed Mar 23 16:58:10 2022
[root@iwtm ~]# cat /opt/iw/tm5/etc/consul/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 ~]#
```



```

Администратор: Windows PowerShell ISE
Файл Дравка Вид Сервис Отладка Дополнительные компоненты Справка
Безымянный1.ps1* X
1 New-NetFirewallRule -Action Allow -Direction Inbound -Name "Crawler 1337" -DisplayName "Crawler 1337" -Profile Any -Protocol TCP -LocalPort 1337
2 New-NetFirewallRule -Action Allow -Direction Inbound -Name "Crawler 6556" -DisplayName "Crawler 6556" -Profile Any -Protocol TCP -LocalPort 6556

PS C:\Windows\system32> New-NetFirewallRule -Action Allow -Direction Inbound -Name "Crawler 1337" -DisplayName "Crawler 1337" -Profile Any -Protocol TCP -LocalPort 1337
New-NetFirewallRule -Action Allow -Direction Inbound -Name "Crawler 6556" -DisplayName "Crawler 6556" -Profile Any -Protocol TCP -LocalPort 6556

Name      : Crawler 1337
DisplayName : Crawler 1337
Description :
DisplayGroup :
Group     :
Enabled   : True
Profile   : Any
Platform  :
Direction  : Inbound
Action    : Allow
EdgeTraversalPolicy : Block
LocalSourceMapping : False
LocalOnlyMapping : False
Owner     :
PrimaryStatus : OK
Status    : Правило было успешно проанализировано из хранилища. (65536)
EnforcementStatus : NotApplicable
PolicyStoreSource : PersistentStore
PolicyStoreSourceType : Local

```

Стр. 48 Столб. 25 |

New-NetFirewallRule –Action Allow –Direction Inbound –Name “Crawler 1337” –DisplayName “Crawler 1337” –Profile Any –Protocol TCP –LocalPort 1337

New-NetFirewallRule –Action Allow –Direction Inbound –Name “Crawler 6556” –DisplayName “Crawler 6556” –Profile Any –Protocol TCP –LocalPort 6556

(Необходимо открыть от имени администратора)



(зайти на iwtm с iwdm (ssh))

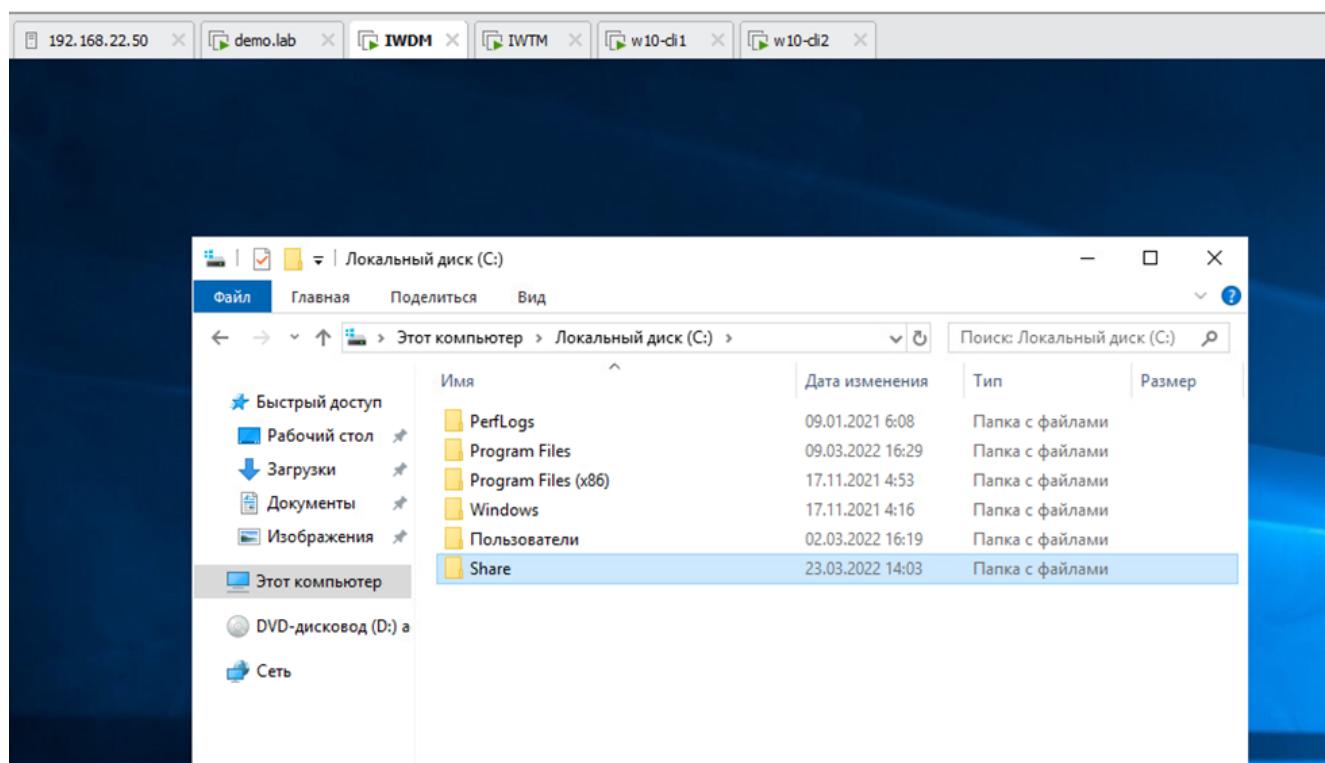
```

        },
        "blackboard": {"enabled": 1},
        "crawler": { "enabled": 1 },
        "export": { "enabled": 1 },
        "import": { "enabled": 1 },
        "notifier": {"enabled": 1 },
        "querytracker": {"enabled": 1 },
        "reporthandler": {"enabled": 1 },
        "reporttracke": {"enabled": 1 },
        "samplecompil": {"enabled": 1 },
        "selection": {"enabled": 1 },
        "systemcheck": {"enabled": 1 },
        "xapisampleco": {"enabled": 1 },
        "kickers_count": 10,
        "kickers_timeout": 1000,
        "mail": {
            "line_break": 0
        }
    }
}

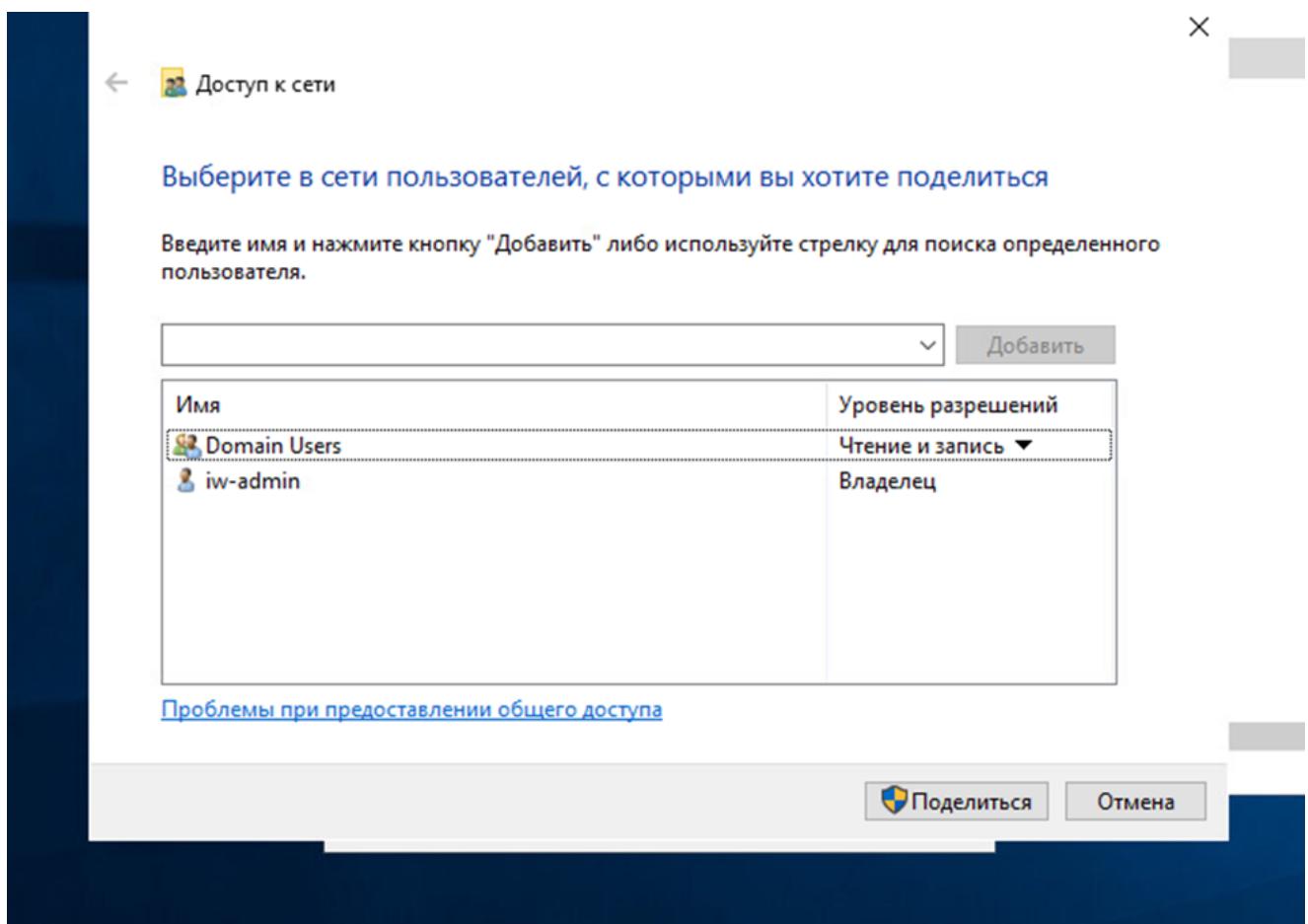
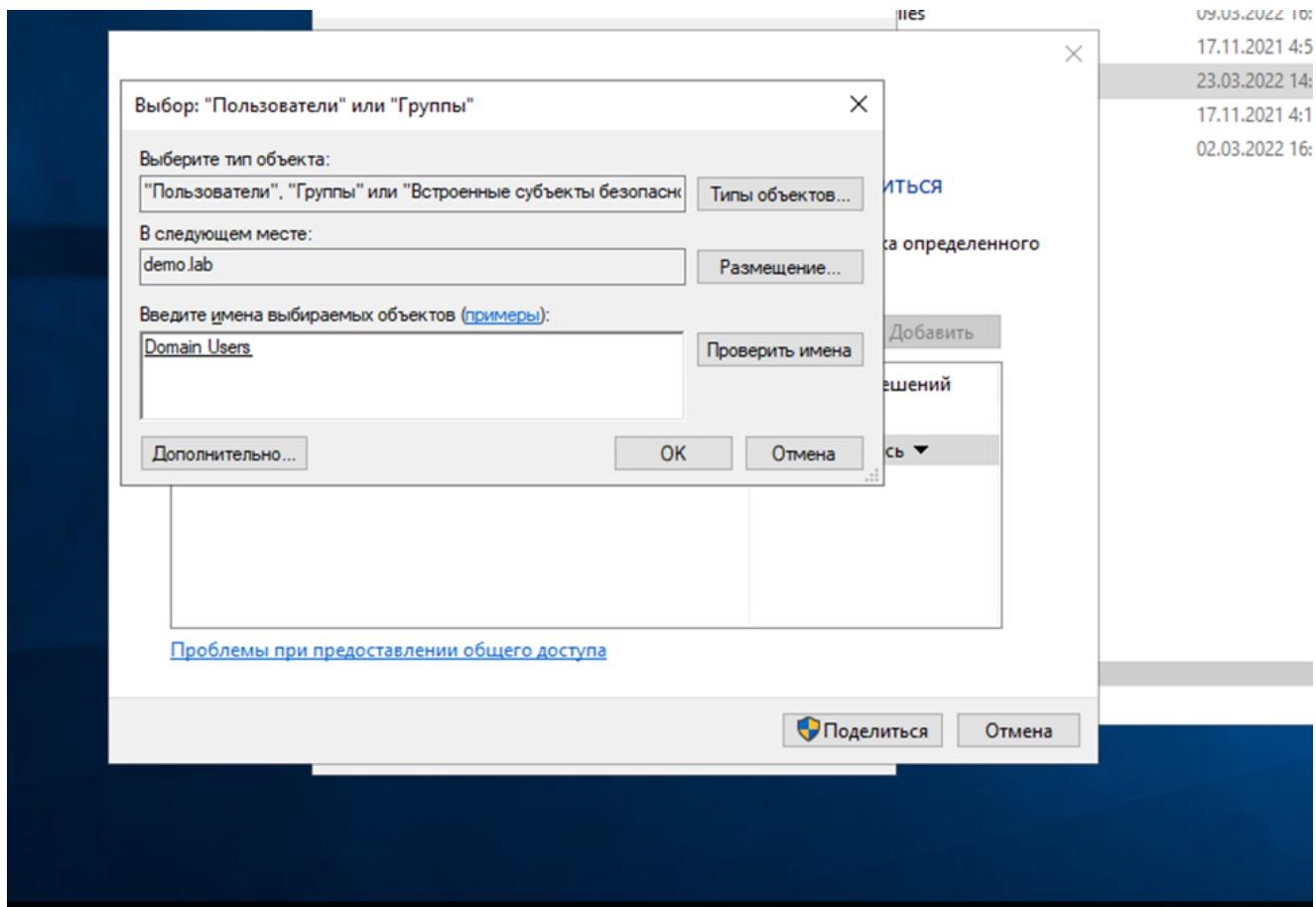
^G Get Help          ^O WriteOut      ^R Read File      ^Y Prev Page      ^K Cut Text      ^C Cur Pos
^X Exit             ^J Justify       ^W Where Is       ^N Next Page

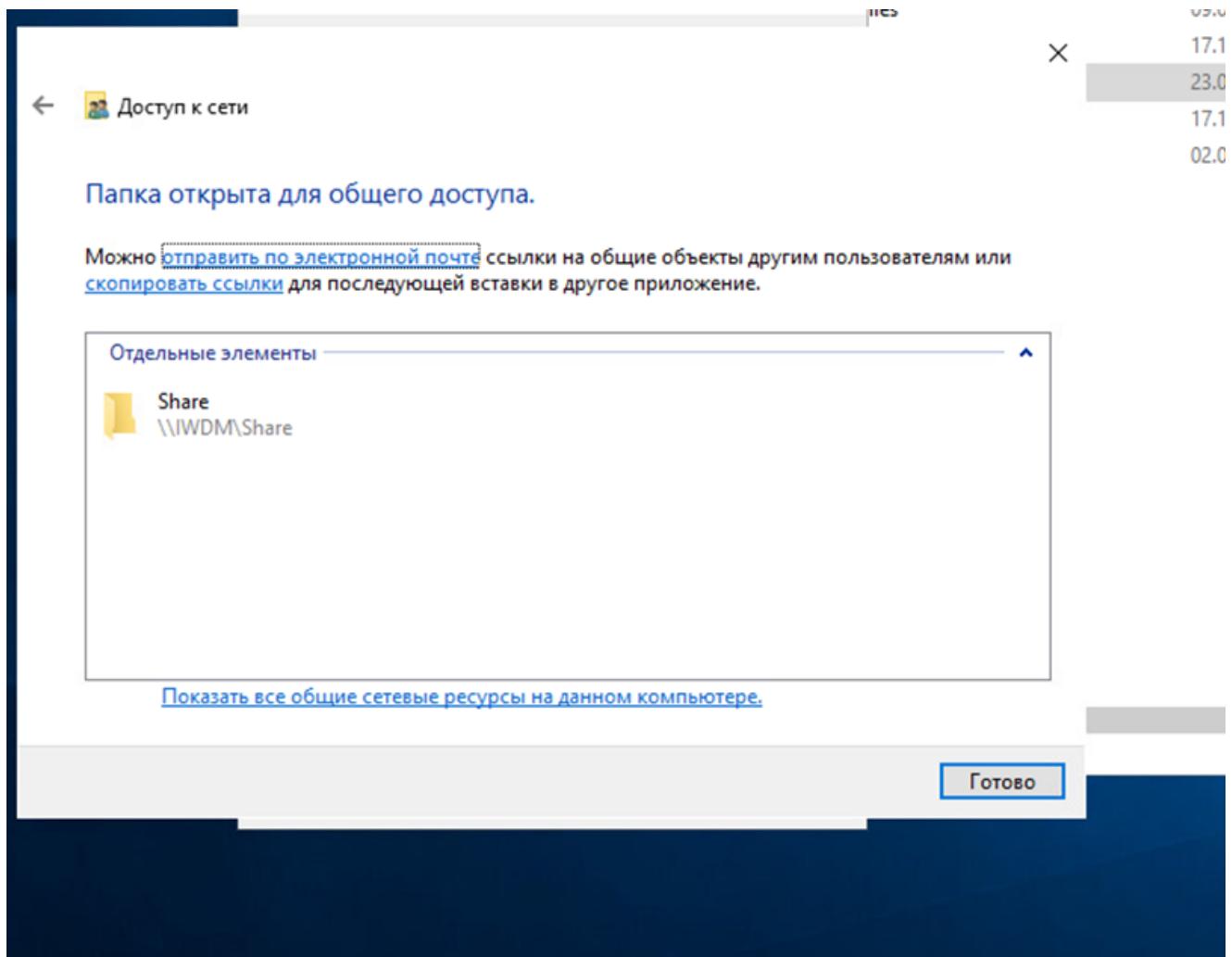
```

Изменить значение 0 на значение 1 напротив Crawler (спуститесь на одну строку ниже crawler и нажмите кнопку назад)



09.05.2022 10:
17.11.2021 4:5
23.03.2022 14:
17.11.2021 4:1
02.03.2022 16:





Папка открыта для общего доступа.

Можно [отправить по электронной почте](#) ссылки на общие объекты другим пользователям или [скопировать ссылки](#) для последующей вставки в другое приложение.

Отдельные элементы

Share
\\IWDM\\Share

[Показать все общие сетевые ресурсы на данном компьютере.](#)

Готово

A screenshot of the InfoWatch Traffic Monitor Enterprise web interface. The top navigation bar includes links for 'Сводка' (Summary), 'События' (Events), 'Отчеты' (Reports), 'Технологии' (Technologies), 'Объекты защиты' (Protected objects), 'Персоны' (Persons), 'Политики' (Policies), 'Списки' (Lists), 'Управление' (Management), and 'Краулер' (Crawler). The 'Краулер' tab is selected. On the left, there is a sidebar with a 'Краулер' section containing a 'Редактировать сканер' (Edit scanner) button and a set of icons for managing tasks. The main content area displays the message 'Нет задач' (No tasks). The URL in the browser address bar is https://172.16.22.2/crawler.

Если же ваш краулер не отобразился, то проверьте выключен ли брандмауэр на demo.lab и перезагрузите эту машину. Далее проверьте на iwtm наличие dns и также перезагрузите. IWDM лучше тоже перезапустить.

Сводка События Отчеты Технологии ▾ Объекты защиты Персоны Политики Списки ▾ Управление ▾ Краулер

Краулер Редактировать сканер

Создание задачи

Название: Scan
Описание:

Объект сканирования

Цель сканирования: Разделяемые сетевые ресурсы
Сканируемые группы и компьютеры: IWDM X
Режим сканирования: Все папки
 Исключая системные папки

Авторизация

Авторизация сканера:

Расписание:

Период сканирования: Ежедневно
Начало действия: 30/03/2022
Время: 0.00

Искать файлы

Минимальный размер (КБ): 0

Сохранить Отменить

Режим сканирования: Только папки
Фильтр Share *Share C:\Share
 Исключая системные папки

Файл Главная Поделиться Вид

3.202 Эта задача < > < > Этот компьютер > Локальный диск (C:) > Share Поиск: Share /размер

Быстрый доступ Рабочий стол Загрузки Документы Изображения Share

Этот компьютер DVD-дисковод (D:) а

Имя	Дата изменения	Тип	Размер
scanning	30.03.2022 13:06	Текстовый документ	1 КБ
scanning1	30.03.2022 13:10	Текстовый документ	1 КБ

Краулер Редактировать сканер

Scan Скачать XLSX-отчет

Запуск задачи Scan...

Scan Разделяемые сетевые ресурсы
Дата запуска: не запускалась
Статус: не запускалась

Статус	Дата запуска	Дата остановки	Обработано ко...	Не обработано...	Всего файлов/размер	Новых файлов/размер
	30.03.2022, 13:09:55	Отсутствует	0	0	0 / 0.00 MB	0 / 0.00 MB

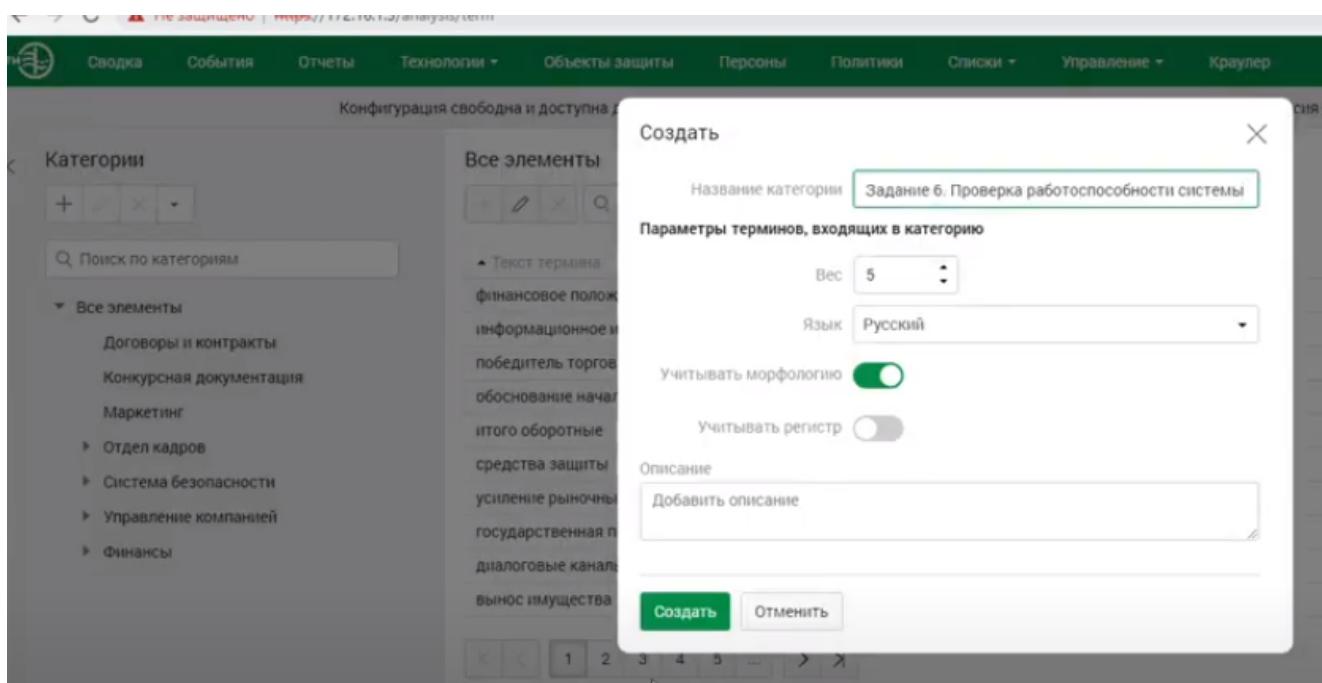
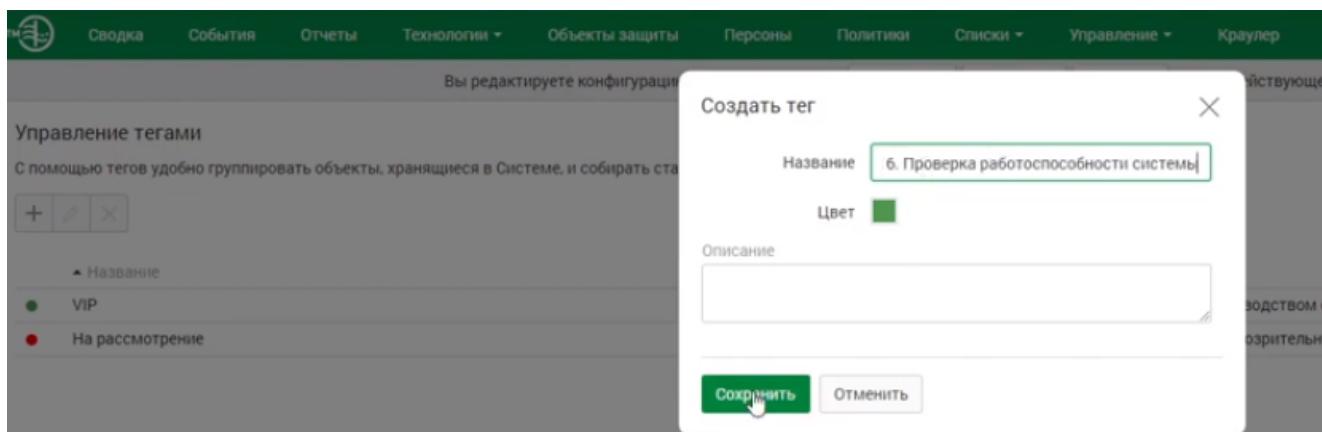
Сделать такой скрин!

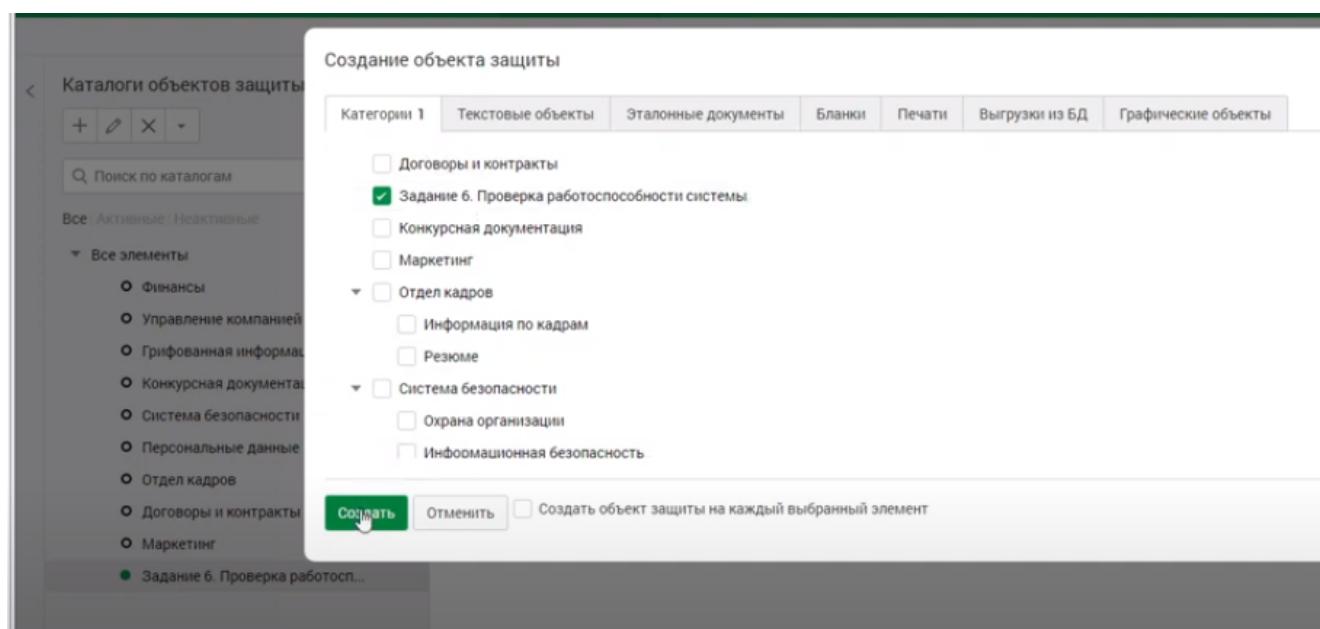
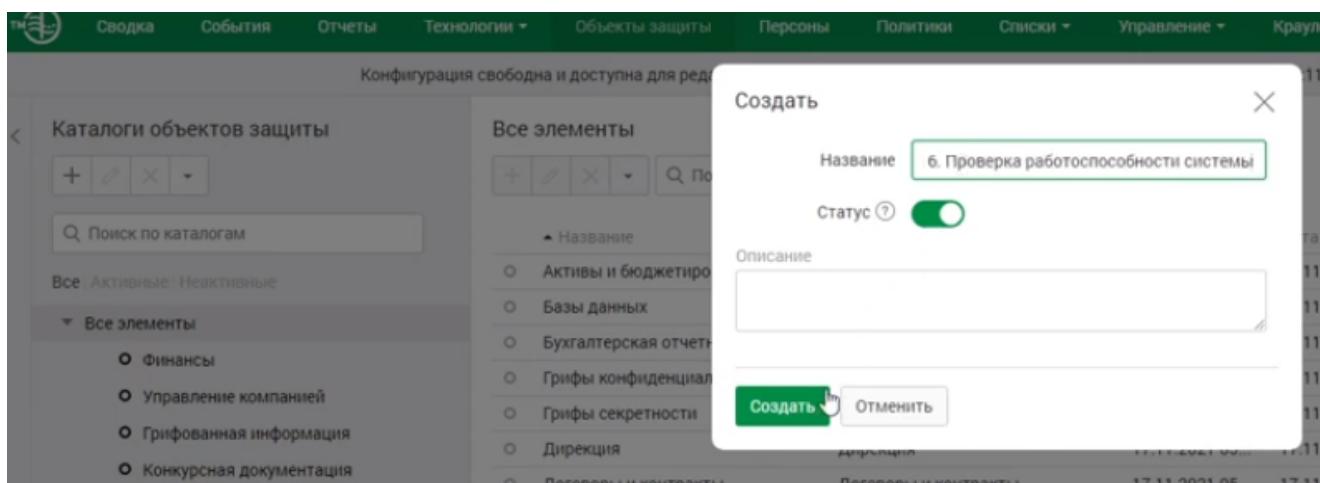
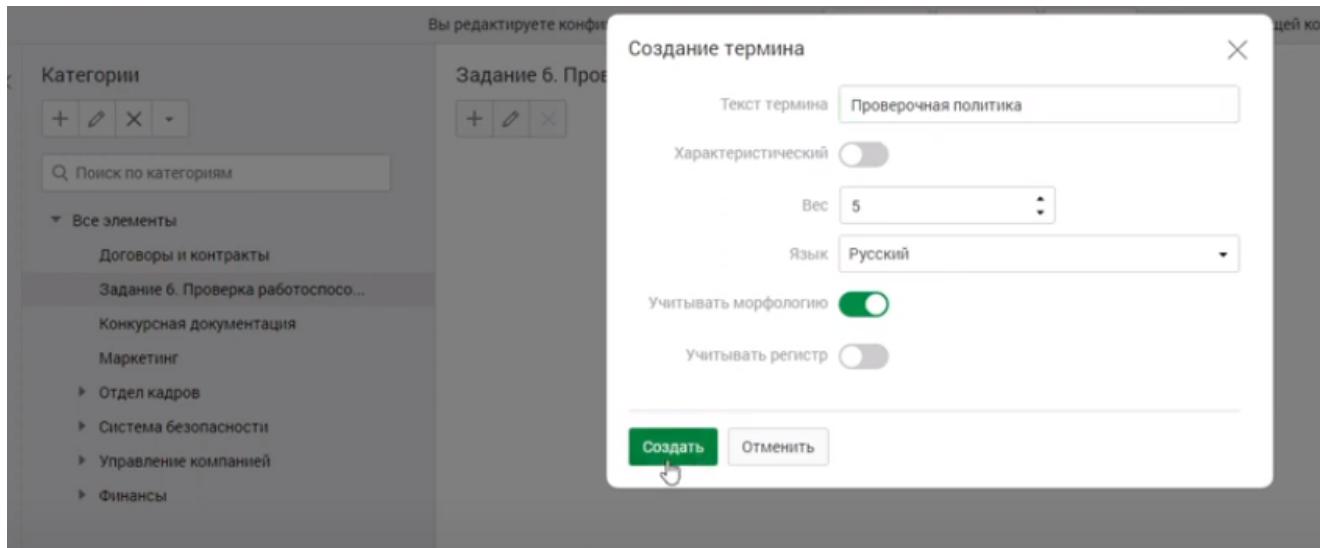
Задание 6: Проверка работоспособности системы

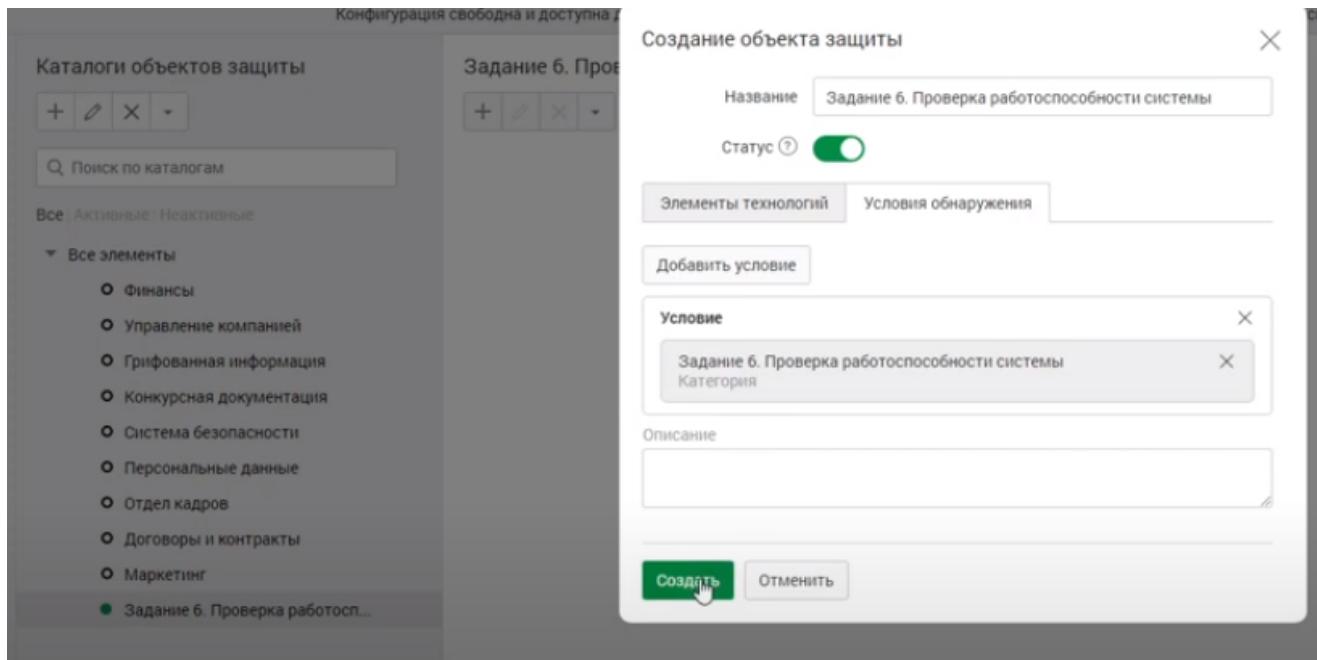
Необходимо создать проверочную политику на правило передачи, копирования, хранения и буфера обмена (или работы в приложениях), все 4 варианта срабатывания событий для данных, содержащих некий термин, установить уровень угрозы для всех событий, добавить тег.

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.







Вы редактируете конфигурацию с 13.05.2022 12:10. Применить Сохранить Сбросить Версия действующей конфигурации - № 9.

Политики	Добавить политику	Фильтр	Политика защиты данных	Добавить правило
Политики защиты данных:			Название: Задание 6. Проверка работоспособности системы I Период действия: Все время Статус: включен	
● Политика защиты данных Политика на любые данные Передача Копирование Хранение Работа в приложениях			Защищаемые данные	

Выбор защищаемых данных

Каталоги объектов защиты 1	Объекты защиты	Файловые форматы
<input type="checkbox"/> Грифованная информация	<input checked="" type="checkbox"/> Задание 6. Проверка работоспособности системы	
<input type="checkbox"/> Договоры и контракты	<input type="checkbox"/> Конкурсная документация	
<input type="checkbox"/> Маркетинг	<input type="checkbox"/> Отдел кадров	
<input type="checkbox"/> Персональные данные	<input type="checkbox"/> Персональные данные	
<input type="checkbox"/> Система безопасности	<input type="checkbox"/> Управление компаний	
<input type="checkbox"/> Управление компанией	<input type="checkbox"/> Финансы	

Сохранить Отменить

Политики	Добавить политику	Фильтр	Политика защиты данных	Добавить правило
Политики защиты данных:			Название: Политика защиты данных Период действия: Все время Статус: включен	
● Политика защиты данных Политика на любые данные Передача Копирование Хранение Работа в приложениях			Защищаемые данные	
<p>Политика сработает при обнаружении хотя бы одного вхождения в каждый из типов данных</p> <p>Каталоги объектов защиты</p> <p>Задание 6. Проверка работоспособности системы</p> <p>Описание: Введите описание</p> <p>Создан: 13.05.2022 12:10 Изменен: 13.05.2022 12:10</p>				

Вы редактируете конфигурацию с 13.05.2022 12:14. Применить Сохранить Сбросить Версия действующей конфигурации - № 13.

Политики

Политики защиты данных:

● Политика защиты данных

Каталог объектов защиты: Задание 6. Проверка работоспособности системы

Передача Копирование Хранение Работа в приложениях

Добавить правило

Отправители: Любой отправитель
Направление маршрута: 11
Получатели: Любой получатель
Действия: не заданы

Действия по умолчанию: не заданы

Правило передачи

Направление маршрута: → В одну сторону, ≠ В оба направления

Тип события: Веб-сообщение, Facebook, ICQ, Mail.Ru Агент, MS Lync, Skype, Telegram, XMPP, ВКонтакте, Почта в Браузере, Почта на Клиенте

Компьютеры: W10-CLI1

Отправители: demo.lab, Пользовательские группы

Получатели: demo.lab, Пользовательские группы

Делаем для передачи

Правило передачи

Получатели: demo.lab, Пользовательские группы

Дни действия правила: Любой день недели

Часы действия правила: 0:00 - 0:00

Действия при срабатывании правила

Отправить почтовое уведомление: Начните вводить текст

Назначить событию вердикт: Разрешить

Назначить событию уровень нарушения: Низкий

Назначить событию теги: Задание 6. Проверка работоспособности системы

Назначить отправителю статус: Выберите статус

Удалить событие: Активация Windows

Сохранить Отменить

Чтобы активировать Windows, перейдите в раздел "Параметры".

12:16 13.05.2022

Политики

Добавить политику Фильтр

Политики защиты данных:

● Политика защиты данных

Каталог объектов защиты: Задание 6. Проверка работоспособности системы

Передача 1 Копирование Хранение Работа в приложениях

Добавить правило

Ресурс: Любой
Отправители: Любой отправитель
Действия: не заданы

Действия по умолчанию: не заданы

Правило копирования

Направление маршрута: → В одну сторону, ≠ В оба направления

Тип события: FTP, Облачное хранилище, Сетевой ресурс, Съемное устройство, Терминальная сессия, Печать

Компьютеры: W10-CLI1

Отправители: demo.lab, Пользовательские группы

Приемник копирования: Начните вводить текст

Источник копирования: Начните вводить текст

Дни действия правила: Любой день недели

Часы действия правила: 0:00 - 0:00

Действия при срабатывании правила

Для копирования

Правило копирования

Отправители	=	<input type="button" value="demo.lab X"/> <input type="button" value="Пользовательские группы X"/>	<input type="button" value="+"/>
Приемник копирования	<input type="text" value="Начните вводить текст"/> <input type="button" value="+"/>		
Источник копирования	<input type="text" value="Начните вводить текст"/> <input type="button" value="+"/>		
Дни действия правила	<input type="text" value="Любой день недели"/>		
Часы действия правила	0:00	-	0:00

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 type="radio"/> Низкий
Назначить событию теги	<input type="text" value="Задание б. Проверка работоспособности системы"/> <input type="button" value="+"/>
Назначить отправителю статус	<input type="text" value="Выберите статус Windows"/> <input type="button" value="+"/>

Сохранить Отменить

Политики

Политики защиты данных:

• Политика защиты данных	
Каталог объектов защиты: Задание б. Проверка работоспособности системы	
Передача 1	Копирование 1
Хранение	Работа в приложениях
Добавить правило	
Тип события	Краулер
Место хранения	<input type="checkbox"/> W10-CLI1
Владельцы файла	<input type="checkbox"/> user-agent1
Кому доступен файл	<input type="checkbox"/> Доступно всем
Действия	не заданы
Действия по умолчанию	

Добавить политику Фильтр

Правило хранения

Тип события	Краулер
Место хранения	<input type="checkbox"/> W10-CLI1
Владельцы файла	<input type="checkbox"/> user-agent1
Кому доступен файл	<input type="checkbox"/> Начните вводить текст
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 type="radio"/> Низкий
Назначить событию теги	<input type="text" value="Задание б. Проверка работоспособности системы"/> <input type="button" value="+"/>
Назначить отправителю статус	<input type="text" value="Выберите статус"/> <input type="button" value="+"/>
Удалить событие	

Активация Windows
Активация Windows, перейдите в раздел

Хранение

Правило работы в приложениях

Тип события: Буфер обмена
Компьютер: W10-CLI1
Приложение-источник: Любое приложение
Приложение-предназначение: Любое приложение
Действия: не заданы
Действия по умолчанию: не заданы

Правило работы в приложениях

Приложения: Начните вводить текст

Только для терминальной сессии: включен

Приложение-источник: Начните вводить текст

Приложение-предназначение: Начните вводить текст

Дни действия правила: Любой день недели

Часы действия правила: 0:00 - 0:00

Действия при срабатывании правила

Отправить почтовое уведомление: Начните вводить текст

Назначить событию вердикт: Разрешить (selected)

Назначить событию уровень нарушения: Низкий

Назначить событию теги: Задание 6. Проверка работоспособности системы

Назначить отправителю статус: Активация Windows

Сохранить | Отменить | Параметры

Сделать конечный скрин политики

Задание 7: Защита системы с помощью сертификатов

Создайте дерево сертификатов формата PKCS для защиты веб-соединения с DLP-сервером по протоколу HTTPS. Сертификат и используемый ключ должен удовлетворять общепринятым на сегодня стандартам и требованиям, параметры сертификата должны соответствовать атрибутам компании.

Утилита для создания сертификата — на выбор участника из доступных в операционных системах и дистрибутивах (openssl или аналоги). Дерево сертификатов должно включать:

1. корневой root-сертификат (ca)
2. серверный (server) сертификат
3. по желанию допускается использование пользовательского и промежуточного сертификата.

Атрибуты для сертификатов:

Страна: RU

Область: Tomskaya

Организация: WorldSkills

Город: Tomsk

Отдел организации: IT

E-mail: support@demo.lab

После генерации сертификатов необходимо установить серверный сертификат на веб-сервер DLP-системы, а также установить корневой сертификат как доверенный в контроллер домена для использования на всех компьютерах в сети для доверенного подключения к веб-консоли DLP-системы уровня сети. Итоговый результат должен включать:

Дерево из 2-3 сертификатов, упакованных в пакет PKCS (.p12), а также представленные в виде отдельных файлов ключей и сертификатов, расположенных на рабочем столе. Содержимое команд по генерации ключей и сертификатов в текстовом файле на рабочем столе с комментариями. Скриншоты успешного подключения к консоли сервера DLP без ошибок сертификата, скриншоты окон просмотра сертификата в системе с помощью

оснастки «Сертификаты» операционной системы (вкладки «Общие», «Путь сертификации»).

Описание модуля 2:

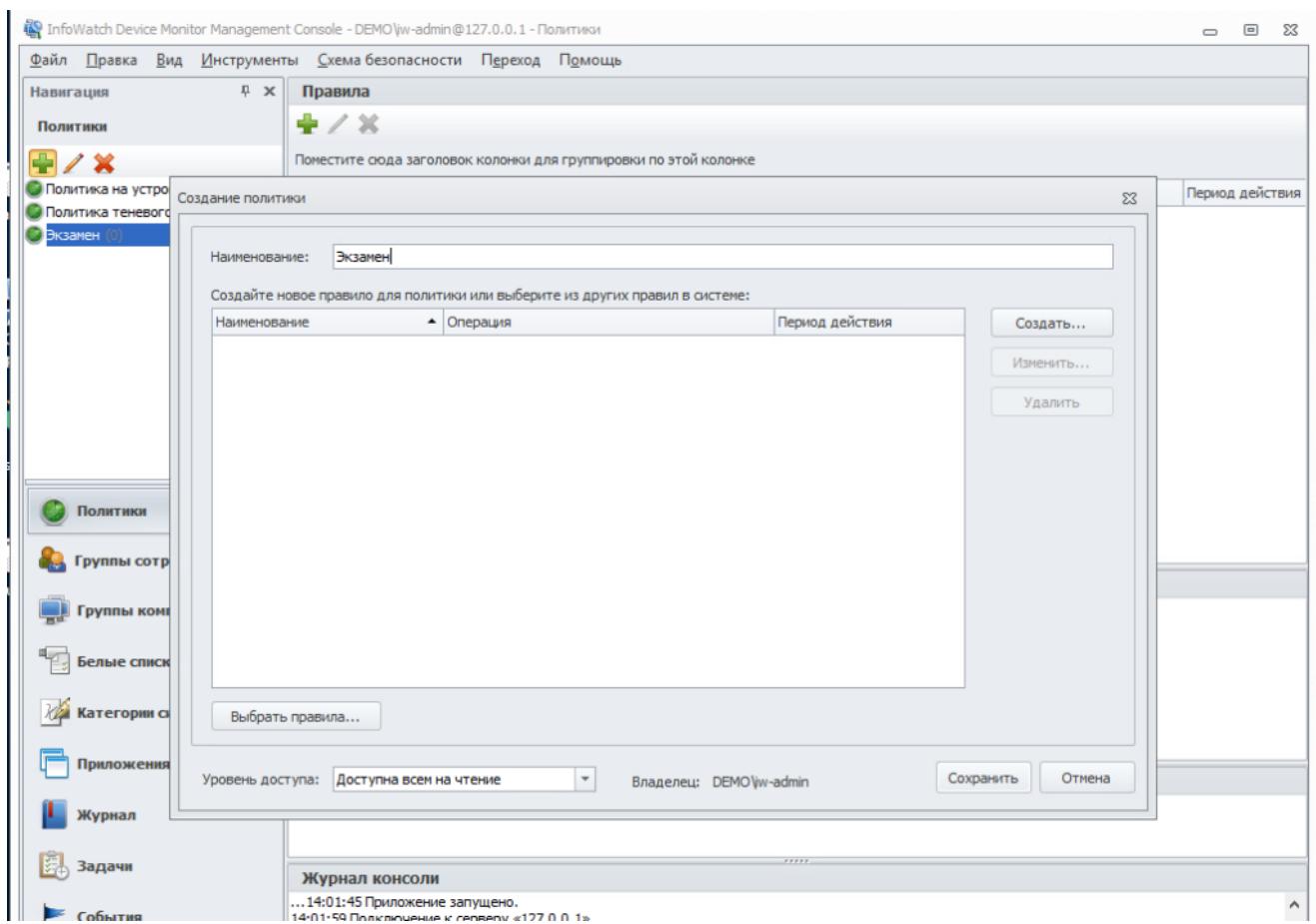
Задания выполняются только с помощью компонентов DLP системы или групповых политик (указано в задании). Все сценарии заданий (где применимо) необходимо воспроизвести и зафиксировать результат.

Называйте созданные вами разделы/политики/группы и т. п. в соответствии с заданием, например, «Политика 1» или «Правило 1.2» и т. д., иначе проверка заданий может быть невозможна. Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно).

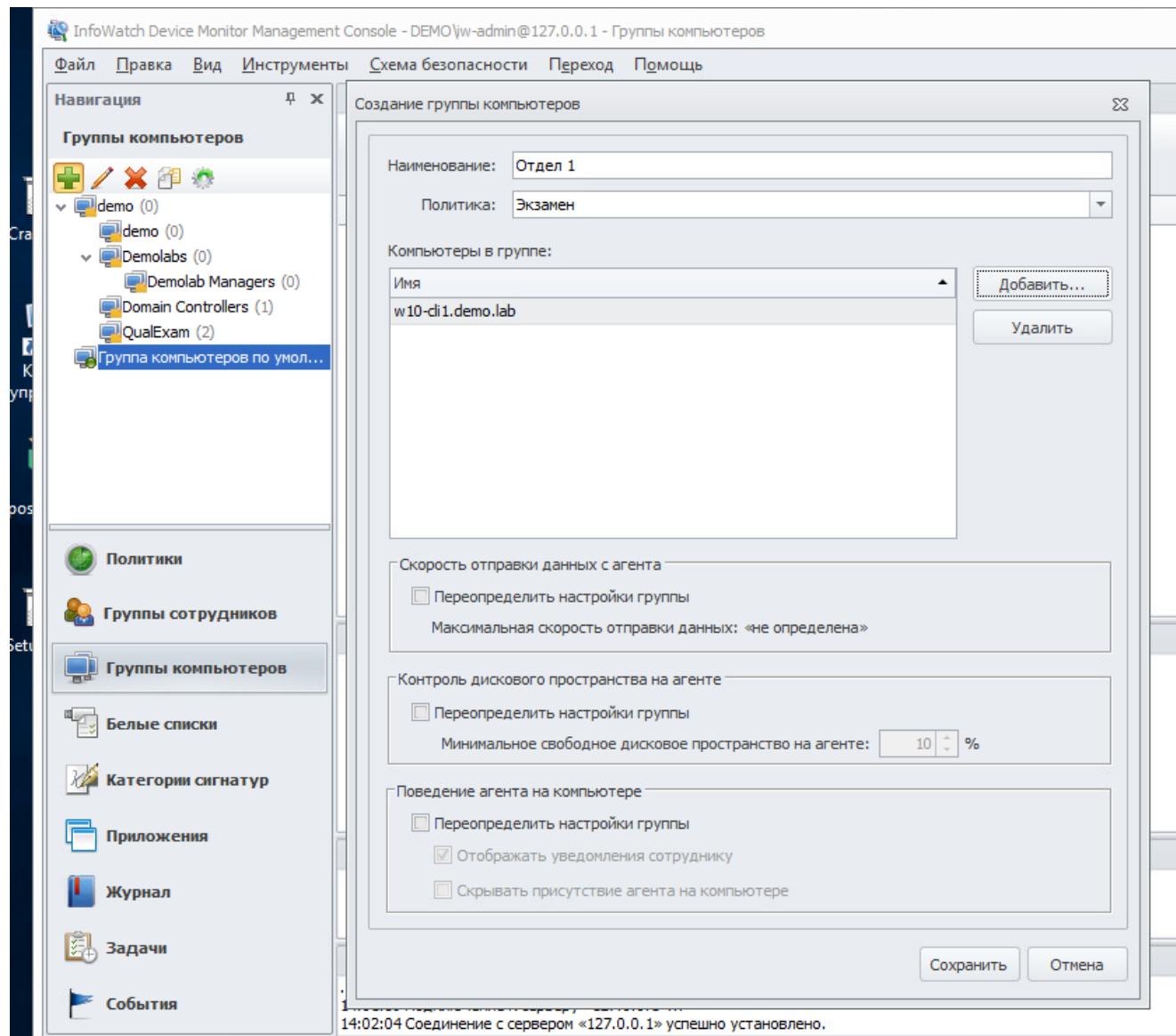
Задание 1

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.



Переходим во вкладку «группы компьютеров»



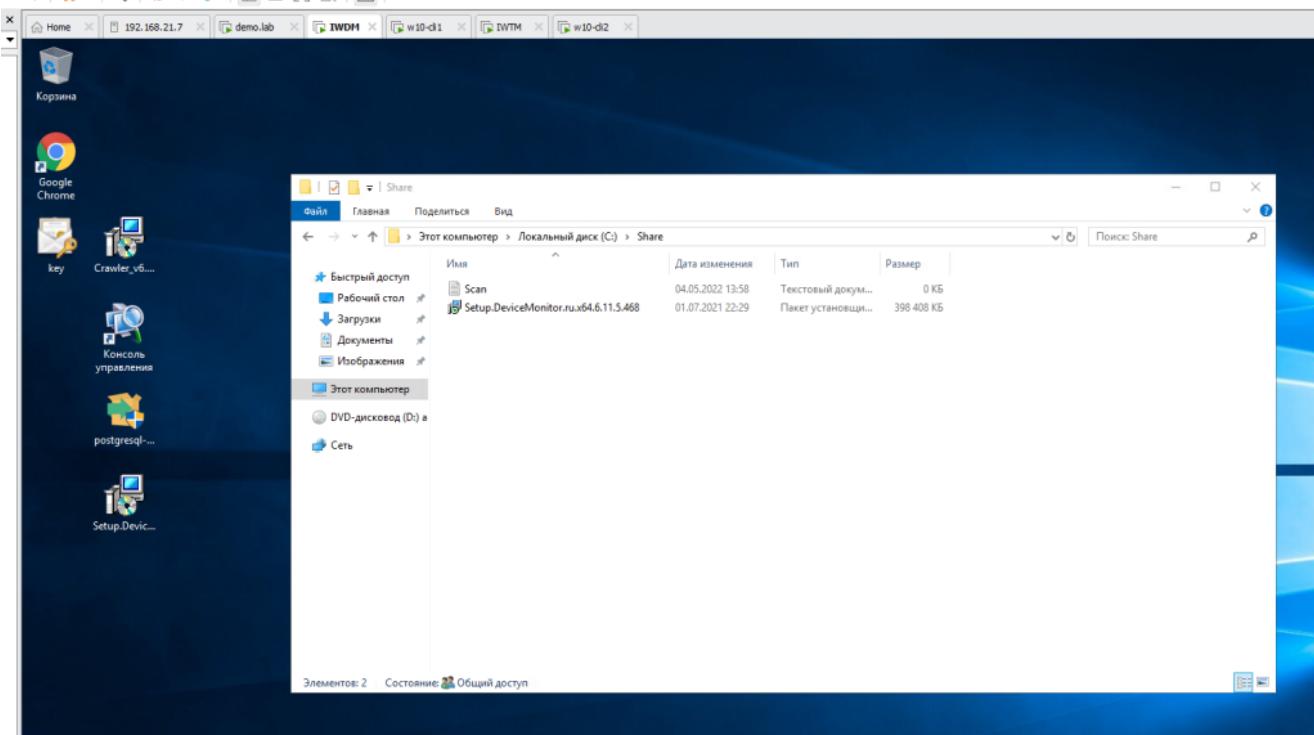
Сделать такой скрин!

По аналогии сделать вторую политику

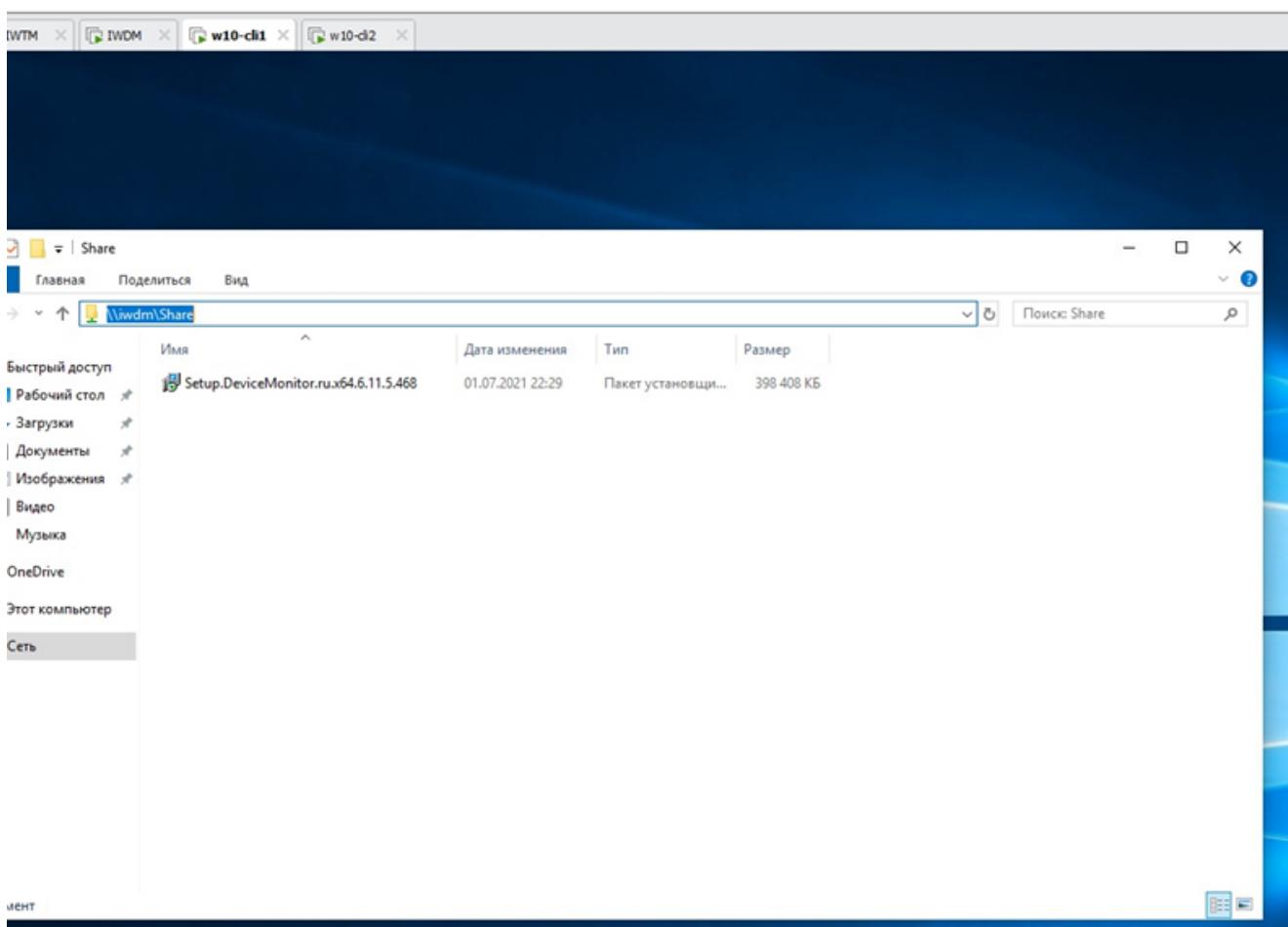
Задание 2

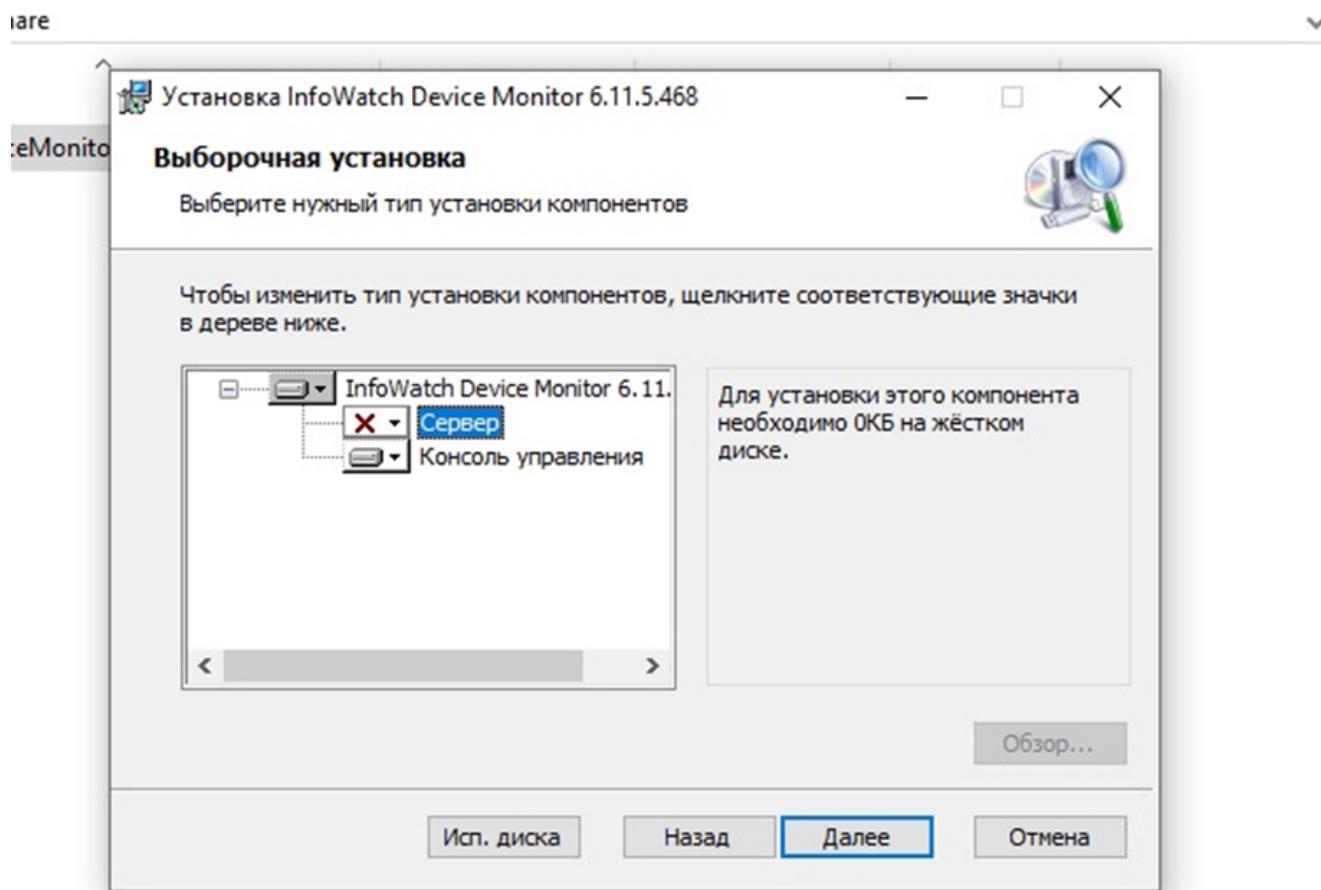
Для удобства работы офицера безопасности необходимо установить дополнительную консоль управления сервером агентского мониторинга на машину W10-agent1 для удаленного доступа к серверу агентского мониторинга.

Следующие правила создаются в политике «Отдел1».



Не копируем, а полностью переносим





В консоль управления использовать ip iwdm

Следующие правила создаются в политике «Отдел1».

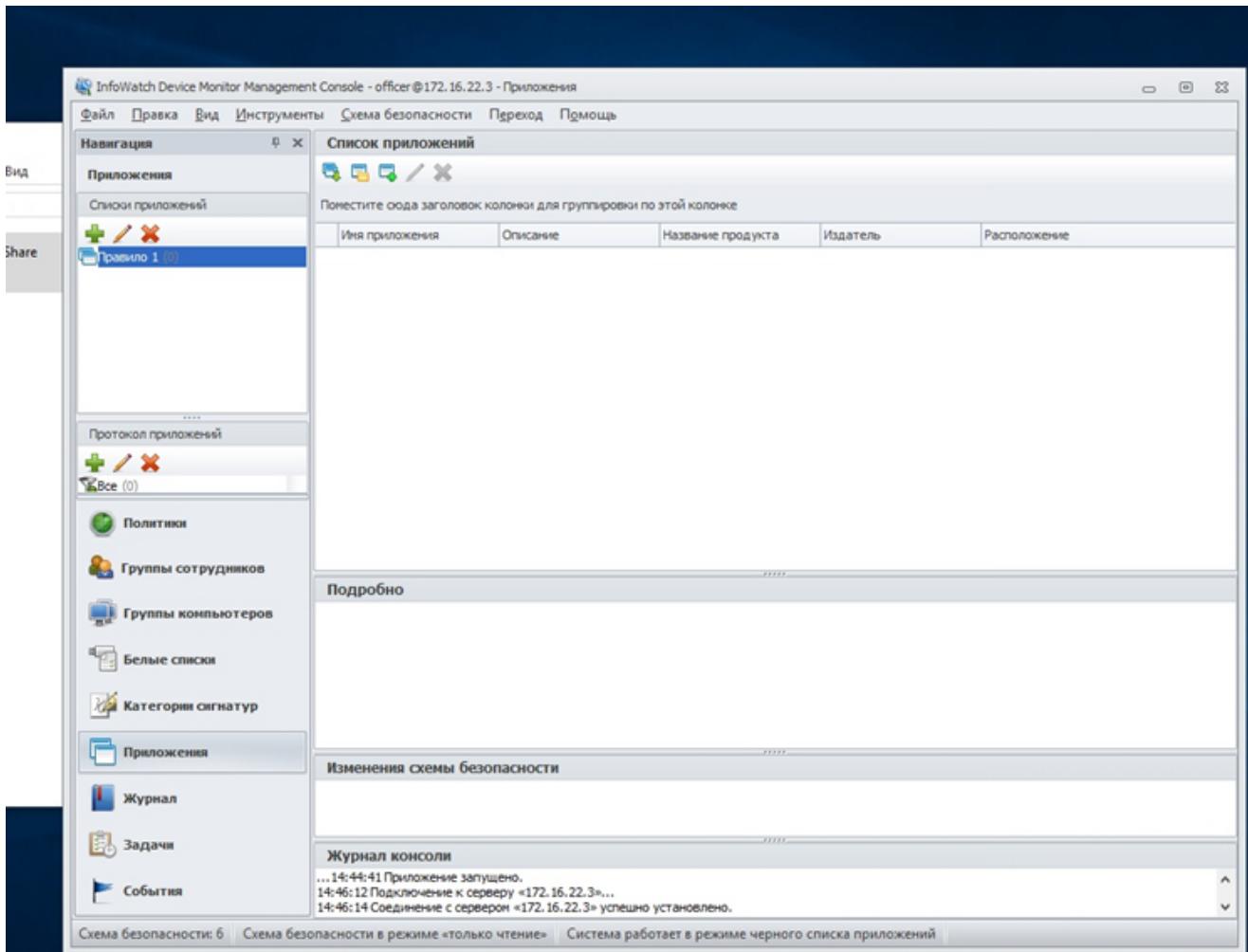
Правило 1

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

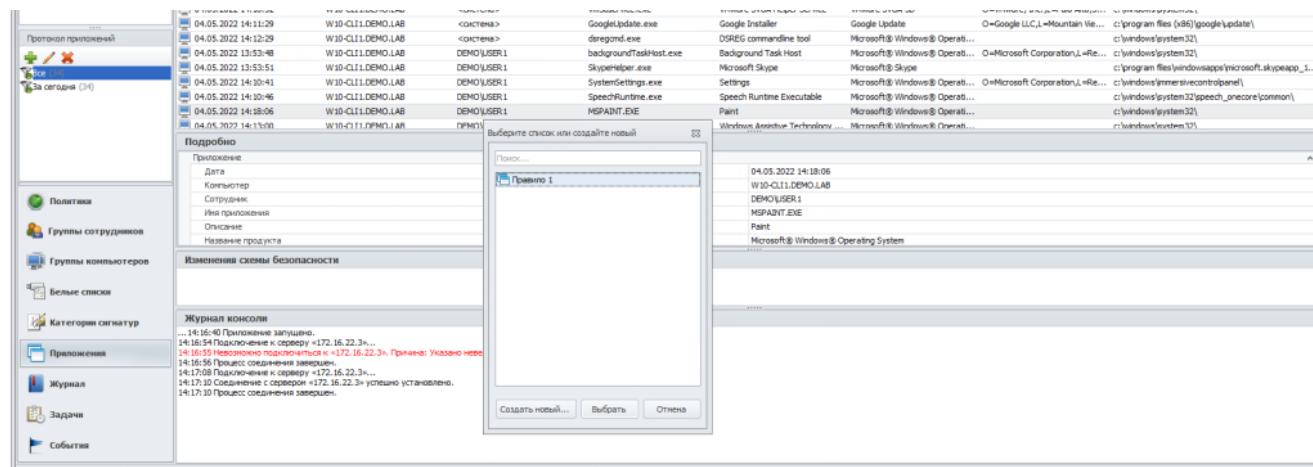
Проверить работоспособность и зафиксировать выполнение скриншотом.

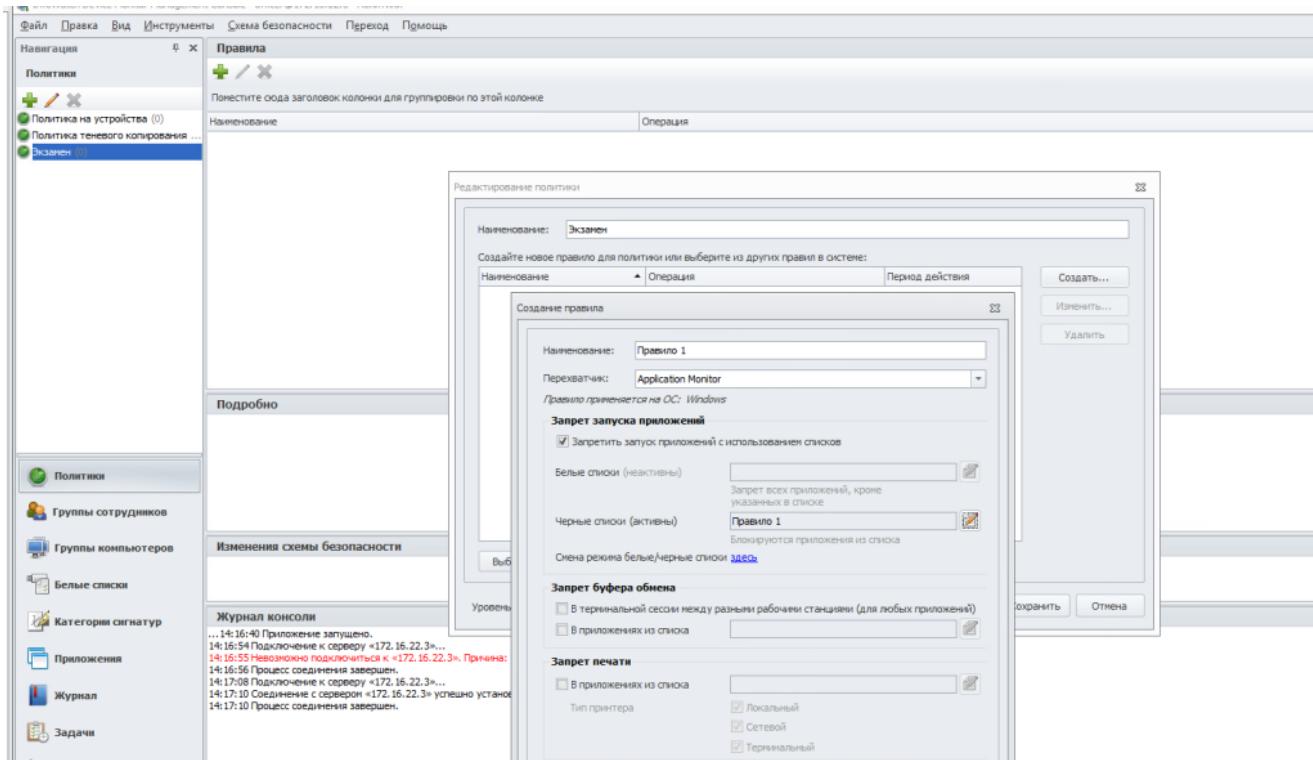
Ответ: Создание списков приложений. На каждое правило отдельный список желательно.

Лучше работать в консоли на клиенте.

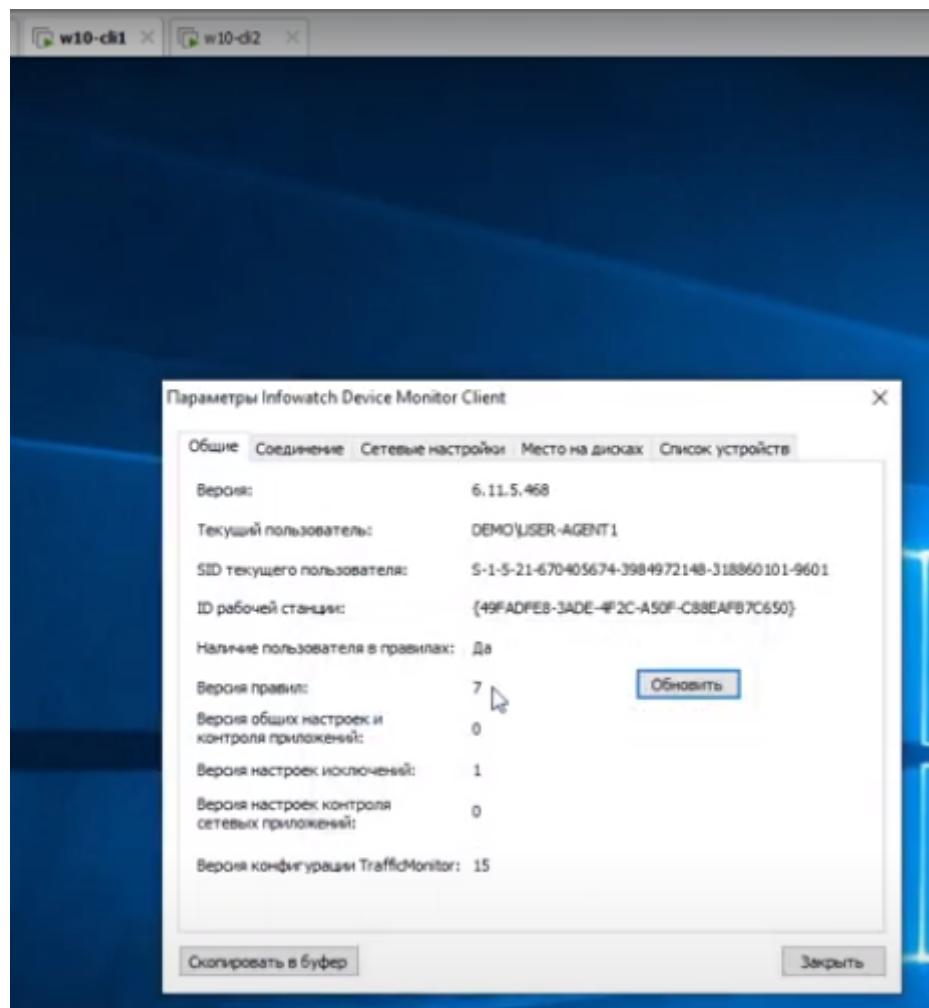


Для того, чтобы создать и настроить правило, вам необходимо вернуться к разделу «Политики» в Device Monitor Console и перейти к политики «Экзамен», после чего нажать кнопку «Создать правило...» (не путать с «создать политику...») обозначенную уже привычным зеленым плюсиком.





Сделать такой скрин



Проверка правила – обновить и попробовать запустить paint, после каждого правила обновлять

Правило 2

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

Перед этим также как и при создании первого правила требуется создать список (во вкладке приложения) и внести в него calc (excel отсутствует) — перед этим нужно запустить это приложения найдя его в поисковике windows

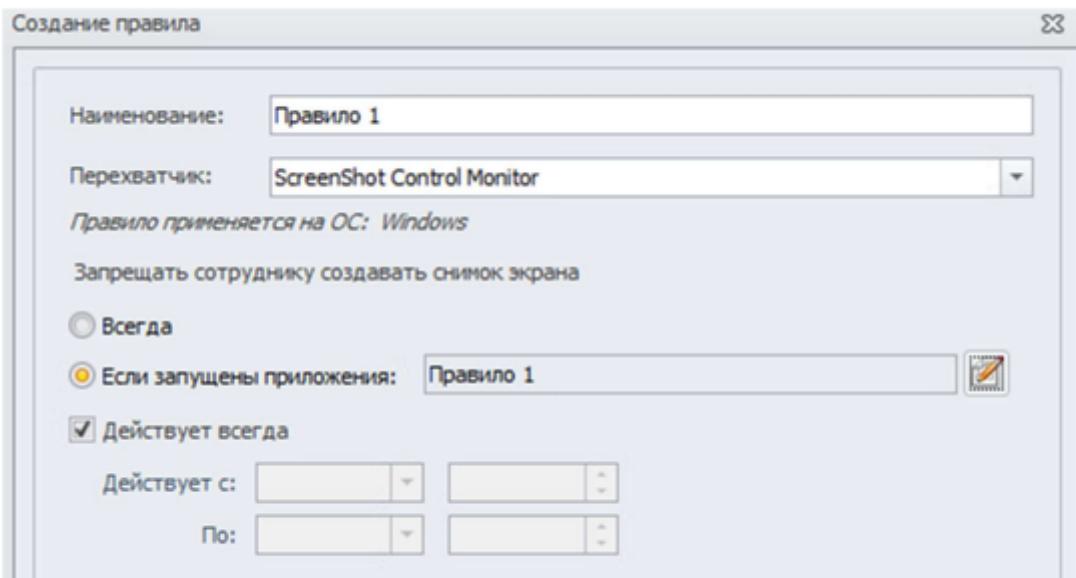
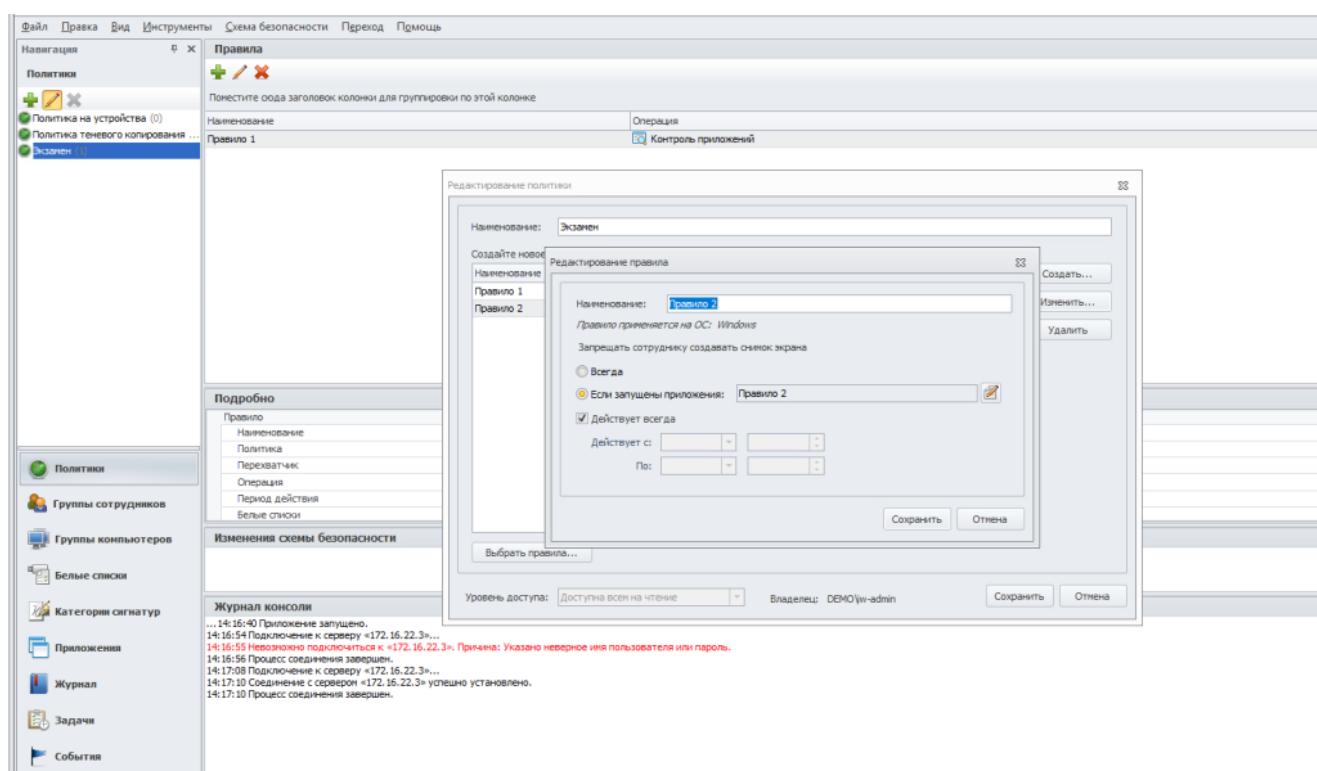


Рисунок 60 – «Правило 1»

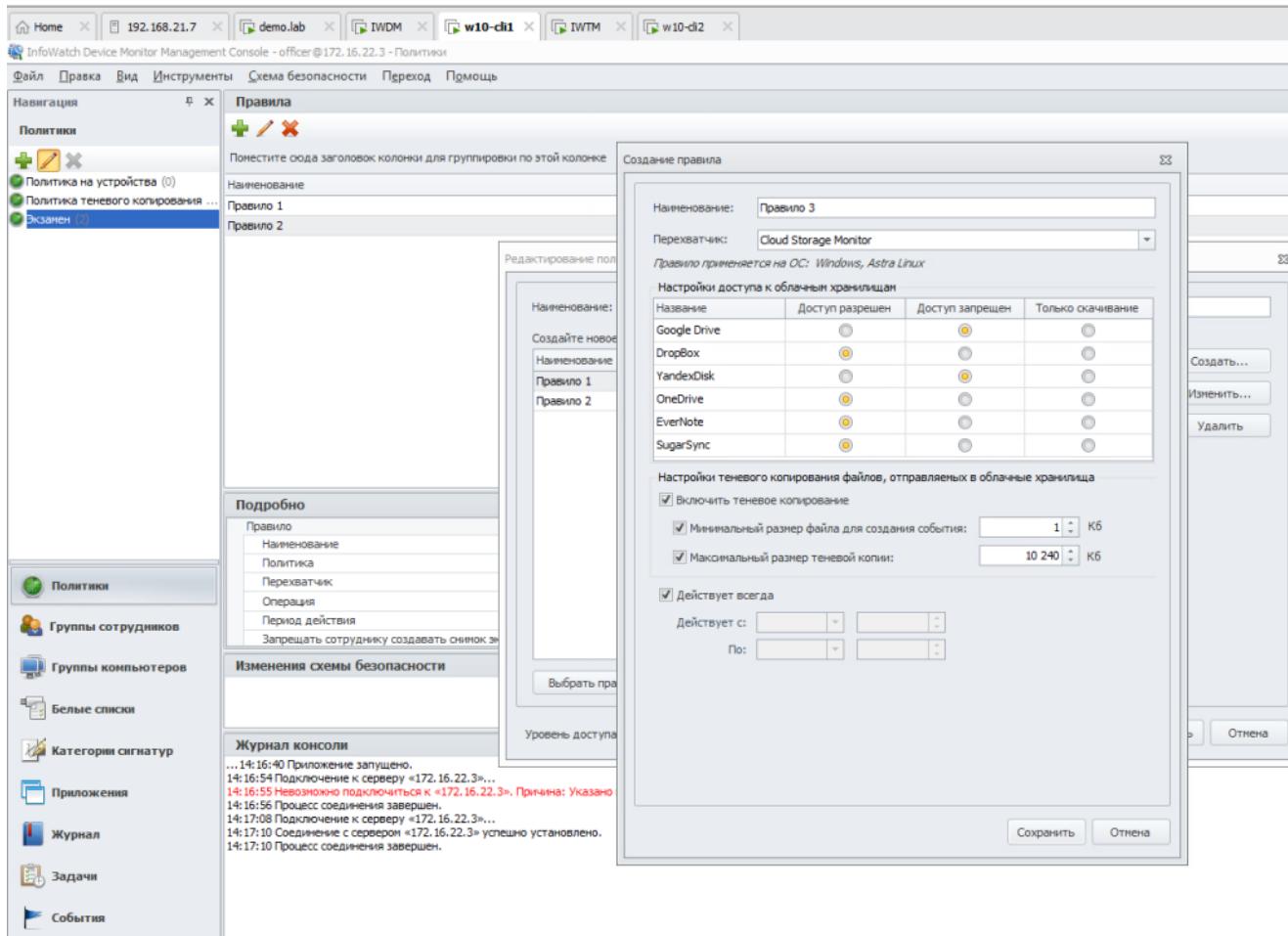


Сделать такой скрин

Правило 3

Ограничить доступ к облачным хранилищам GoogleDrive и YandexDisk.

Проверить работоспособность и зафиксировать выполнение



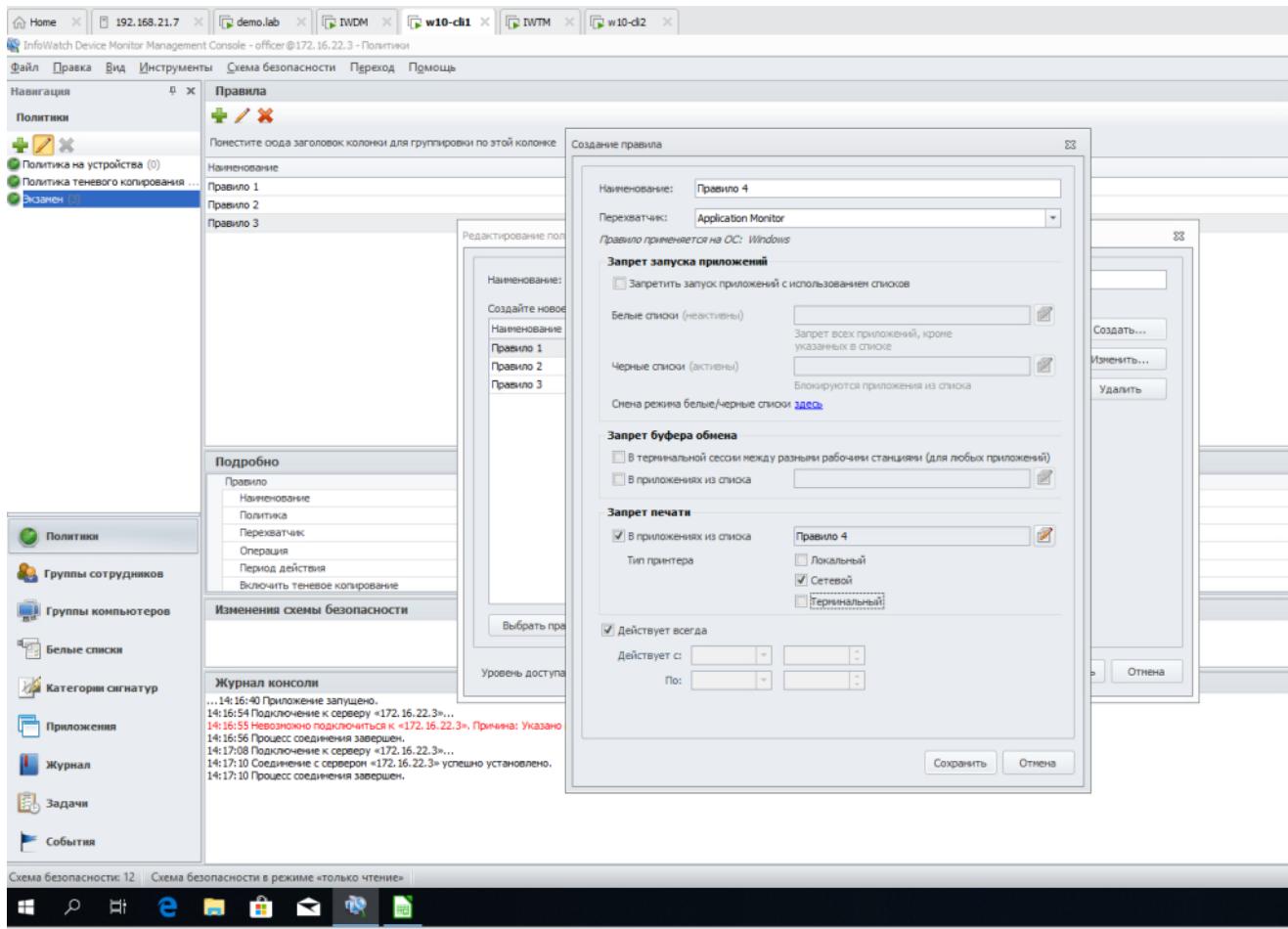
Здесь не создаем список, а сразу переходим в политику. **Сделать такой скрин**

Правило 4

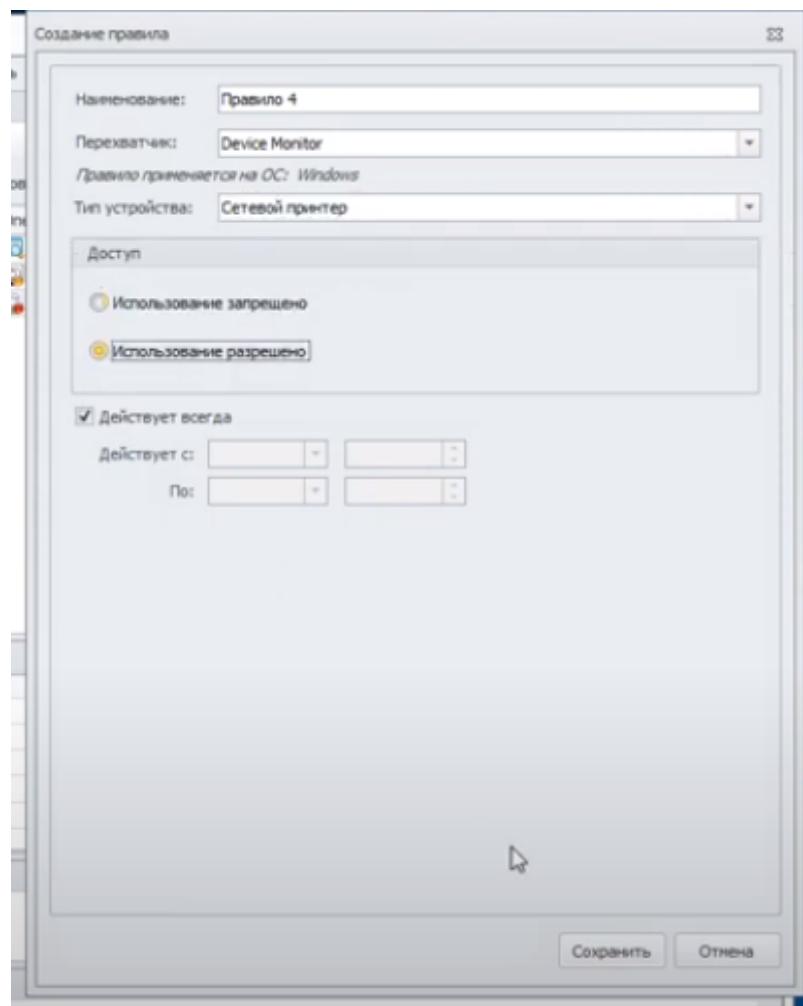
Необходимо запретить печать на сетевых принтерах.

Зафиксировать создание политики скриншотом.

Создаем список и добавляем в него все приложения есть



Сделать такой скрин

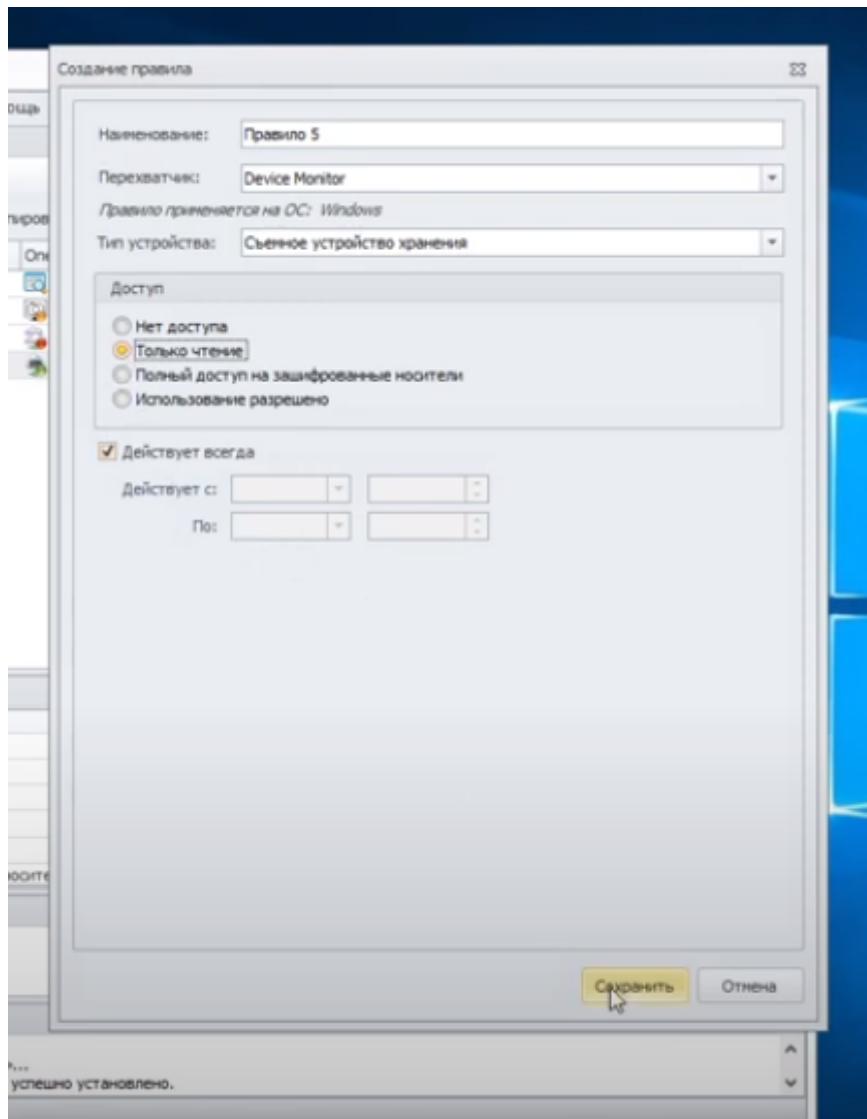


Или можно так

Правило 5

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

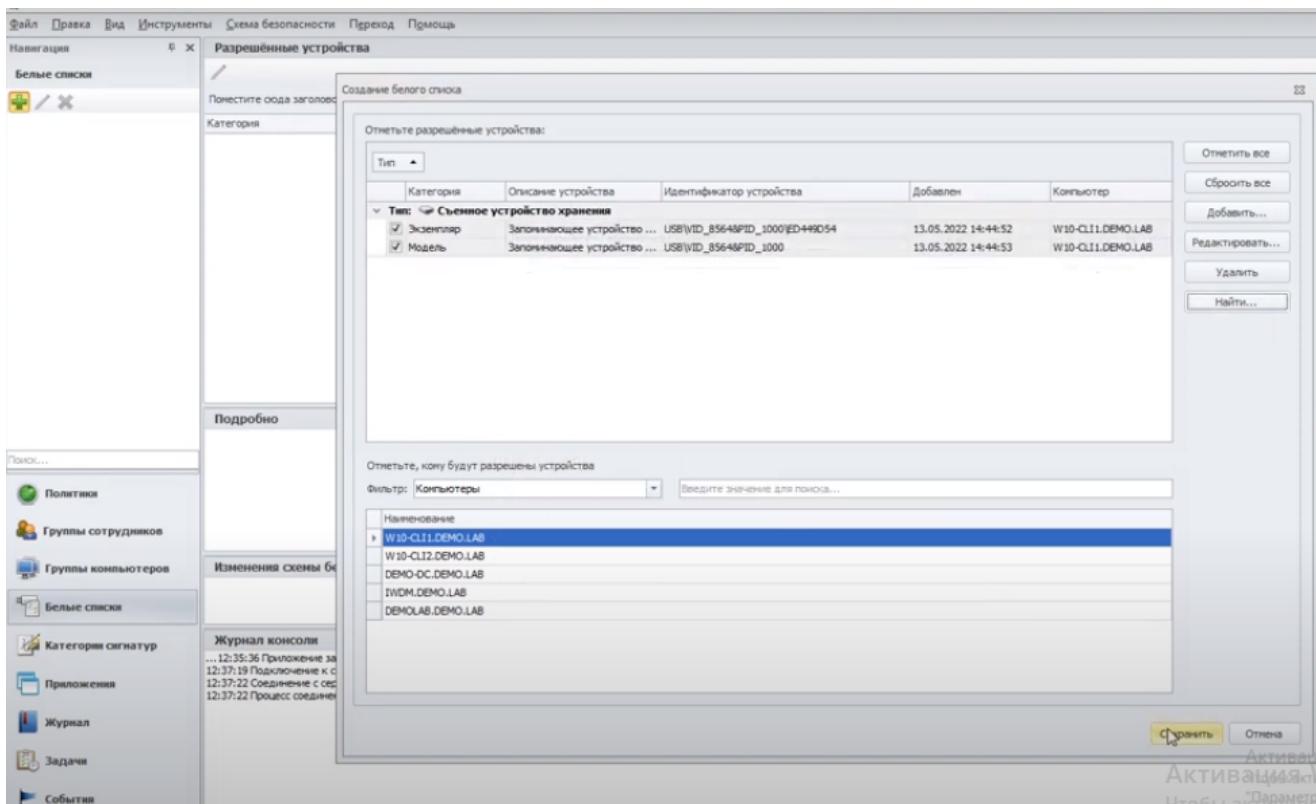
Проверить работоспособность и зафиксировать выполнение



Правило 6

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

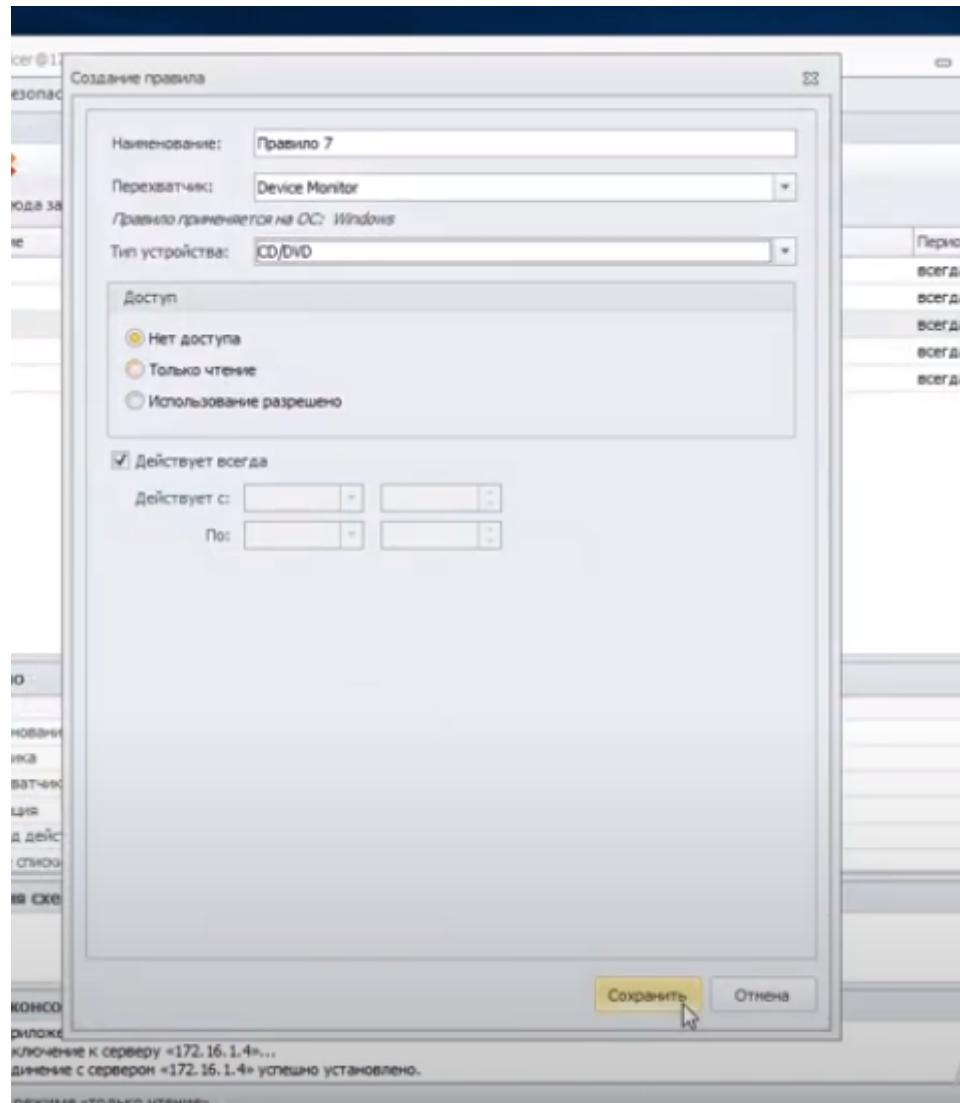
Проверить работоспособность и зафиксировать выполнение



Правило 7

Полностью запретить использование CD/DVD-дисковода.

Проверить работоспособность и зафиксировать выполнение

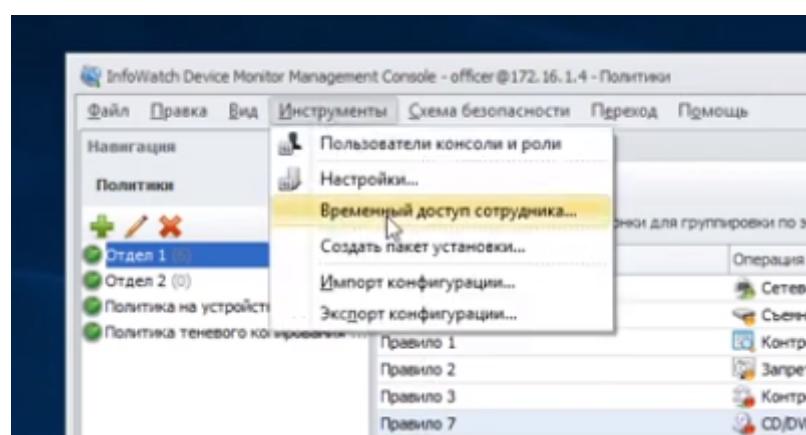


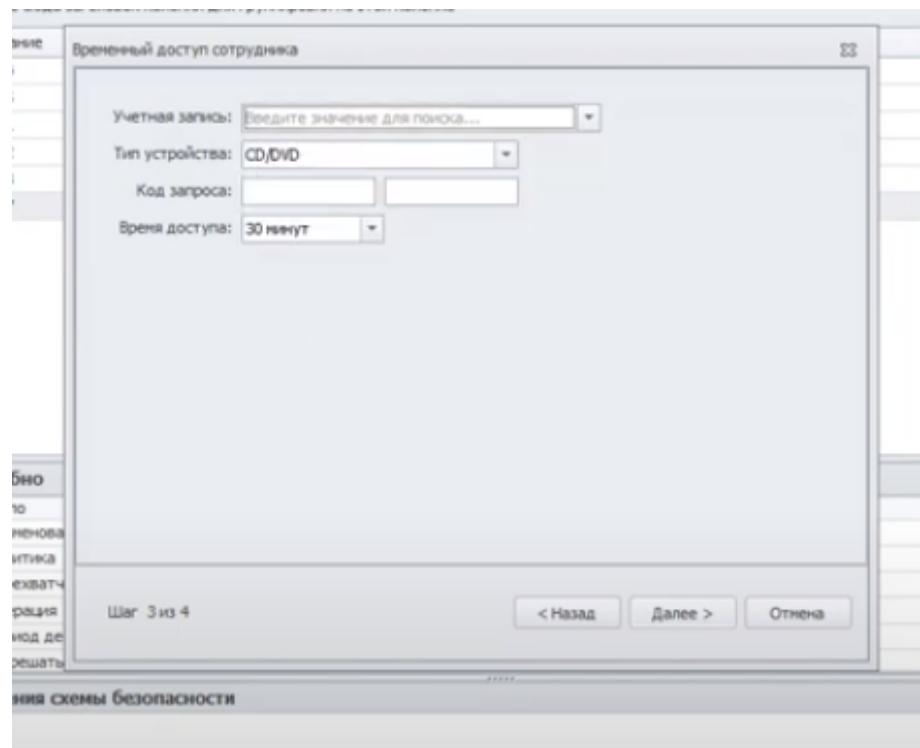
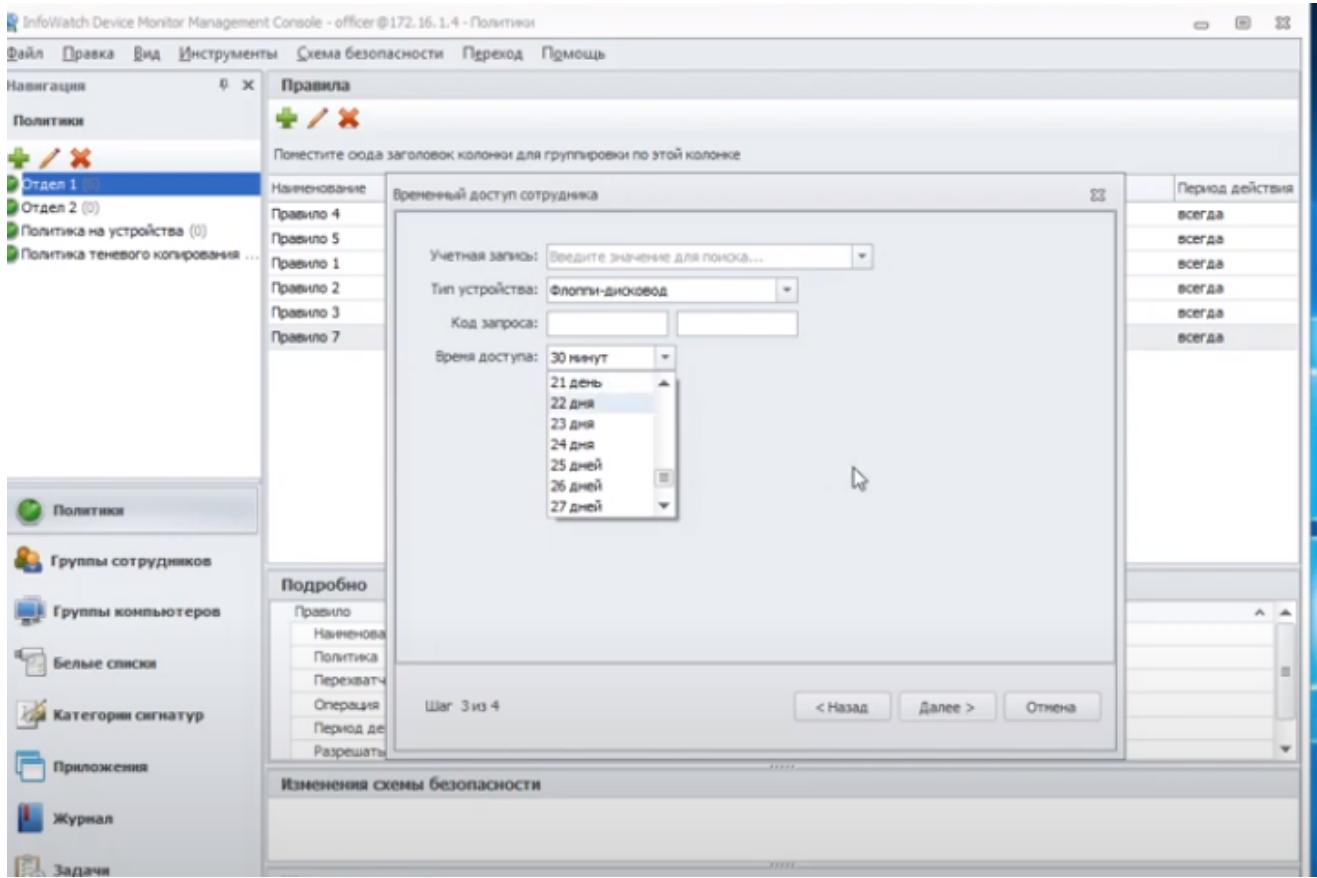
Правило 8

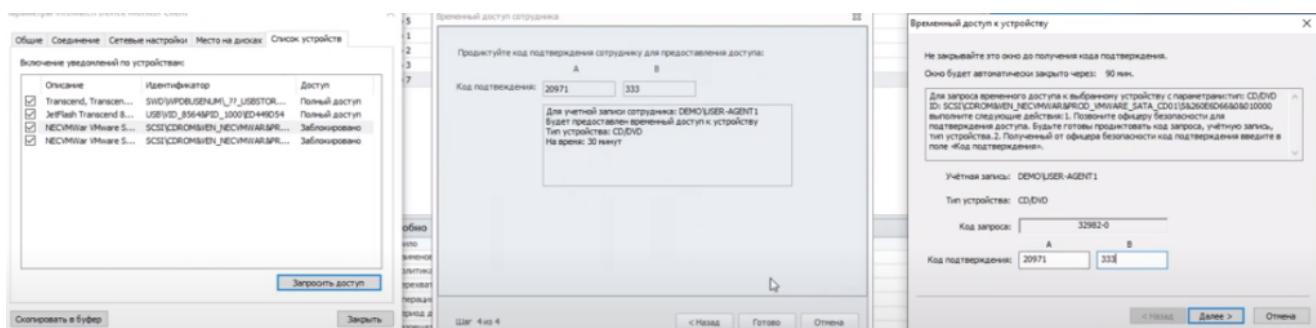
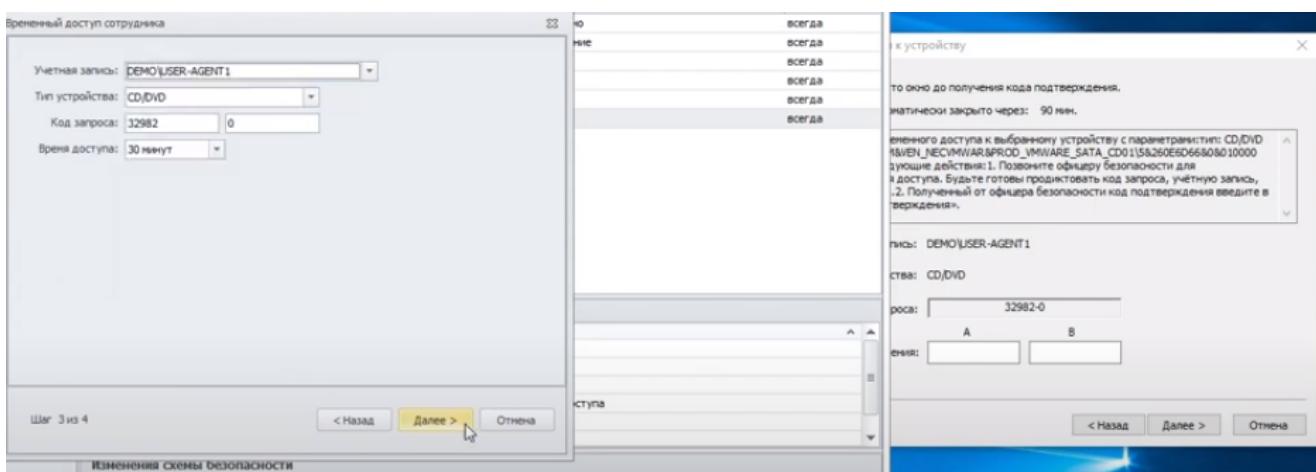
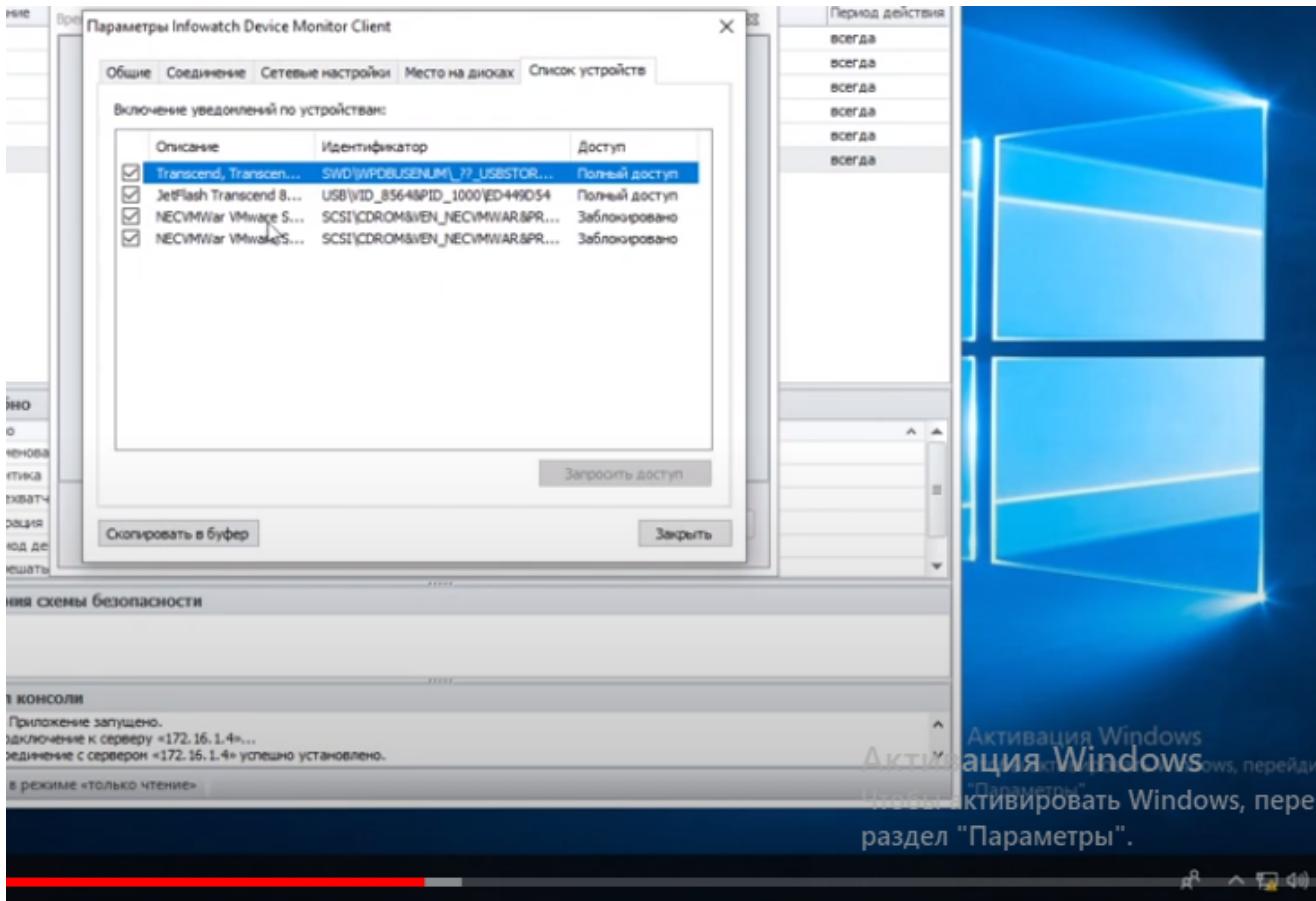
С учетом ранее выполненного запрета необходимо предоставить временный доступ для устройства на 7 минут для пользователя.

Зафиксировать этапы выдачи доступа и работоспособность скриншотами.

Следующие правила создаются в политике «Отдел2».





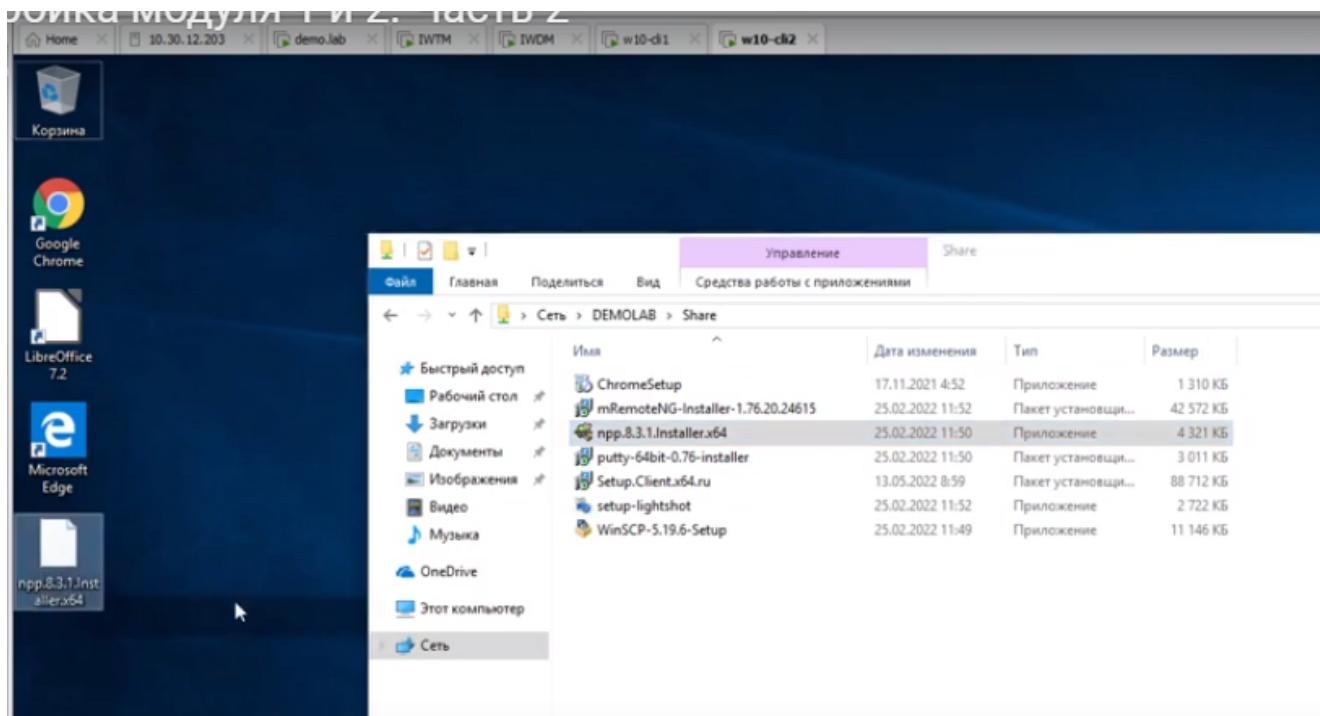


Правило 9

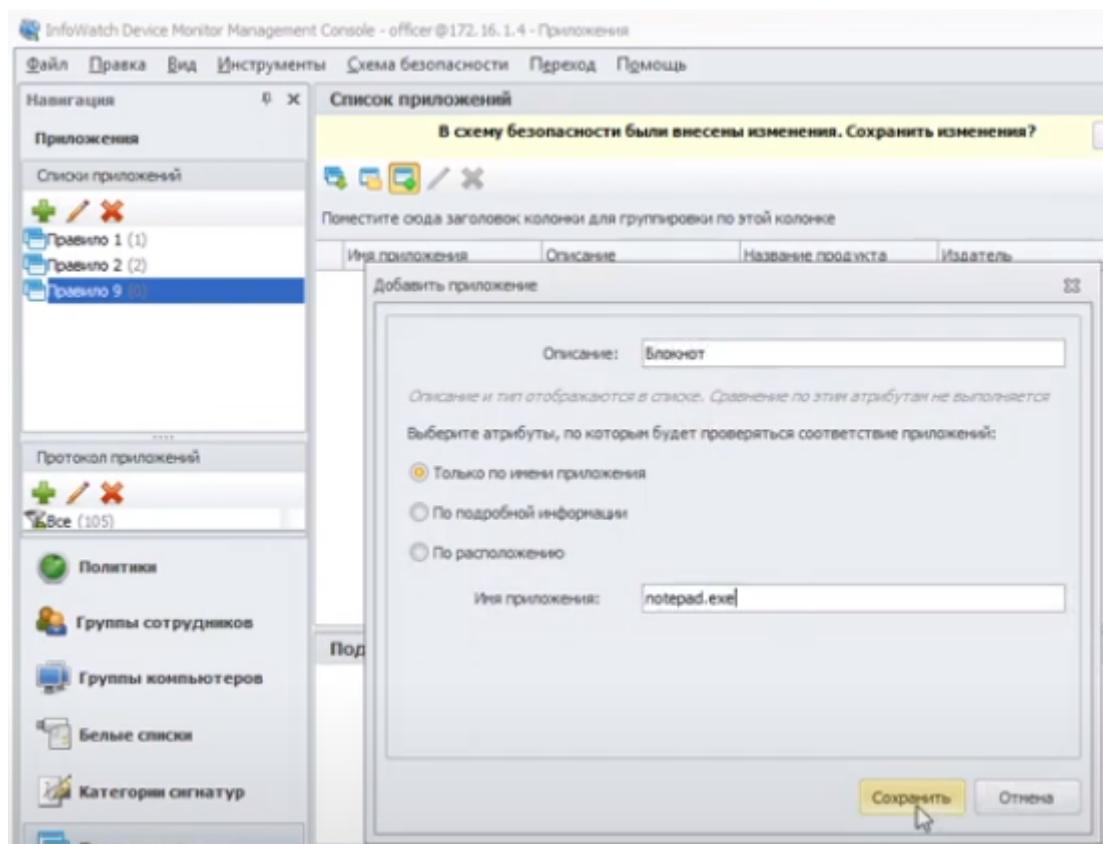
Необходимо поставить на контроль буфер обмена в блокноте и потерад++.

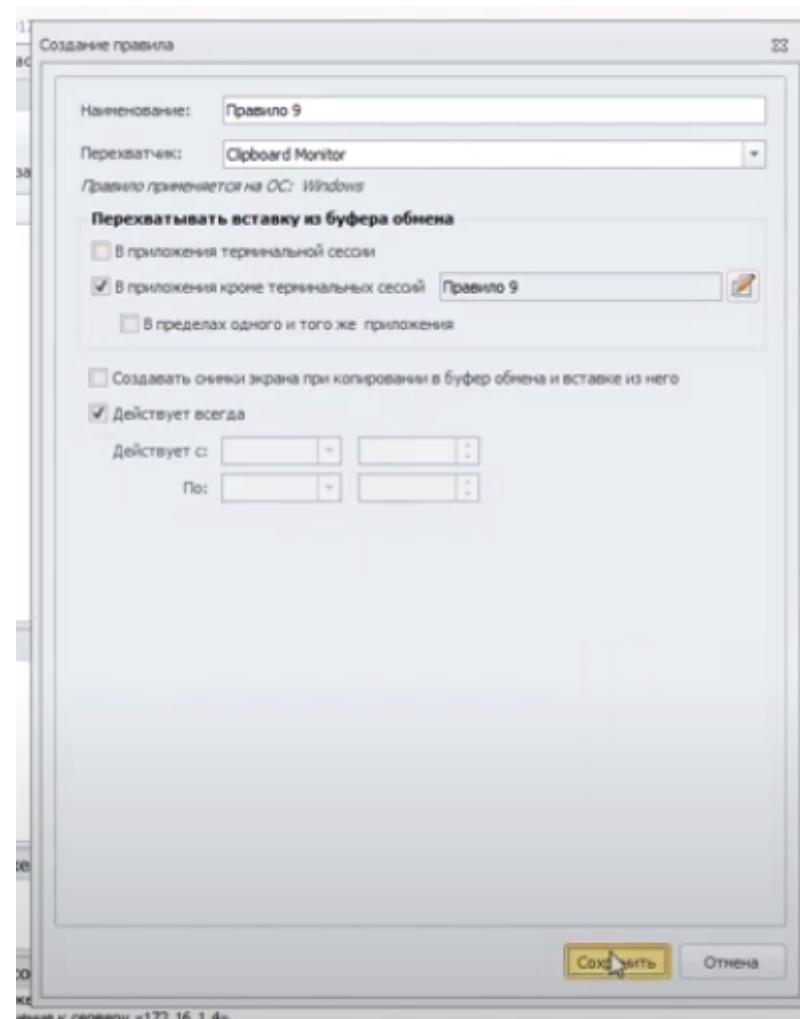
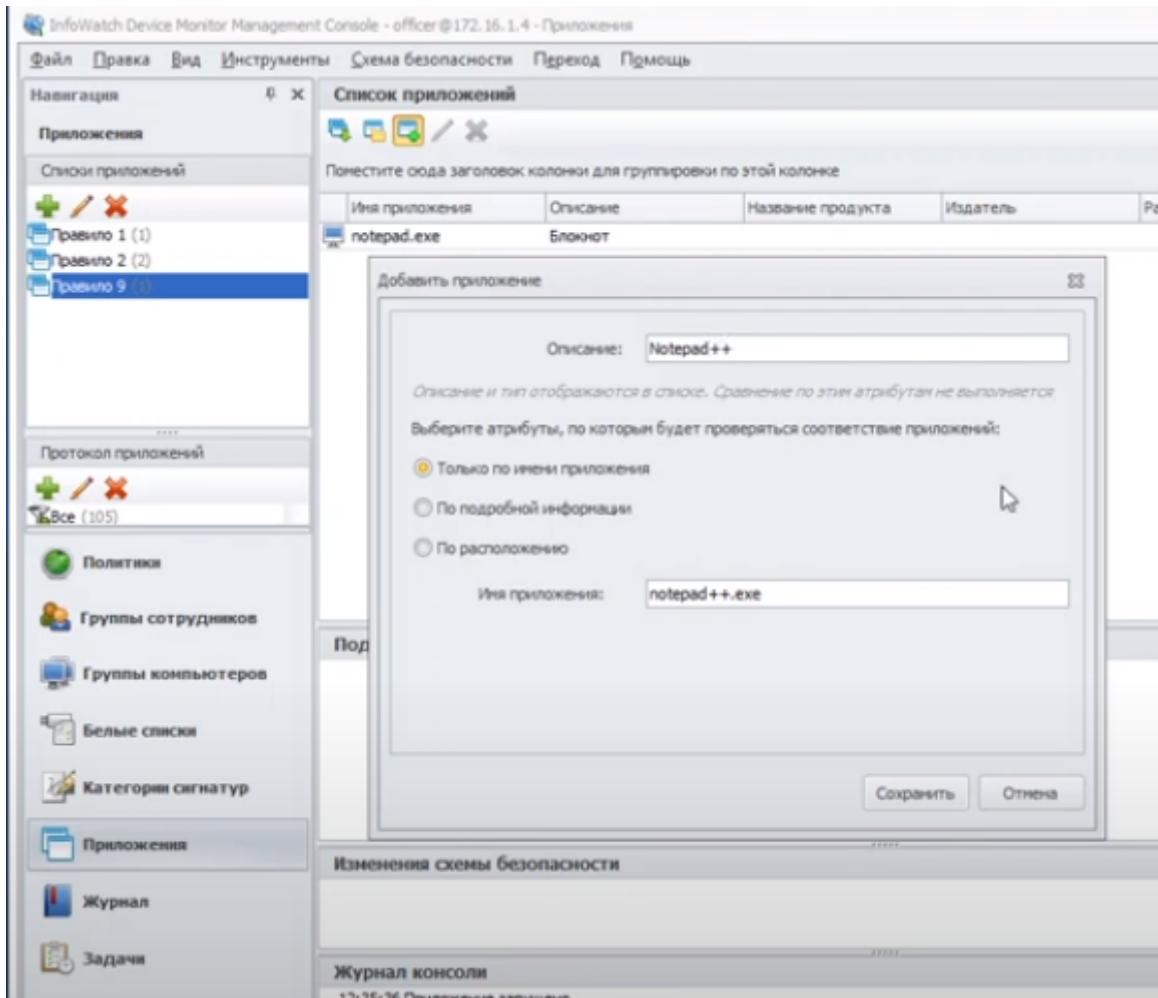
Проверить занесение нескольких событий в WEB-консоль.

Проверить работоспособность и зафиксировать выполнение скриншотом.



Установить если отсутствует



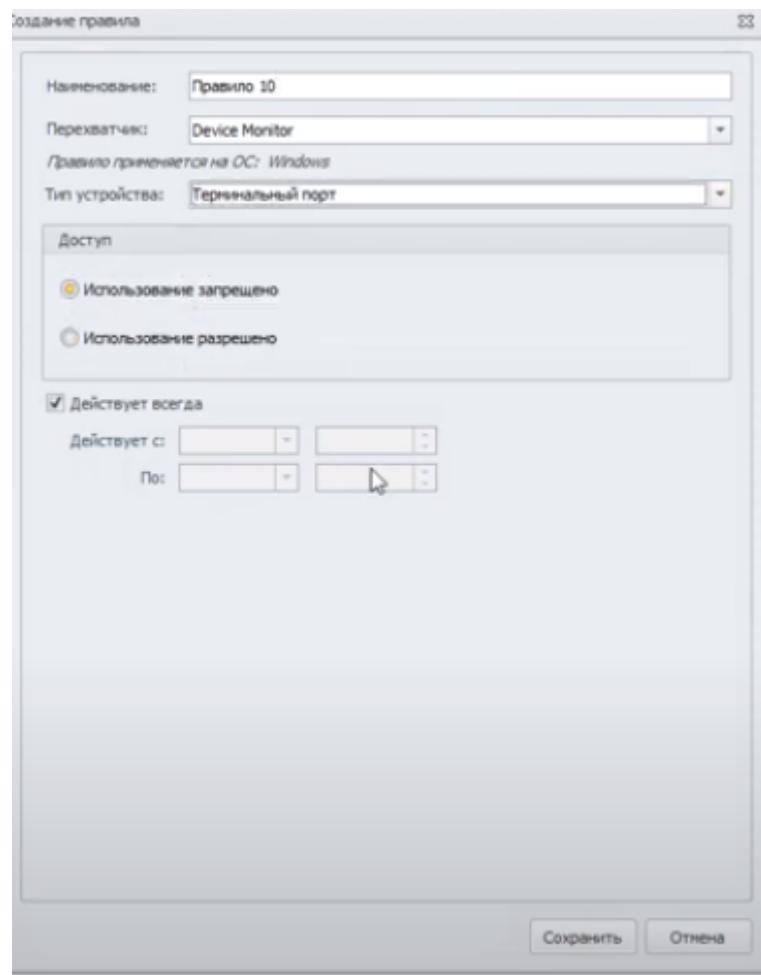


Поместите сюда заголовок колонки для группировки по этой колонке											
#	Шаг	Время	Объект	Действие	Селектор	Поле	Старое значение	Новое значение	Пользователь	Порядок	
38	1	13.05.2022 14:55:43	Правило	Добавление	34/Отдел 2/Правило 9	Действует с		01.01.1753 0:00:00	officer		
38	2	13.05.2022 14:55:43	Правило	Добавление	34/Отдел 2/Правило 9	Действует по		31.12.9999 23:59:59	officer		
38	3	13.05.2022 14:55:43	Правило	Добавление	34/Отдел 2/Правило 9	Операция		Контроль буфера обмена	officer		
37	1	13.05.2022 14:54:09	Приложение	Добавление	33/Правило 9/Notepad ++	Имя приложения		notepad++.exe	officer		
37	2	13.05.2022 14:54:09	Приложение	Добавление	33/Правило 9/Notepad ++	Описание		Notepad++	officer		
37	3	13.05.2022 14:54:09	Приложение	Добавление	33/Правило 9/Notepad ++	Название продукта		officer	officer		
37	4	13.05.2022 14:54:09	Приложение	Добавление	33/Правило 9/Notepad ++	Изобретатель		officer	officer		
37	5	13.05.2022 14:54:09	Приложение	Добавление	33/Правило 9/Notepad ++	Расположение		officer	officer		
37	6	13.05.2022 14:54:09	Приложение	Добавление	33/Правило 9/Notepad ++	Проверка соответствия		Только по имени прилож...	officer		
36	1	13.05.2022 14:53:34	Опрос приложений	Добавление	32/Правило 9	Наименование		Правило 9	officer		
36	2	13.05.2022 14:53:34	Приложение	Добавление	32/Правило 9/Блокнот	Имя приложения		notepad.exe	officer		
36	3	13.05.2022 14:53:34	Приложение	Добавление	32/Правило 9/Блокнот	Описание		Блокнот	officer		
36	4	13.05.2022 14:53:34	Приложение	Добавление	32/Правило 9/Блокнот	Название продукта		officer	officer		
36	5	13.05.2022 14:53:34	Приложение	Добавление	32/Правило 9/Блокнот	Издатель		officer	officer		
36	6	13.05.2022 14:53:34	Приложение	Добавление	32/Правило 9/Блокнот	Расположение		officer	officer		

Правило 10

Необходимо запретить использовать терминальные сессии для пользователя.

Проверить работоспособность и зафиксировать выполнение

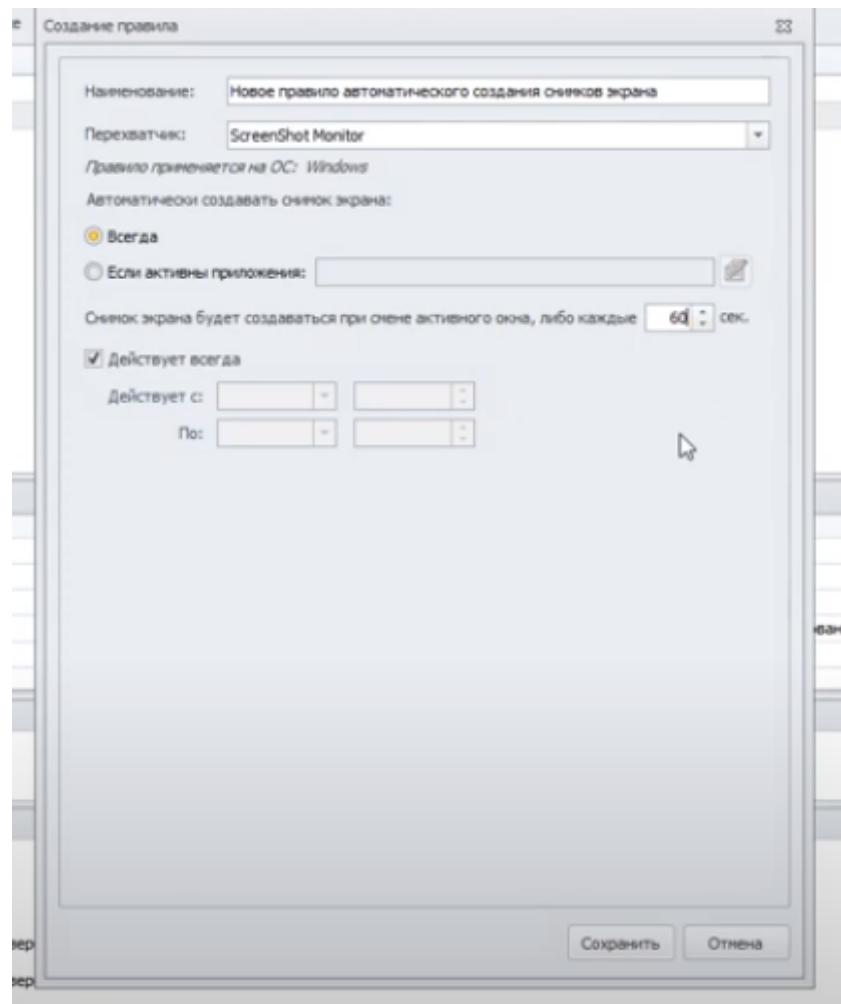


Правило 11

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

окна.

Проверить работоспособность и зафиксировать выполнение



Правило 12

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

Проверить работоспособность и зафиксировать выполнение

Создание правила

Наименование: Правило 12
Перехватчик: File Monitor
Правило применяется на ОС: Windows, Astra Linux

Условие срабатывания правила

Источник копирования
 Приемник копирования

Тип приемника: Сетевые ресурсы
Ресурсы: любые ресурсы

Маска файла: *.jpg, *.jpeg
 Категория файла: Графические данные
 Размер файла: 0 [+] MB [+] - [+] 2 [+] MB [+]

Действие при срабатывании правила

Разрешить копирование и не создавать события
 Разрешить копирование и создавать события без теневых копий
 Разрешить копирование и создавать события с теневыми копиями
 Запретить копирование и создавать события

Приоритеты правил с различными действиями

Действует всегда

Действует с: [] []
Пот: [] []

Сохранить Отмена

Сводка События Отчеты Технологии **Объекты защиты** Персоны Политики Списки Управление Краулер

21. Версия

Конфигурация свободна и доступна для редактирования

Управление тегами

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

+ / X

▲ Название

- VIP
- Задание б. Проверка работоспособности системы
- На рассмотрение

Создать тег

Название: Правило 12. DM запрет передачи файлов jpg
Цвет:

Описание:

Сохранить Отменить

The screenshot shows the 'Catalogs of protected objects' section. A modal dialog box titled 'Create' is open, prompting for a name ('Name') which is currently 'Правило 12 (DM) запрет передачи ipr'. The 'Status' toggle switch is turned on. The 'Description' field is empty. At the bottom are 'Create' and 'Cancel' buttons, with 'Create' being highlighted. In the background, the main interface lists categories like 'Finance', 'Management of the company', etc., and a table of objects with columns for name, description, creation date, and update date.

The screenshot shows the TMS software interface with the following elements:

- Top Navigation Bar:** Сводка, События, Отчеты, Технологии, Объекты защиты, Персоны, Политики, Списки, Управление, Краулер.
- Left Sidebar:** Категории (Categories). It includes a search bar ("Поиск по категориям") and a tree view of categories:
 - Все элементы (All elements):
 - Договоры и контракты
 - Задание 6. Проверка работоспособности
 - Конкурсная документация
 - Маркетинг
 - Отдел кадров
 - Система безопасности
 - Управление компаниями
 - Финансы
- Center Content:** Конфигурация свободна и доступна для редактирования.
- Right Dialog Box:** Создать (Create) - Правило 12 (DM) запрет передачи jpg.
 - Название категории: Правило 12 (DM) запрет передачи jpg
 - Параметры терминов, входящих в категорию:
 - Вес: 5
 - Язык: Русский
 - Учитывать морфологию:
 - Учитывать регистр:
 - Описание: Добавить описание

The screenshot shows a software application with a dark-themed interface. At the top, there is a navigation bar with items: Сводка, События, Отчеты, Технологии, Объекты защиты, Персоны, Политики, Списки, Управление, and Краулер. Below the navigation bar, a message says "Вы редактируете конфигурацию". On the left side, there is a sidebar titled "Категории" with a search bar "Поиск по категориям" and a list of categories: Все элементы, Договоры и контракты, Задание б. Проверка работоспособ..., Конкурсная документация, Маркетинг, Отдел кадров, Правило 12 (DM) запрет передачи j..., Система безопасности, Управление компаниями, and Финансы. The "Правило 12 (DM) запрет передачи j..." item is currently selected. In the center, there is a modal window titled "Создание термина". Inside the modal, there are fields for "Текст термина" (set to "jpeg"), a toggle switch for "Характеристический" which is turned on, a dropdown for "Вес" set to "5", a dropdown for "Язык" set to "Русский", and two toggle switches: "Учитывать морфологию" (turned on) and "Учитывать регистр" (turned off). At the bottom of the modal are two buttons: "Создать" (Create) and "Отменить" (Cancel), with a cursor pointing at the "Создать" button.

Вы редактируете конфигурацию - Правило 12 (DM) запрет передачи jpg

Создание термина

Текст термина: jpg

Характеристический:

Вес: 5

Язык: Русский

Учитывать морфологию:

Учитывать регистр:

Создать **Отменить**

Вы редактируете конфигурацию с 13.05.2022 15:29. | Применить | Сохранить | Сбросить | Версия действующей конфигурации - № 18.

Политики

Политики защиты данных:

- Политика защиты данных #1
 - Политика на любые данные
 - Передача Копирование Хранение Работа в приложениях
- Политика защиты данных
 - Каталог объектов защиты: Задание 6. Проверка работоспособности системы
 - Передача 1 Копирование 1 Хранение 1 Работа в приложениях 1

Добавить политику **Фильтр**

Правила защиты данных #1 **Добавить правило**

Название: Правило 12 (DM) запрет передачи jpg

Период действия: Всё время

Статус:

Защищаемые данные

Выбрать

Политика срабатывает при обнаружении хотя бы одного прохождения в каждый из типов данных

Каталоги объектов защиты: Правило 12 (DM) запрет передачи jpg

Файловые форматы: Изображение JPEG

Описание: Введите описание

Создан: 13.05.2022 15:29 | Изменен: 13.05.2022 15:29

Активация Windows

Вы редактируете конфигурацию с 13.05.2022 15:29. | Применить | Сохранить | Сбросить | Версия действующей конфигурации - № 18.

Политики

Политики защиты данных:

- Правило 12 (DM) запрет передачи jpg
 - 2 объектов из 2 типов. Каталог объектов защиты: Правило 12 ... jpg. Файловый формат: Изображение JPEG. Смотреть все
 - Передача Копирование Хранение Работа в приложениях
- Политика защиты данных
 - Каталог объектов защиты: Задание 6. Проверка работоспособности системы

Добавить правило

Направление маршрута: В одну сторону В оба направления

Тип события: Веб-сообщение, Facebook, ICO, Mail.Ru Агент, MS Lync, Skype, Telegram, XMPP, ВКонтакте, Почта в Браузере, Почта на Клиенте

Компьютеры: W10-CL12

Отправители: Начните вводить текст

Получатели: Начните вводить текст

Дни действия правила: Любой день недели

Часы действия правила: 0:00 - 0:00

Правило передачи

Действия при срабатывании правила

Отправить почтовое уведомление: Начните вводить текст

Политики защиты данных:

● Правило 12 (DM) запрет передачи jpg
2 объектов из 2 типов. Каталог объектов защиты: Правило 12 ... jpg. Файловый формат: Изображение JPEG. Смотреть все

Передача Копирование Хранение Работа в приложениях

Добавить правило

Тип события Facebook, ICQ, MS Lync, Mail.Ru Агент, Skype, Telegram, XMPP, ВКонтакте, Веб-сообщение, Почта в браузере, Почта на клиенте

Отправители Любой отправитель

Направление маршрута Любой получатель

Получатели W10-CL12

Компьютер не заданы

Действия не заданы

Действия по умолчанию не заданы

● Политика защиты данных
Каталог объектов защиты: Задание 6. Проверка работоспособности системы

Передача 1 Копирование 1 Хранение 1 Работа в приложениях 1

Компьютеры W10-CL12

Отправители Начните вводить текст

Получатели Начните вводить текст

Дни действия правила Любой день недели

Часы действия правила 0:00 - 0:00

Действия при срабатывании правила

Отправить почтовое уведомление Начните вводить текст

Назначить событию вердикт Заблокировать

Назначить событию уровень нарушения Высокий

Назначить событию тип Правило 12: DM запрет передачи файлов jpg

Назначить отправителю статус Выберите статус

Удалить событие Активация Windows

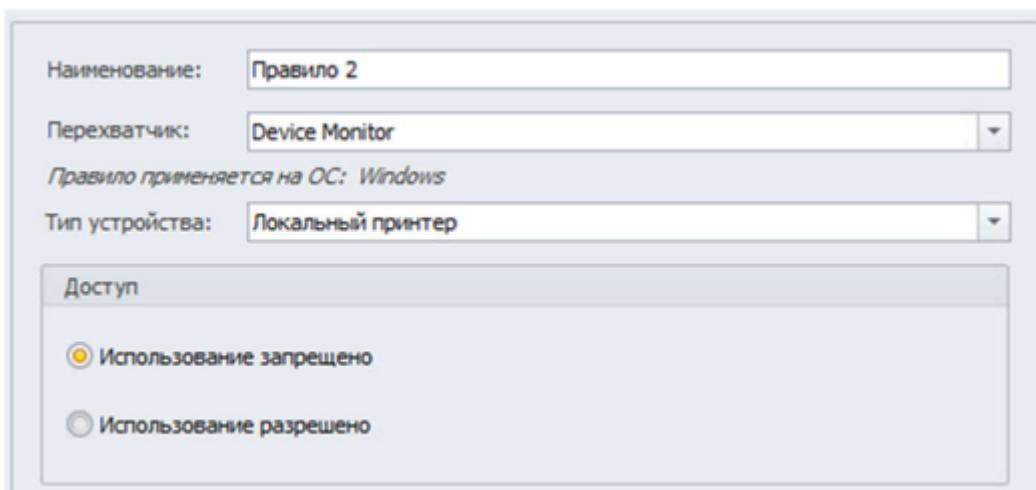
Чтобы активировать Windows, перейдите в раздел "Диспетчер" и выберите "Активировать Windows, перейдите в

Сохранить **Отменить**

Правила доп

Необходимо запретить печать на локальных принтерах, но при этом оставить возможность печати на сетевых принтерах.

Зафиксировать создание политики скриншотом



Создать политику по блокировке копирования исполняемых exe-файлов на USBнакопители. Проверить работоспособность и зафиксировать выполнение (зафиксировать результаты в виде скриншотов).

Проверить работоспособность и зафиксировать выполнение скриншотом.

Наименование: Правило 3

Перехватчик: File Monitor

Правило применяется на ОС: Windows, Astra Linux

Условие срабатывания правила

Источник копирования
 Приемник копирования

Тип приемника: Съемные устройства

Ресурсы [2](#)

Маска файла: *.exe

Категория файла: Исполняемые файлы

Размер файла: 0 [+] [Мб] - [+] [Мб]

Действие при срабатывании правила

Разрешить копирование и не создавать события
 Разрешить копирование и создавать события без теневых копий
 Разрешить копирование и создавать события с теневыми копиями
 Запретить копирование и создавать события

В связи с небезопасностью ftp-серверов разрешить только скачивание по протоколу ftp, загрузку файлов на сервер запретить.

Проверить работоспособность на любом доступном файловом сервере и зафиксировать выполнение скриншотом.

Наименование: Правило 4

Перехватчик: FTP Monitor

Правило применяется на ОС: Windows

Условия срабатывания правила

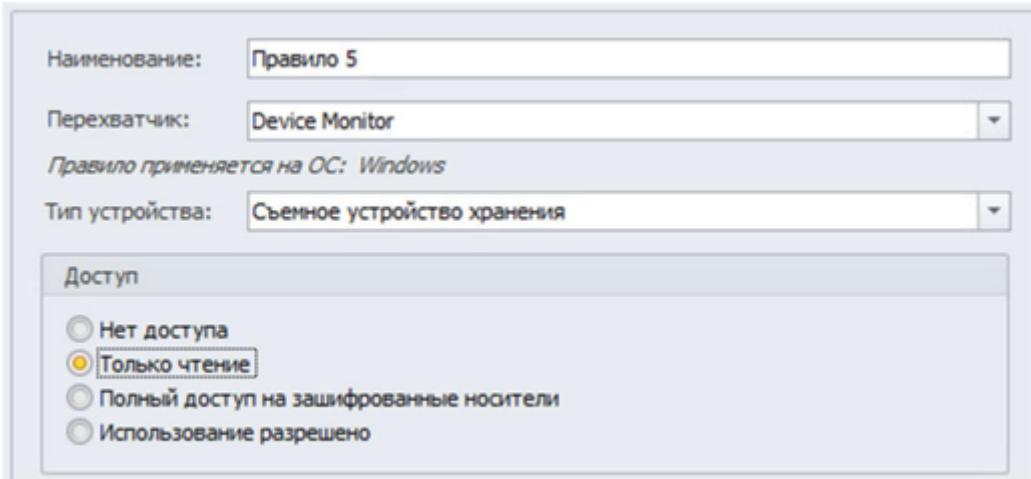
FTP адреса [2](#): любые ресурсы

Размер файла: 0 [+] [Кб] - [+] [Кб]

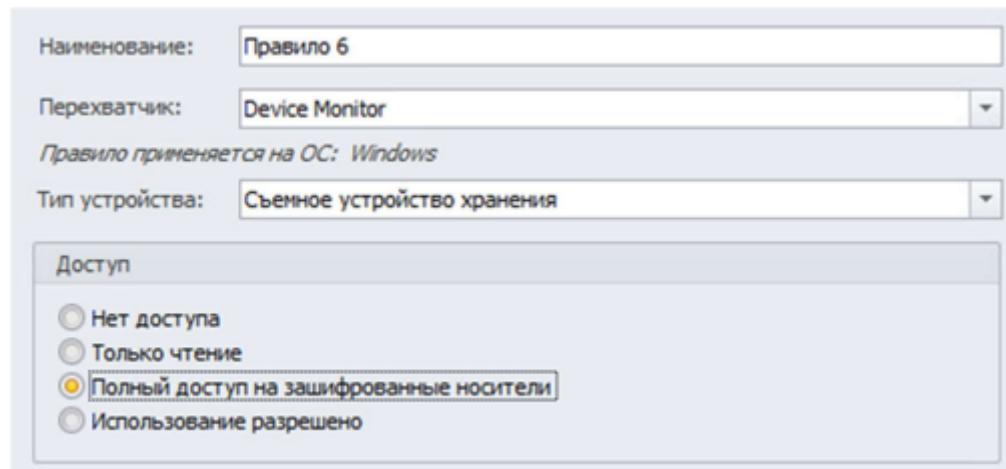
Действие при срабатывании правила

Разрешить скачивать и записывать на FTP. Не создавать события
 Разрешить скачивать и записывать на FTP. Создавать события с теневыми копиями для случаев записи
 Разрешить скачивать и записывать на FTP. Создавать события без теневых копий для случаев записи
 Разрешить скачивать из FTP. Запретить записывать на FTP.
 Не создавать события
 Запретить вход на FTP адреса

Необходимо запретить запись файлов на все съемные носители информации (флешки), оставив возможность чтения и копирования с них.
Проверить работоспособность и зафиксировать выполнение скриншотом.



С учетом ранее созданной политики необходимо разрешить запись файлов на доверенный носитель. Запрет на запись на остальные носители оставить в силе.
Проверить работоспособность и зафиксировать настройку и выполнение скриншотами



На виртуальной машине необходимо запретить использование буфера обмена при подключении к удаленным машинам по протоколу RDP, а в группе компьютеров по умолчанию необходимо контролировать буфер обмена при копировании из/в терминальных сессий.
Проверить работоспособность попыткой копирования текста из сеанса RDP

и зафиксировать выполнение скриншотом как блокировки, так и контроля.
Для работы RDP может потребоваться дополнительная настройка.

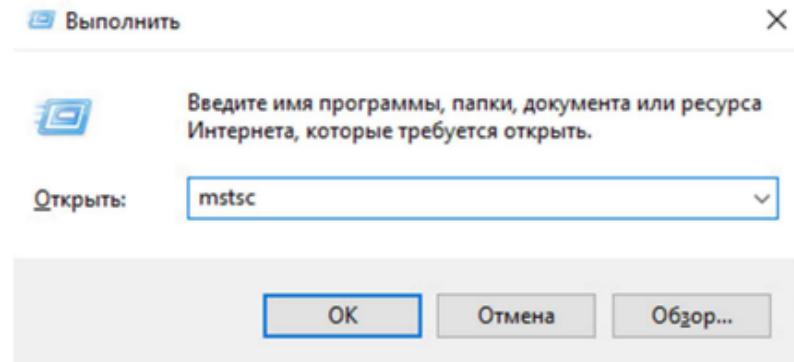
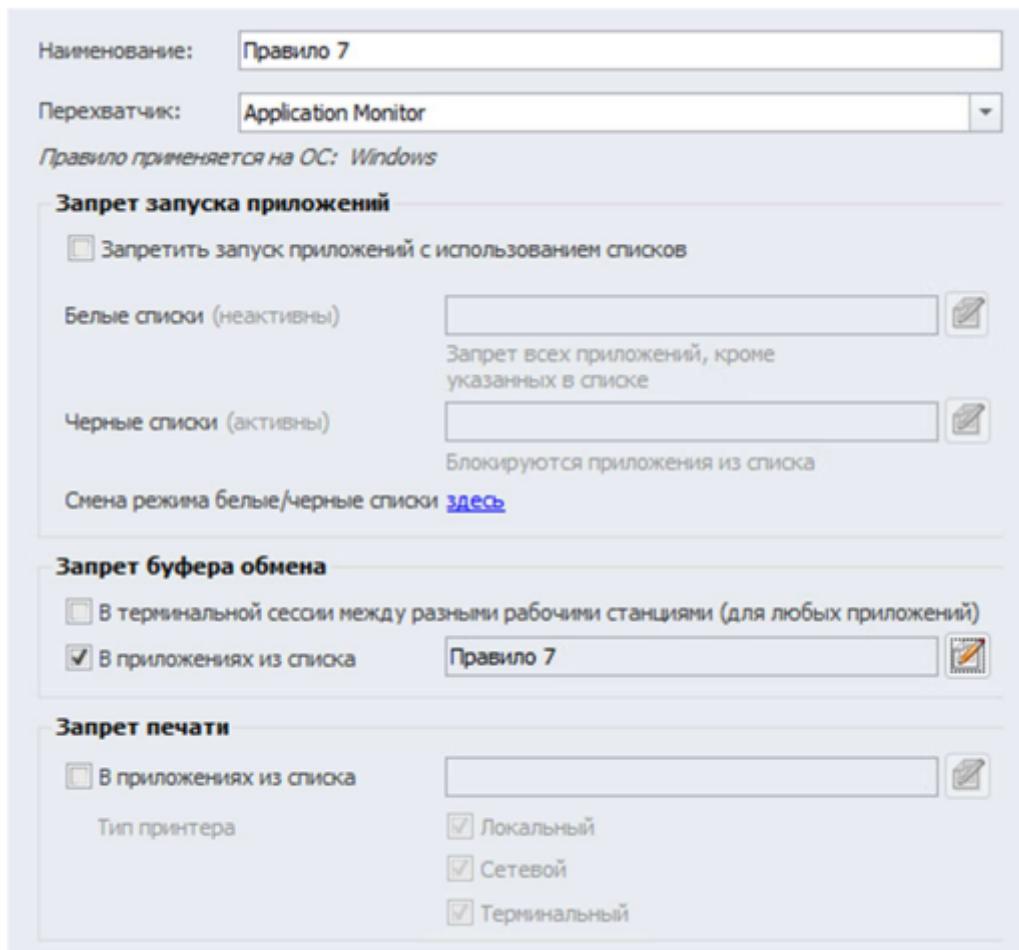
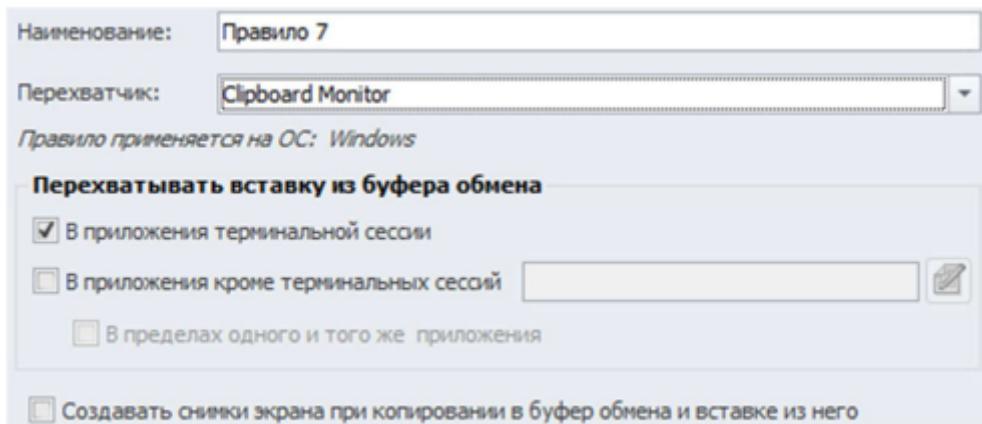


Рисунок 66 – «Открытие подключение к удаленному рабочему столу»

Теперь вернитесь к Device Monitor Console и создайте список приложений для правила, добавив в него «mstsc.exe». Вернитесь к политике «Отдел 2» и создайте правило в соответствии с рисунком 67. Затем, перейдите к политике «Политика на устройства» и создайте правило в соответствии с рисунком 68.

Актив
Чтобы а
раздел '

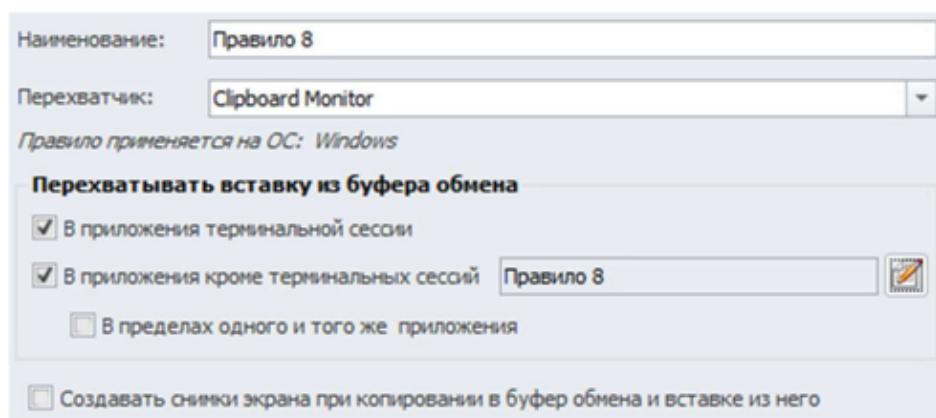




Необходимо поставить на контроль буфер обмена в текстовых процессорах (Word или Writer или Wordpad).

Проверить работоспособность и зафиксировать выполнение занесением пары событий в IWTM на любые политики.

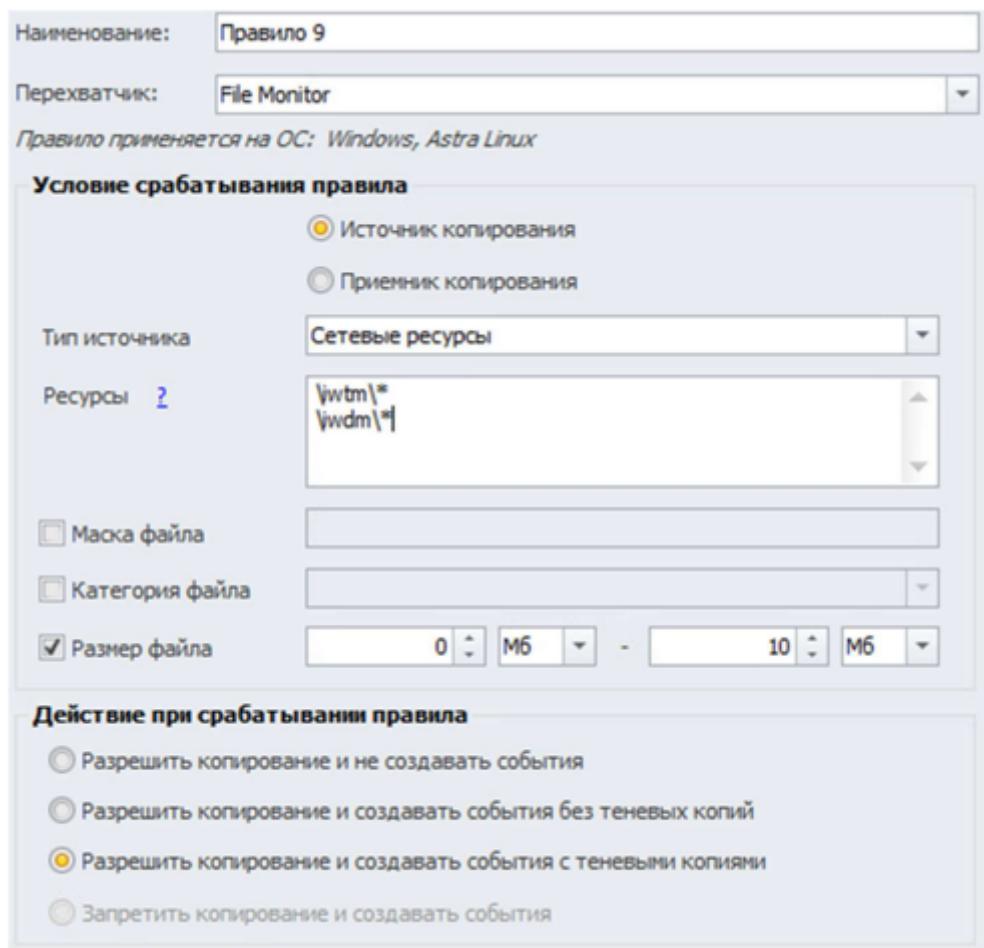
оба. Что бы открыть их воспользуйтесь поиском Windows: для LibreOffice Writer – LibreOffice Writer, для WordPad – WordPad. Открыв оба приложения, вернитесь к Device Monitor Console. Во вкладке «Приложения» найдите «WORDPAR.exe» и «swriter.exe», после чего создайте список «Правило 8» и добавьте их к списку.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



Для предотвращения неэффективного расхода рабочего времени сотрудников отслеживать движение видео контента (*.avi, *.mkv, *.mp4) в общих папках компании. Отдельно контролировать файлы больше 10 Мбайт и меньше 10

Мбайт. (1 Мбайт = 1000 Кбайт)

Проверить работоспособность и зафиксировать выполнение скриншотом



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).

Ответ : «Создать объект групповой политики в этом домене и связать его...» назовите объект произвольным именем (прим.: Office). Затем сразу отредактируйте фильтры безопасности созданной политики. Для этого откройте созданный объект политики, удалите «Прошедшие проверку» и добавьте ПК 2 (на машину пользователя W10-Agent).

office

Область Сведения Параметры Делегирование

Связи

Показать связи в расположении: demo.lab

С GPO связаны следующие сайты, домены и подразделения:

Размещение	Принудительный	Связь задействована	Путь
demo lab	Нет	Да	demo lab

< >

Фильтры безопасности

Параметры данного объекта групповой политики применяются только для следующих групп, пользователей и компьютеров:

Имя
Прошедшие проверку

Добавить... Удалить Свойства

Фильтр WMI

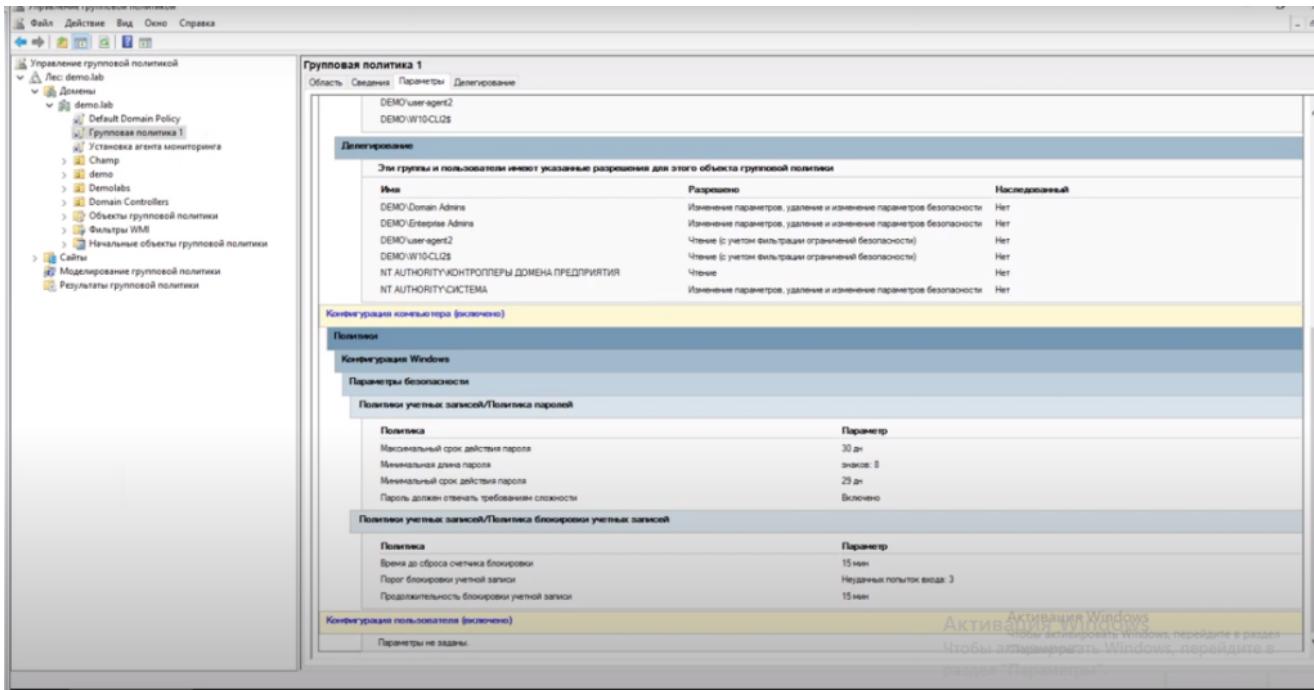
Объект GPO связан со следующим фильтром WMI:

«отсутствует» Открыть

нужно добавить комп нарушителя, а также пользователя для этого пк

Групповая политика 1

Настроить политику паролей и блокировки: Максимальный срок действия пароля — 192 дня, Минимальная длина пароля — 8, пароль должен отвечать требованиям сложности, Блокировка учетной записи при повторном вводе неверного пароля (3 раза), продолжительность блокировки 15 минут.



Делать вот такой скрин

Зафиксировать настройки политики скриншотами.

Ответ: Конфигурация компьютера – Политики – Конфигурация Windows – Параметры безопасности – Политика паролей – далее идет установка необходимых настроек

Групповая политика 2

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

Зафиксировать настройки политики и выполнение скриншотами.

1. Конфигурация пользователя – административные шаблоны – система – не запускать указанные приложения виндовс – установить «Включено», а затем нажать по кнопке «Показать» в пункте «Список запрещенных программ» – указать список запрещенных программ powershell.exe,

SnippingTool.exe, msinfo32.exe

Групповая политика 3

Запретить использование панели управления стандартными политиками.

Зафиксировать настройки политики и выполнение скриншотами.

Ответ: Конфигурация пользователя — Политики — Административные шаблоны — Панель управления — Запретить доступ к панели управления — включено.

Групповая политика 4

Запретить пользователю самостоятельно менять обои рабочего стола.

Зафиксировать настройки политики и выполнение скриншотами.

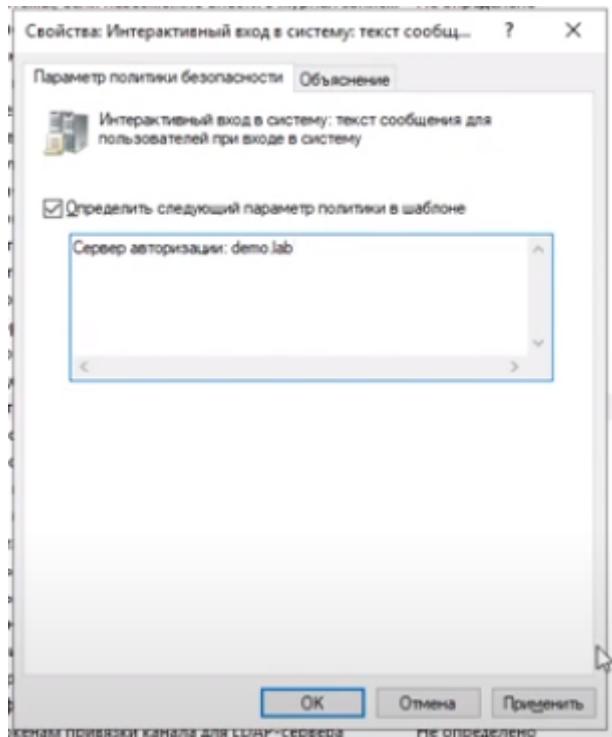
Конфигурация пользователя — административные шаблоны — панель управления — персонализация — запрет изменения фона рабочего стола — нажать «включено»

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.

Политика	Параметр политики
DCOM: Ограничения компьютера на доступ в синтаксисе SDDL (Security Descriptor Definition Language)	Не определено
DCOM: Ограничения компьютера на запуск в синтаксисе SDDL (Security Descriptor Definition Language)	Не определено
Аудит: аудит доступа глобальных системных объектов	Не определено
Аудит: аудит использования привилегий на архивацию и восстановление	Не определено
Аудит: немедленное отключение системы, если невозможно внести в журнал записи аудита	Не определено
Аудит: принудительно переопределяет параметры категории политики аудита параллельного доступа	Не определено
Доступ к сети: Разрешить трансляции анонимного SID в имя	Не определено
Завершение работы: очистка файла подкачки виртуальной памяти	Не определено
Завершение работы: разрешить завершение работы системы без выполнения входа в систему	Не определено
Интерактивный вход в систему: поведение при извлечении смарт-карты	Не определено
Интерактивный вход в систему: заголовок сообщения для пользователя при входе в систему	Не определено
Интерактивный вход в систему: количество предыдущих подключений к кешу (в службах)	Не определено
Интерактивный вход в систему: напоминать пользователям об истечении срока действия пароля	Не определено
Интерактивный вход в систему: не отображать имя пользователя при входе в систему	Не определено
Интерактивный вход в систему: не отображать учетные данные последнего пользователя	Не определено
Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL	Не определено
Интерактивный вход в систему: отображать сведения о пользователе, если сеанс заброшен	Не определено
Интерактивный вход в систему: пороговое число неудачных попыток входа	Не определено
Интерактивный вход в систему: предел простой компьютера	Не определено
Интерактивный вход в систему: текст сообщения для пользователей при входе в систему	Не определено
Интерактивный вход в систему: требовать Windows Hello для бизнеса или смарт-карту	Не определено
Интерактивный вход в систему: требовать проверки на контроллере домена для отключения	Не определено
Клиент сети Microsoft: использовать цифровую подпись (всегда)	Не определено
Клиент сети Microsoft: использовать цифровую подпись (с согласия сервера)	Не определено
Клиент сети Microsoft: отправлять незашифрованный пароль сторонним SMB-серверам	Не определено
Консоль восстановления: разрешить автоматический вход администратора	Не определено
Консоль восстановления: разрешить копирование диска и доступ ко всем дискам и устройствам	Не определено
Контроллер домена: запретить изменение пароля учетных записей компьютера	Не определено
Контроллер домена: разрешать узловые подключения защищенным каналом	Не определено



Гр доп

Отключить возможность локального входа для пользователей iwtm-officer и Idapsync-user с помощью групповых политик

Выполнение задания подтвердить скриншотами.

Ответ:

Конфигурация компьютера Политики Конфигурация Windows

Параметры безопасности Локальные политики Назначение

прав пользователя Запретить локальный вход = DEMO\iwtmofficer,

DEMO\Idapsync-user

С помощью редактора групповой политики запретить показ анимации при входе в систему. Выполнение задания подтвердить скриншотами.

Ответ:

Конфигурация компьютера Политики Административные

шаблоны Система Вход в систему Показать анимацию при

первом входе в систему = Отключено.

Описание модуля 3:

Создайте в DLP-системе политики безопасности согласно нижеперечисленным заданиям. Политики должны автоматически блокировать трафик и/или предупреждать о нарушении в соответствии с заданием. Способ, которым создана корректная политика, оставлен на усмотрение самого экзаменуемого.

При выявлении уязвимости DLP-система должна автоматически устанавливать уровень угрозы в соответствии с заданием. После создания всех политик может быть запущен автоматический «генератор трафика», который передаст поток данных, содержащих как утечки, так и легальную информацию.

При правильной настройке политики должны автоматически выявить (или блокировать) и маркировать инциденты безопасности. Не должно быть ложных срабатываний. Не должно быть неправильной маркировки. Должны быть выявлены все инциденты безопасности.

Для некоторых политик могут понадобиться дополнительные файлы, расположение которых можно узнать из карточки задания или у экспертов.

Выполнение отдельных заданий необходимо подтвердить скриншотом (это всегда указывается отдельно). Скриншоты необходимо сохранить в папке «Модуль 3».

Скриншоты необходимо называть в соответствии с номером задания и типом задания (Например Политика 2, Задание 1–1 и т. д.) Задания на разработку политик можно выполнять в любом порядке.

Наиболее сложные политики находятся в конце.

При разработке политик стоит учитывать, что все политики трафика могут передаваться как через веб-сообщения, так и через почтовые сообщения. В случае, если данный пункт не соблюден, то проверка заданий может быть невозможной.

Списки сотрудников, занимаемые позиции и отделы сотрудников представлены в разделе «Персоны» по результатам LDAP-синхронизации.

Список тегов для политик: Политика 1, Политика 2, Политика 3, ...

Задание 1

Необходимо выключить или удалить стандартные политики и отключить стандартные каталоги объектов защиты.

The screenshot shows a software interface for managing protection policies and objects. On the left, a list of policies is shown:

- демоэкзамен** (selected)
- Договоры и контракты**
- Отдел кадров**
- Маркетинг**
- Грифованная информация**
- Конкурсная документация**

Each item has a sub-menu with options: Передача, Копирование, Хранение, Работа в приложениях.

On the right, a detailed view of the selected policy 'демоэкзамен' is displayed:

- Название:** демоэкзамен
- Период действия:** Все время
- Статус:** включен (green switch)
- Защищаемые данные:** Выбрать
- Описание:** Введите описание
- Создан:** 17.12.2021 05:30
- Изменен:** 17.12.2021 05:31

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

(выключить и удалить все к черту)

The screenshot shows a software interface for managing protection objects. On the left, a sidebar shows catalog types:

- Все (All)
 - Активные (Active)
 - Все элементы (All elements)
 - Финансовые (Financial)
 - Управление (Management)
 - Грифы (Griffes)
 - Конкурсная документация (Competitive documentation)
 - Система безопасности (Security system)
 - Персональные данные (Personal data)
 - Отдел кадров (Human resources department)
 - Договоры и контракты (Contracts)
 - Маркетинг (Marketing)

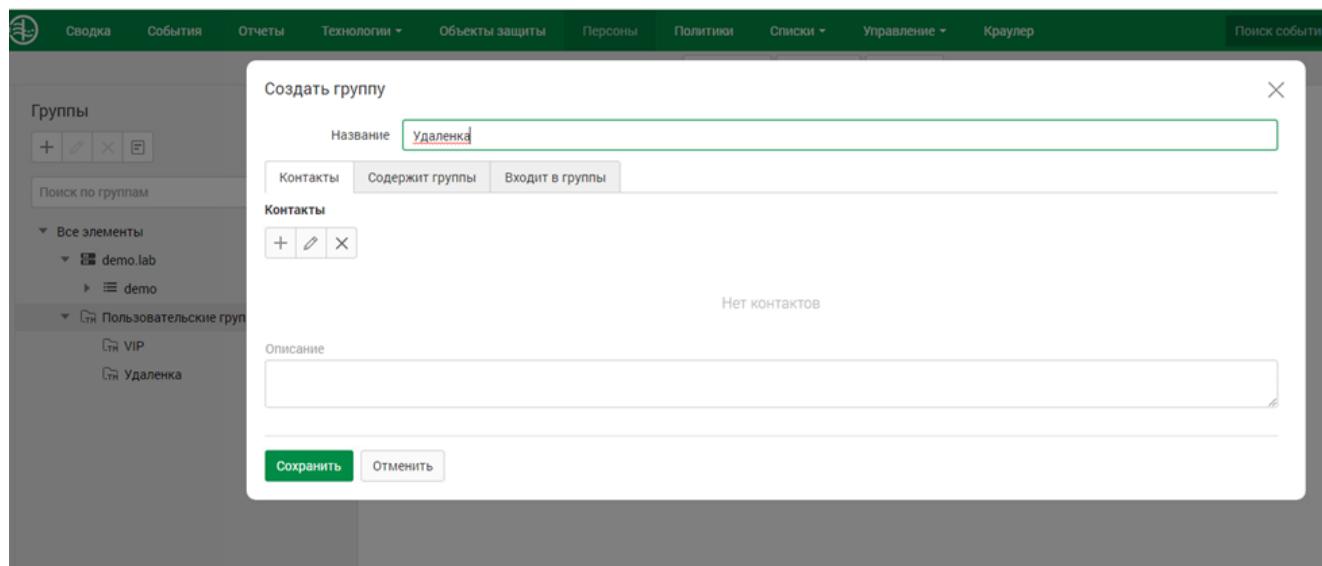
A context menu is open over the 'Грифы' item, showing options: Активировать (Activate), Деактивировать (Deactivate), Импортировать (Import), Экспортировать (Export), Создать политику защиты данных (Create a protection policy for data), and Создать политику защиты данных на агенте (Create a protection policy for data on agent).

On the right, a table lists protection policies:

Название	Элементы технологий	Дата создания	Дата изменения	Описание
Грифы конфиденциальности	Грифы конфиденциальности	17.11.2021 05:29	17.11.2021 05:29	
Грифы секретности	Грифы секретности	17.11.2021 05:29	17.11.2021 05:29	

Задание 2

Создайте локальную группу пользователей «Удалёнка» и добавьте в нее 3 пользователей. Перейдите в раздел Персоны. 2. В левой части рабочей области выберите Пользовательские группы. 3. На панели инструментов в левой части рабочей области нажмите Создать группу. 4. В открывшемся окне укажите название новой группы и при необходимости введите примечание. Также вы можете указать контакты группы. В качестве контактов могут выступать Электронная почта и Электронная почта Lotus. 5. Нажмите Сохранить.



The screenshot shows the Traffic Monitor application's user management interface. On the left, there's a sidebar titled 'Группы' (Groups) with a tree view. Under 'demo.lab', there's a group named 'Удаленка'. On the right, a main panel titled 'Удаленка' displays three users: Agafonov A Luka, Berezhnaya Maria, and Danilov A Valentin. Each user has a small profile picture, their name, title ('менеджер отдела договоров'), email address, and phone number.

Задание 3

Создать список веб-ресурсов. Добавить в список следующие сайты: rt.ru, infotechs.ru, dnevnik.ru\. В веб-интерфейсе Traffic Monitor, в верхней части сайта перейдите ко вкладке «Списки» и из контекстного меню выберите «Веб-ресурсы». В левой части найдите кнопку «Создать список веб-ресурсов». Назовите его «Сайты партнеров». Как то называть этот список. Перейдите к созданному списку и нажмите кнопку «Добавить веб-ресурс» и начните добавлять необходимые ресурсы.

The screenshot shows the 'Списки' (Lists) section of the Traffic Monitor interface. A modal window titled 'Создать список веб-ресурсов' (Create web resources list) is open. In the 'Название' (Name) field, the value 'Сайты партнеров' is entered. The 'Описание' (Description) field is empty. At the bottom, there are 'Сохранить' (Save) and 'Отменить' (Cancel) buttons. Below the modal, a table lists various web resources with their descriptions: 'Анонимайзеры', 'Блоги', 'Веб-почта', 'Медиа', 'Мусорный трафик', 'ПО и обновления', 'Поиск работы', and 'Потенциально опасные ресурсы'. To the right of the table, there are several small text entries under the heading 'Тематика для взрослых' (Topic for adults).

Добавить веб-ресурс



Значение

kb.infowatch.com

Описание

Сохранить

Отменить

(значения будут отличаться)

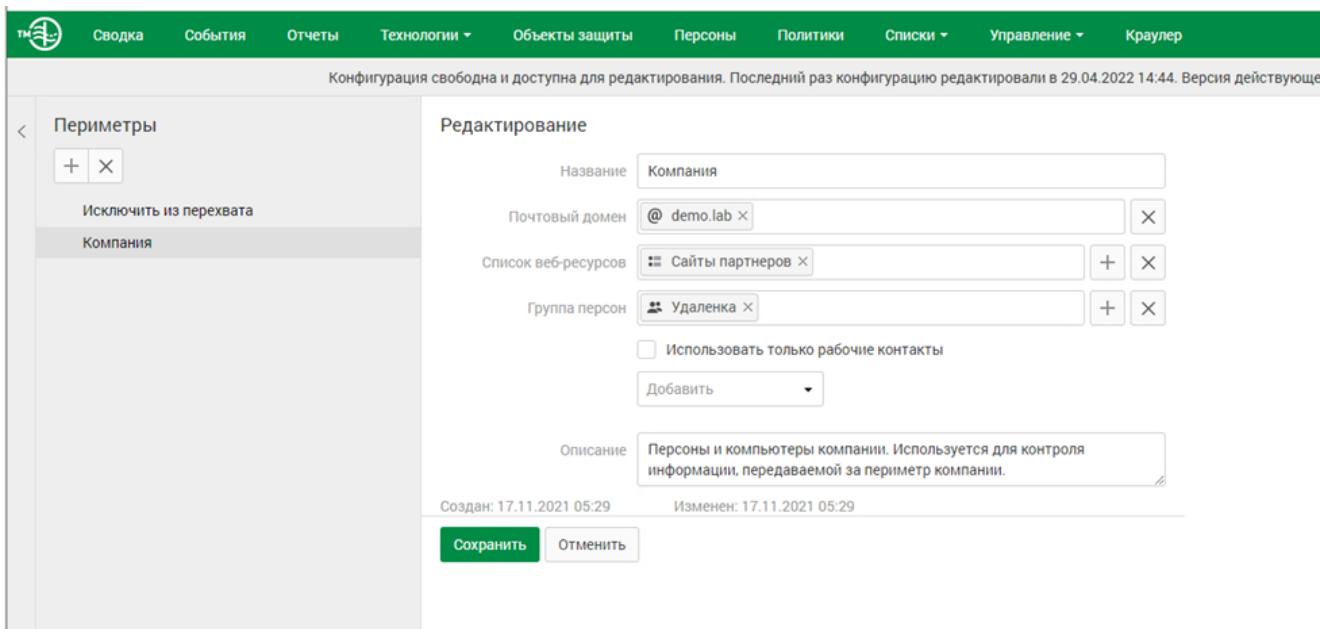
Вы редактируете конфигурацию с 29.04.2022 14:43. Применить Сохранить Сбросить Версия действующей конфигурации - № 8.

Значение	Описание
dnevnik.ru\	
infotechs.ru	
rt.ru	

Задание 4

Для работы системы необходимо настроить периметр компании: Почтовый домен компании, список веб-ресурсов, группа персон «Удалёнка», исключить из перехвата почту генерального директора.

(раздел списки — периметры)



Конфигурация свободна и доступна для редактирования. Последний раз конфигурацию редактировали в 29.04.2022 14:44. Версия действующе

Редактирование

Название: Компания

Почтовый домен: @ demo.lab

Список веб-ресурсов: Сайты партнеров

Группа персон: Удаленка

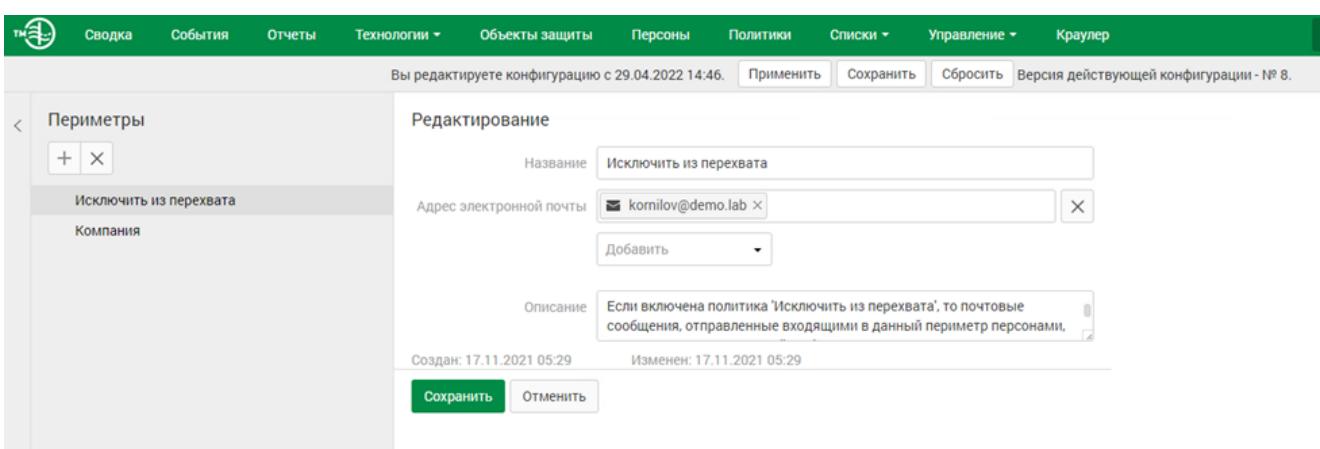
Использовать только рабочие контакты

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



Вы редактируете конфигурацию с 29.04.2022 14:46. Применить Сохранить Сбросить Версия действующей конфигурации - № 8.

Название: Исключить из перехвата

Адрес электронной почты: kornilov@demo.lab

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

Политика 1

В связи с тем, что компания является оператором обработки персональных данных, необходимо запретить всем сотрудникам, кроме отдела кадров отправлять документы, содержащие информацию о паспортных данных за пределы компании. Отдел кадров может отправлять файлы без ограничений.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 1

Вход во вкладку каталоги объектов защиты. Создание объектов защиты (5 технология в объекте) – поиск паспорт. Вторая вкладка. Добавить условия обнаружения

Создаём тег политика 1

Создаем политику – далее передача.

Политика защиты данных

Защищаемые данные

Объекты –

Добавили объект защиты

Добавляем правила – в одну сторону тип события – все – ПК – все отправитель – группы – не равно отдел кадров – получатель не равно – компания– тег ранее созданный

The screenshot shows a 'Create Tag' dialog box overlaid on a main application window. The dialog has fields for 'Name' (set to 'Политика 1') and 'Color' (a green square). At the bottom are 'Save' and 'Cancel' buttons. The background application window shows a list of tags and a configuration interface.

The screenshot shows a 'Create Protection Object' dialog box. On the left, a sidebar lists categories like 'Financials', 'Management of companies', etc. The main area shows a list of 'Text Objects' with two items selected: 'Diplomatic passport...' and 'Passport of a citizen...'. At the bottom are 'Create' and 'Cancel' buttons, along with a checkbox for creating multiple objects.

Сводка События Отчеты Технологии **Объекты защиты** Персоны Политики Списки Управление Краулер Помощь Помощь

Каталоги объектов защиты

Персональные данные

Конфигурация свободна и доступна для редактирования. Последний раз конфигурацию редактировали в 29.04.2022 14:47. Версия действующей конфигурации № 9.

Каталоги объектов защиты

Порталы

Создание объекта защиты

Категории Текстовые объекты 4 Этапонные документы Бланки Печати Выгрузки из БД Графические объекты

Поиск

Название Кредитная карта Паспорт гражданина РФ

Дата создания 17.11.2021 05:29 Описание Система срабатывает на изображение лицевой стороны б... Система срабатывает на изображение главного разворота...

Создать Отменить Создать объект защиты на каждый выбранный элемент

Сводка События Отчеты Технологии **Объекты защиты** Персоны Политики Списки Управление Краулер Помощь Помощь

Конфигурация свободна и доступна для редактирования. Последний раз конфигурацию редактировали в 29.04.2022 14:47. Версия действующей конфигурации № 9.

Каталоги объектов защиты

Персональные данные

Создание объекта защиты

Название Политика 1

Статус **включен**

Элементы технологий Условия обнаружения

Добавить условие

Условие

Паспорт гражданина РФ Графический объект

и

Загранпаспорт гражданина РФ Текстовый объект

Порог встречаемости 1

и

Дипломатический паспорт РФ Текстовый объект

Порог встречаемости 1

Создать Отменить

Сводка События Отчеты Технологии **Объекты защиты** Персоны Политики Списки Управление Краулер Помощь Помощь

Политики

Политики защиты данных:

- Политика защиты данных**
- Политика на любые данные
- Передача Копирование Хранение

Выбор защищаемых данных

Каталоги объектов защиты Объекты защиты 1 Файловые форматы

Поиск

Название	Элементы технологий	Дата создания	Дата изменения	Описание
Политика 1	Паспорт гражданина РФ, Дипломатический паспорт РФ, Резюме	29.04.2022 14:55	29.04.2022 14:55	
Резюме		17.11.2021 05:29	17.11.2021 05:29	
Сведения о государственной регистрации	ОГРН, ОГРНИП, Регистрационный номер	17.11.2021 05:29	17.11.2021 05:29	
Стратегия компании	Стратегия компании	17.11.2021 05:29	17.11.2021 05:29	
Удостоверение личности	Паспорт гражданина РФ, Загранпаспорт гражданина РФ	17.11.2021 05:29	17.11.2021 05:29	

Сохранить Отменить

Вы редактируете конфигурацию с 04.05.2022 14:45. [Применить] [Сохранить] [Сбросить] Версия действующей конфигурации - № 11.

Добавить политику **Фильтр**

Политика защиты данных

Название: Политика 1
Период действия: Всё время
Статус: Включен

Защищаемые данные

Выбрать

Политика сработает при обнаружении хотя бы одного вхождения в каждый из типов данных

Объекты защиты

Политика 1

Описание: Введите описание

Создан: 04.05.2022 14:45 Изменен: 04.05.2022 14:45

Сохранить **Отменить**

Отправители

Контакты Группы 1 Персоны Домены Периметры

- Enterprise Admins**
- Enterprise Read-only Domain Controllers**
- Financial**
- Group Policy Creator Owners**
- HR**
- IT**
- Key Admins**
- Protected Users**
- RAS and IAS Servers**

Сохранить **Отменить**

Получатели

Контакты Группы Персоны Домены Веб-ресурсы Периметры 1

Поиск:

- Название**
- Исключить из перехвата**
- Компания**

Описание: Если включена политика 'Исключить из перехвата', то почтовые сообщения, отправленные...

Действия при срабатывании правила

- Отправить почтовое уведомление**
- Начните вводить текст**
- Назначить событию вердикт**
- Разрешить**

Назначить событию вердикт

Действия при срабатывании правила

- Отправить почтовое уведомление**
- Начните вводить текст**
- Назначить событию вердикт**
- Разрешить**
- Отсутствует**

Сохранить **Отменить**

Правило передачи

Направление маршрута: → В одну сторону, ⇔ В оба направления

Тип события: Веб-сообщение, Facebook, ICQ, Mail.Ru Агент, MS Lync, Skype, Telegram, XMPP, ВКонтакте, Почта в Браузере, Почта на Клиенте

Компьютеры: DEMO-DC, DEMOLAB, IWDM, W10-CLI1, W10-CLI2

Отправители: HR

Получатели: Компания

Дни действия правила: Любой день недели

Часы действия правила: 0:00 - 0:00

Действия при срабатывании правила

Отправить почтой: Начните вводить текст

Назначить событию вердикт: Разрешить

Назначить событию уровень нарушения: Низкий

Сохранить **Отменить**

Правило передачи

Компьютеры: W10-CLI1, W10-CLI2

Отправители: HR

Получатели: Компания

Дни действия правила: Любой день недели

Часы действия правила: 0:00 - 0:00

Действия при срабатывании правила

Отправить почтой: Начните вводить текст

Назначить событию вердикт: Разрешить

Назначить событию уровень нарушения: Низкий

Назначить событию теги: Политика 1

Назначить отправителю статус: Выберите статус

Удалить событие:

Сохранить **Отменить**

Политика 2

Для контроля за движением документов необходимо вести наблюдение за передачей шаблона документа договора за пределы компании. Стоит учесть, что содержимое документа может изменяться в пределах 50%. Для настройки используйте файл примера из AdditionalFiles.iso в datastore1.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 2

Диск на iwdm – эталонные файлы

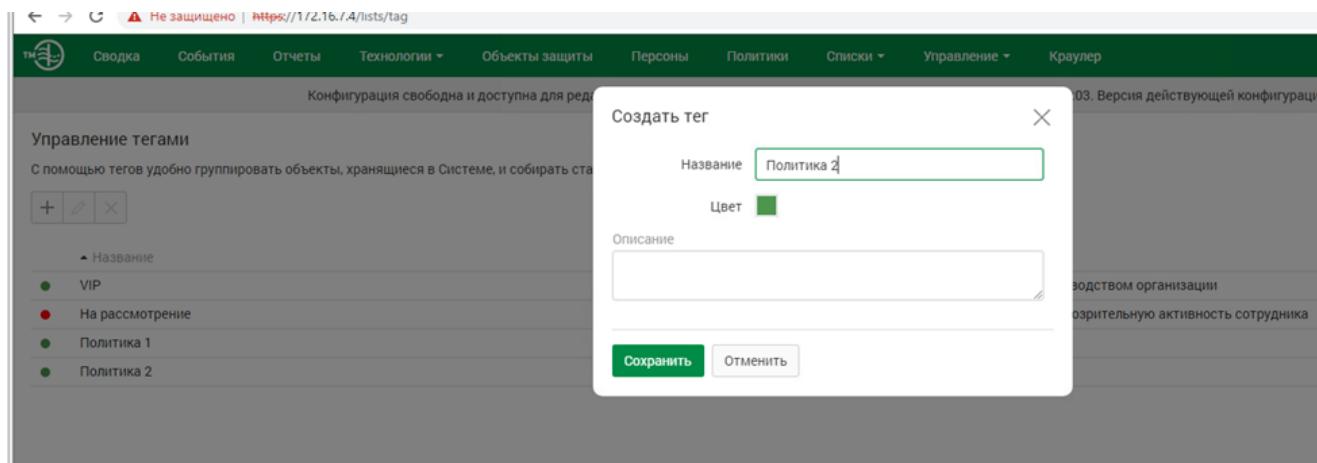
Создаем тег, после технологии – далее в объект – далее в политики (только объект)

В одну сторону

Отправитель не изменяется

Получатель не равно компания

Время и дата не изменяются Тег ранее созданный



The screenshot shows the InfoWatch Traffic Monitor Enterprise web interface. The main menu includes Home, 192.168.21.7, demo.lab, IWDM, w10-d1, IWTM, and w10-d2. The current page is 'InfoWatch Traffic Monitor Enterprise' with the URL https://172.16.22.2/protected. A warning message 'Не защищено' (Not protected) is displayed.

The main content area shows 'Каталоги объектов защиты' (Protection Object Catalogs) and a list of elements. A modal dialog titled 'Создать' (Create) is open, prompting for a name ('Название') set to 'Политика 2' and a status ('Статус') which is turned on. The 'Описание' (Description) field is empty.

Название	Статус	Описание
Политика 2	On	

This screenshot shows the 'Create Protection Object' dialog. The tabs at the top are Категории, Текстовые объекты, Эталонные документы 1, Бланки, Печати, Выгрузки из БД, and Графические объекты. The 'Эталонные документы 1' tab is selected.

The left sidebar shows 'Каталоги объектов защиты' and a list of categories. The 'Эталонные документы' section shows a list of documents with checkboxes for 'Название' and 'Файл'. One document, 'Договор.doc', is selected.

Название	Файл	Размер файла	Дата создания	Описание
Договор.doc	Документ Microsoft Word	Договор.doc	40.5 KB	04.05.2022

At the bottom of the dialog are 'Создать' (Create), 'Отменить' (Cancel), and a checkbox for 'Создать объект защиты на каждый выбранный элемент' (Create protection object for each selected element).

Создание объекта защиты

Название: Политика 2

Статус: включен

Элементы технологий | Условия обнаружения

Выбрать элементы

Договор.doc
Эталонный документ.

Описание:

Создать Отменить

Каталоги объектов защиты

Политика 2

Все | Активные, Неактивные

- Грифованная информация
- Договоры и контракты
- Конкурсная документация
- Маркетинг
- Отдел кадров
- Персональные данные
- Политика 2
- Система безопасности
- Управление компанией

Вы редактируете конфигурацию с 04.05.2022 14:53.

Добавить политику | Фильтр

Политики защиты данных

Название: Политика 2

Период действия: Всё время

Статус: включен

Защищаемые данные

Выбрать

Политика сработает при обнаружении хотя бы одного вхождения в каждый из типов данных

Объекты защиты

Политика 2

Описание:

Введите описание

Создан: 04.05.2022 14:53 Изменен: 04.05.2022 14:53

Сохранить Отменить

Политики

Политики защиты данных:

- Политика защиты данных
- Политика на любые данные
- Передача Копирование Хранение Работа в приложениях

Политика 1

Объект защиты: Политика 1

Передача 1 Копирование Хранение Работа в приложениях

Политика 3

У генерального директора компании недавно появился котик и его фото утекло в сеть компании. Теперь сотрудники обмениваются смешными картинками с подписями и масками внутри компании и выкладывают их в социальные сети. Директор решил, что его котик вызвал снижение качества работы сотрудников из-за повышенной милоты картинок и хочет запретить обмен фотографией котика. Необходимо запретить обмен фотографией и немного измененной (до ≈50%) фотографией котика. Для настройки используйте файл примера из AdditionalFiles.iso в datastore1.

Вердикт: блокировать

Уровень нарушения: низкий

Тег: Политика 3

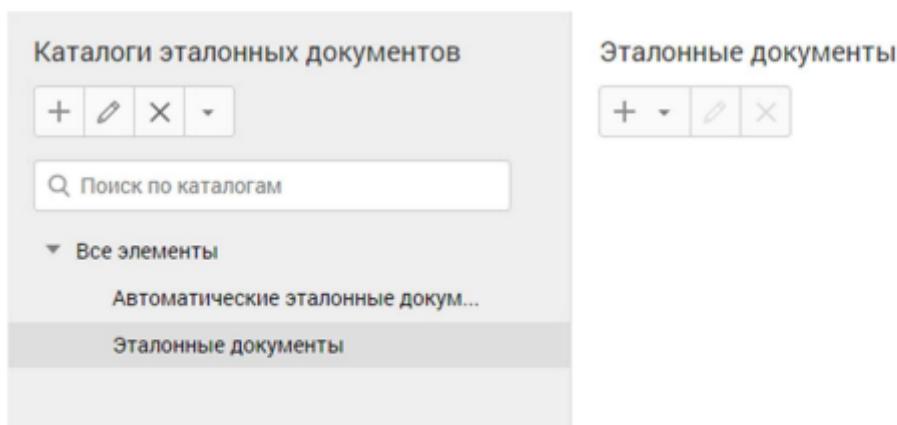


Рисунок 75 – «Эталонные документы»

Найдите кнопку «Создать», располагающуюся под текстом «Каталоги эталонных документов» и создайте новый каталог, назовите его «Политика 1». Установите порог цитируемости для бинарных данных на 50%.

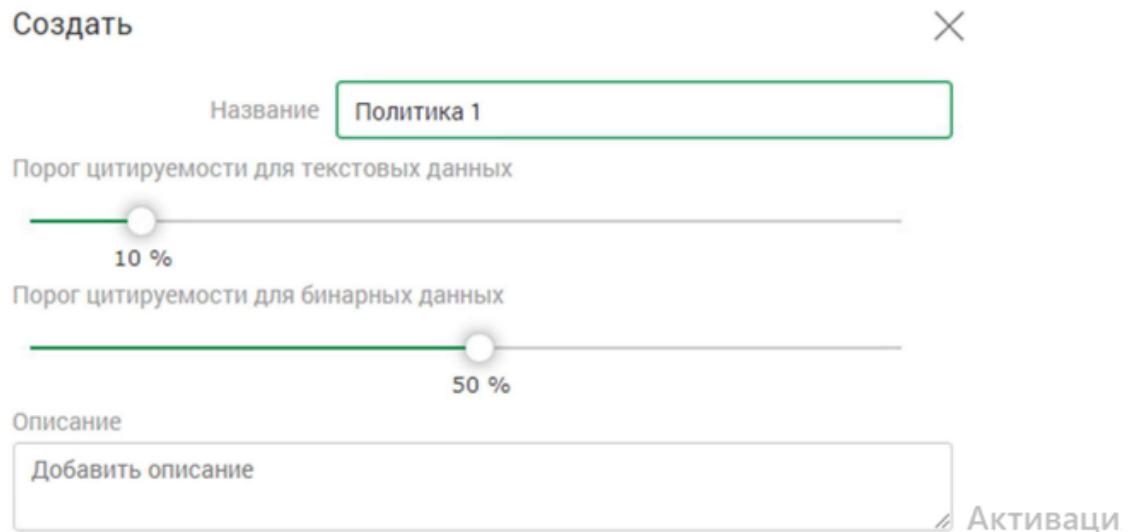


Рисунок 76 – «Создание каталога эталонных документов»

Перейдите к созданному каталогу и нажмите кнопку «+» для добавления эталонного документа. В выпадающем меню выберите «На основе всех типов данных». Загрузите фотографию котика из открывшегося окна приложения Проводник. Настройки документа автоматически будут синхронизированы с настройками каталога. После добавления котика в эталонные документы, перейдите ко вкладке «Объекты защиты» и найдите кнопку «Создать», находящуюся под текстом «Каталоги объектов защиты» и создайте каталог «Политика 3» (политика защиты данных).

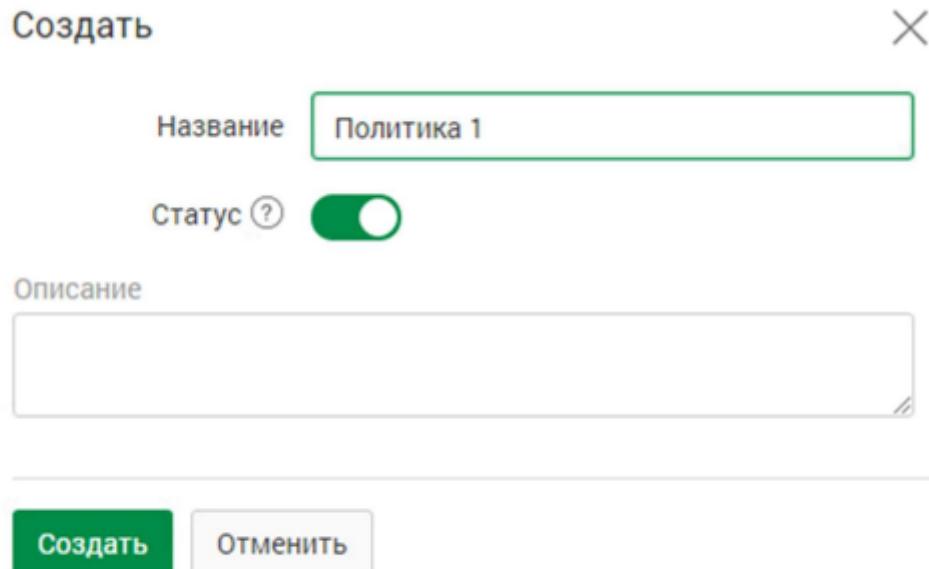
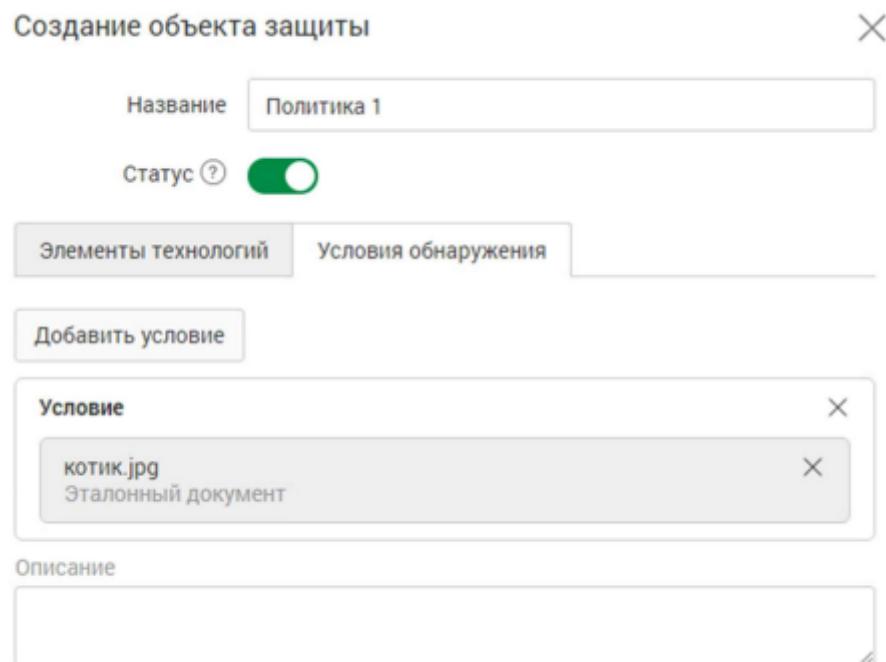


Рисунок 78 – «Создание каталога объектов защиты»

Перейдите к созданному каталогу и нажмите кнопку «Создать», в открывшемся окне создания объекта защиты перейдите ко вкладке «Эталонные документы», перейдите к созданному ранее каталогу и выберите фотографию котика. После чего будет предложено выбрать условие обнаружения – выберите котиков.



После создания объекта защиты перейдите во вкладку «Списки» и в выпадающем меню выберите «Теги». Создайте новый тег «Политика 1». Вернувшись ко вкладке «Политики» найдите созданную политику «Политика 1».

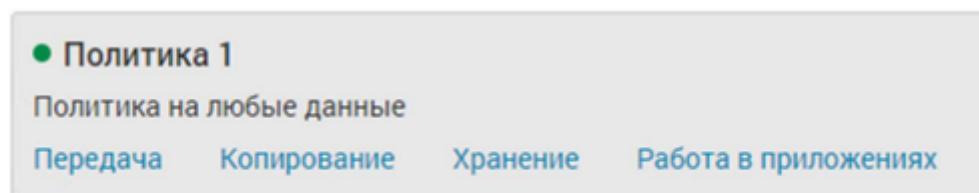


Рисунок 80 – «Политика 1»

Правило передачи

Направление маршрута	<input type="button" value="→ В одну сторону"/> <input type="button" value="⇄ В оба направления"/>
Тип события	<input type="button" value="Тип"/>
Компьютеры	<input type="button" value="DEMO-DC X"/> <input type="button" value="DEMOLAB X"/> <input type="button" value="IWDM X"/> <input type="button" value="W10-CLI1 X"/> <input type="button" value="W10-CLI2 X"/> <input style="float: right; margin-top: -20px;" type="button" value="+"/>
Отправители	<input type="button" value="="/> <input type="text" value="Начните вводить текст"/> <input style="float: right; margin-top: -20px;" type="button" value="+"/>
Получатели	<input type="button" value="="/> <input type="text" value="Начните вводить текст"/> <input style="float: right; margin-top: -20px;" type="button" value="+"/>
Дни действия правила	<input type="text" value="Любой день недели"/>
Часы действия правила	<input type="text" value="0:00"/> <input type="button" value="⌚"/> - <input type="text" value="0:00"/> <input type="button" value="⌚"/>

Действия при срабатывании правила

Отправить почтовое уведомление	<input type="text" value="Начните вводить текст"/> <input style="float: right; margin-top: -20px;" type="button" value="+"/>	Ак Что раз
Назначить событию вердикт	<input type="checkbox"/> Заблокировать	
Назначить событию	<input type="text" value="Новый"/>	

Отправители	<input type="text"/> =	Начните вводить текст	<input type="button" value="+"/>	
Получатели	<input type="text"/> =	Начните вводить текст	<input type="button" value="+"/>	
Дни действия правила	Любой день недели			
Часы действия правила	0:00	<input type="button"/>	0:00	<input type="button"/>

Действия при срабатывании правила

Отправить почтовое уведомление	Начните вводить текст	<input type="button" value="+"/>
Назначить событию вердикт	<input checked="" type="checkbox"/> Заблокировать	<input type="button"/>
Назначить событию уровень нарушения	<input checked="" type="radio"/> Низкий	<input type="button"/>
Назначить событию теги	Политика 1 ×	<input type="button" value="+"/>
Назначить отправителю статус	Выберите статус	<input type="button"/>
Удалить событие	<input type="button"/>	

Акти
Чтобы
разде

Политика 4

Необходимо

отслеживать документы, содержащие печать компании всем сотрудникам, кроме отдела бухгалтерии и генерального директора. Они могут обмениваться документами внутри и за пределами компании без контроля. Для настройки используйте файл примера из AdditionalFiles.iso в datastore1.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 4

Вы редактируете конфигурацию с 04.05.2022 15:28.

Каталоги печатей

Политика 4

Выберите файлы для загрузки.
Система поддерживает следующий список форматов для создания

Открытие

Упорядочить

	Имя	Дата изменения	Тип	Размер
<input checked="" type="checkbox"/>	Быстрый доступ	13.07.2020 15:25	Документ Office ...	18 KB
<input checked="" type="checkbox"/>	Рабочий стол	13.07.2020 15:36	Файл "CSV"	270 KB
<input checked="" type="checkbox"/>	Загрузки	13.07.2020 15:27	Файл "DOC"	41 KB
<input checked="" type="checkbox"/>	Документы	28.11.2020 0:27	Документ Office ...	14 KB
<input checked="" type="checkbox"/>	Изображения	13.07.2020 15:36	Файл "JPG"	259 KB
<input checked="" type="checkbox"/>	Share	13.07.2020 15:44	Файл "PNG"	798 KB
<input checked="" type="checkbox"/>	Печать			

Имя файла: Печать

Открыть Отмена

Создание объекта защиты

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

Каталоги печатей

Печати

	Название	Формат файла	Название файла	Размер файла	Дата создания	Оп
<input checked="" type="checkbox"/>	Печать.png	Изображение PNG	Печать.png	797.86 KB	04.05.202...	

Создать Отменить Создать объект защиты на каждый выбранный элемент

Конфигурация свободна и доступна для редактирования.

Каталоги объектов защиты

Политика 4

Название: Политика 4

Статус: включен

Элементы технологий: Условия обнаружения

Добавить условие

Условие:

- Печать.rpt
- Печать

Описание:

Создать **Отменить**

Все | Активные | Неактивные

Все элементы

- Грифованная информация
- Договоры и контракты
- Конкурсная документация
- Маркетинг
- Отдел кадров
- Персональные данные
- Политика 2
- Политика 3
- Политика 4
- Система безопасности
- Управление компанией
- Финансы

Вы редактируете конфигурацию с 04.05.2022 15:32. Применить Сохранить Сбросить Версия действующей конфигурации - № 27.

Поиск событий iwtm-officer

Политики

Политики защиты данных:

- Политика защиты данных
- Политика на любые данные
- Передача Копирование Хранение Работа в приложениях

- Политика 3
- Объект защиты: Политика 3
- Передача 1 Копирование Хранение Работа в приложениях

- Политика 2
- Объект защиты: Политика 2
- Передача 1 Копирование Хранение Работа в приложениях

- Политика 1
- Объект защиты: Политика 1
- Передача 1 Копирование Хранение Работа в приложениях

Политика защиты данных

Название: Политика 4

Период действия: Все время

Статус: включен

Зашieldedные данные

Выбрать

Политика сработает при обнаружении хотя бы одного вхождения в каждый из типов данных

Объекты защиты:

- Политика 4

Описание: Введите описание

Создан: 04.05.2022 15:32 Изменен: 04.05.2022 15:32

Сохранить **Отменить**

The screenshot shows the InfoWatch Traffic Monitor Enterprise web interface. The main menu includes 'Сводка', 'События', 'Отчеты', 'Технологии', 'Объекты защиты', 'Персоны', 'Политики', 'Списки', 'Управление', and 'Краулер'. A search bar at the top right contains 'iwtm-officer'. The central area displays 'Конфигурация свободна и доступна для редактирования. Последний раз конфигурацию редактировали в 04.05.2022 15:56. Версия действующей конфигурации № 33.' Below this, a section titled 'Политики' lists three policies: 'Политика 4', 'Политика 3', and 'Политика 2'. Each policy has tabs for 'Передача 1' (Copy), 'Хранение' (Storage), and 'Работа в приложениях' (Work with applications). The 'Политика 4' tab is active, showing a 'Добавить правило' (Add rule) button. The 'Правило передачи' (Transmission rule) panel on the right is configured with the following settings:

- Направление маршрута:** В одну сторону (One-way) and В оба направления (Both directions).
- Тип события:** Веб-сообщение: Facebook, ICQ, MS Lync, Mail.Ru Агент, Skype, Telegram, XMPP; ВКонтакте, Почта в Браузере, Почта на Клиенте.
- Компьютеры:** DEMO-DC, DEMOLAB, IWDM, W10-CLI1.
- Отправители:** Kornilov V. Fedosej, Accounting.
- Получатели:** (empty field).
- Дни действия правила:** Любой день недели.
- Часы действия правила:** 0:00 - 0:00.
- Действия при срабатывании правила:**
 - Отправить почтовое уведомление: Начните вводить текст.
 - Назначить событию вердикт: Разрешить.
 - Назначить событию уровень нарушения: Низкий.

At the bottom right of the rule panel are 'Сохранить' (Save) and 'Отменить' (Cancel) buttons.

Политика 5

В последнее время возникла необходимость обработки текстовых данных, а также сканов и фото кредитных карт. Необходимо отслеживать передачу всех возможных данных кредитных карт (в том числе сканов) за пределы компании.

Вердикт: разрешить

Уровень нарушения: средний

Тег: Политика 5

объектов защиты – «Политика 2». В новый каталог добавьте три объекта защиты: Графический объект: Кредитная карта; Текстовый объект: номер кредитной карты; Текстовый объект: номер кредитной карты (16 цифр). Важным моментом при добавлении объектов защиты, является отметка чекбокса (квадратик для выбора) «Создать объект защиты на каждый выбранный элемент».

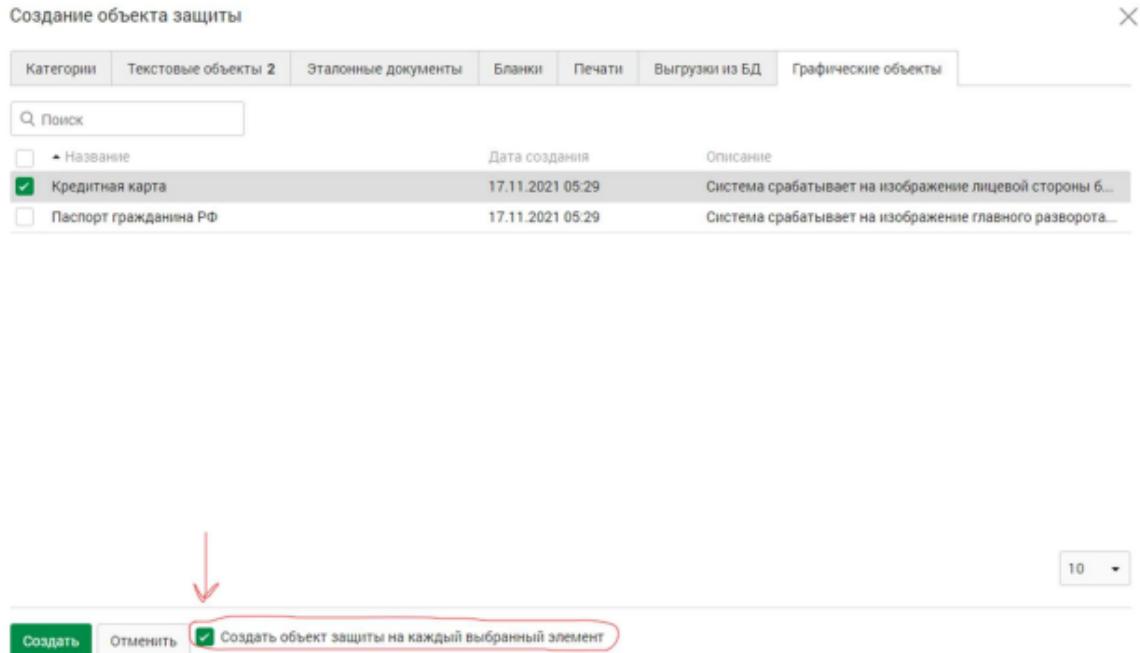


Рисунок 82 – «Чекбокс “создать объект защиты на каждый выбранный элемент”»

После создания объекта защиты, перейдите ко вкладке «Списки» → «Теги». Создайте тег «Политика 2».

Перейдите на вкладку «Политики» и создайте новую политику - «Политика 2» (политика защиты данных). В качестве защищаемых данных выберите каталог объектов защиты «Политика 2».

Политика защиты данных		Добавить правило
Название	Политика 2	
Период действия	Все время	
Статус	<input checked="" type="checkbox"/>	

Защищаемые данные

Политика сработает при обнаружении хотя бы одного вхождения в каждый из типов данных

Активация
Чтобы активи...
раздел "Пара...

Правило передачи

Направление маршрута

Тип события

Компьютеры

W10-CLI1 W10-CLI2



Отправители

Accounting



Получатели

Начните вводить текст



Дни действия правила

Любой день недели

Часы действия правила

0:00



-

0:00



Действия при срабатывании правила

Отправить почтовое уведомление

Начните вводить текст



Акт
Что
разд

Назначить событию вердикт

Заблокировать



Получатели ?	=	<input type="text" value="Начните вводить текст"/>	+
Дни действия правила	<input type="text" value="Любой день недели"/>		
Часы действия правила	0:00	-	0:00

Действия при срабатывании правила

Отправить почтовое ? уведомление	<input type="text" value="Начните вводить текст"/>	+
Назначить событию вердикт	<input checked="" type="checkbox"/> Заблокировать	-
Назначить событию уровень нарушения	<input checked="" type="radio"/> Высокий	-
Назначить событию теги	<input type="text" value="Политика 2 X"/>	+
Назначить отправителю статус	<input type="text" value="Выберите статус"/>	-
Удалить событие	<input checked="" type="checkbox"/>	

Рисунок 84 – «Правило политики 2»

Активация

Политика 6

Сотрудники заподозрены в сливе баз данных клиентов. Необходимо настроить мониторинг выгрузок из БД для контроля движения данных из базы данных страховых компаний только при отправке из определенного отдела, для остальных контролировать не нужно.

Критичными данными в выгрузке являются телефоны, ИНН, Регистрационный номер, ОКФС, ОКВЭД и ОКОПФ и в 1 документе присутствует более 5 компаний. Для настройки используйте файл примера из AdditionalFiles.iso в datastore1.

Вердикт: разрешить

Уровень нарушения: средний

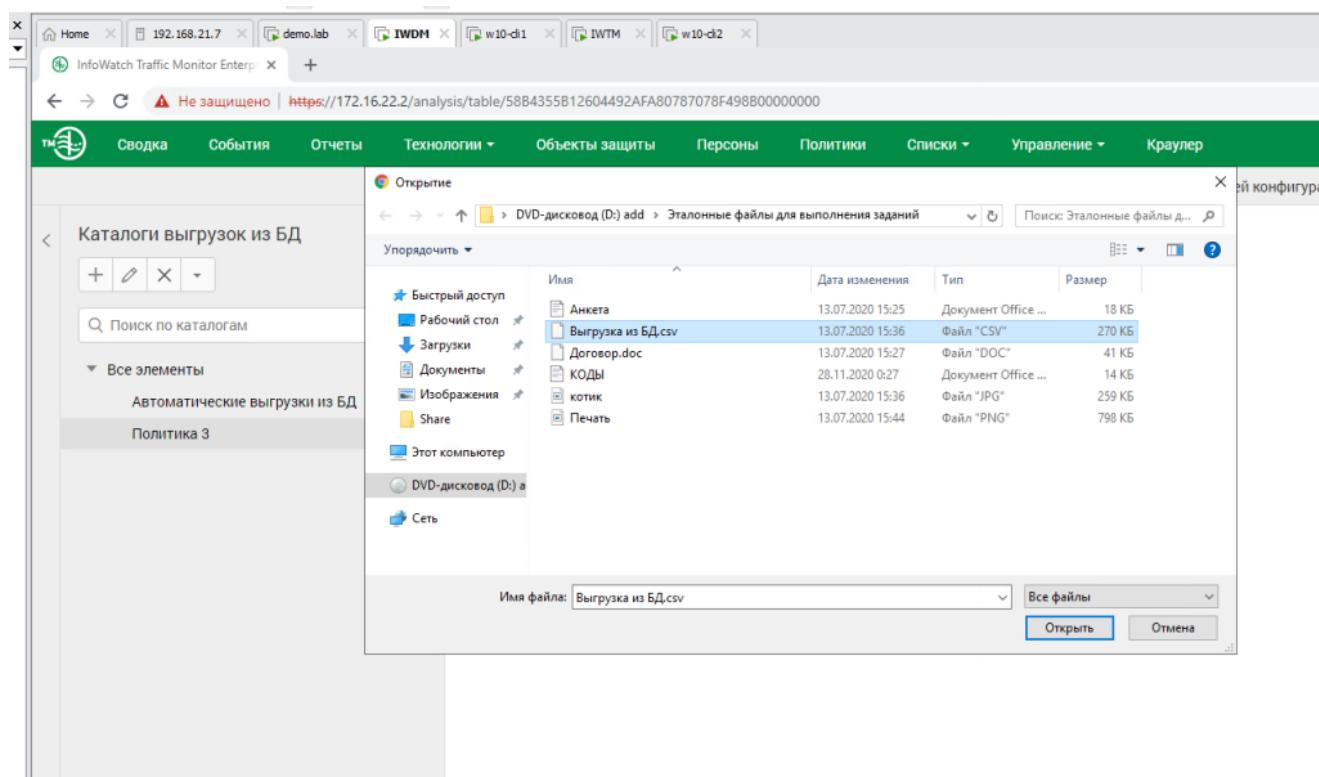
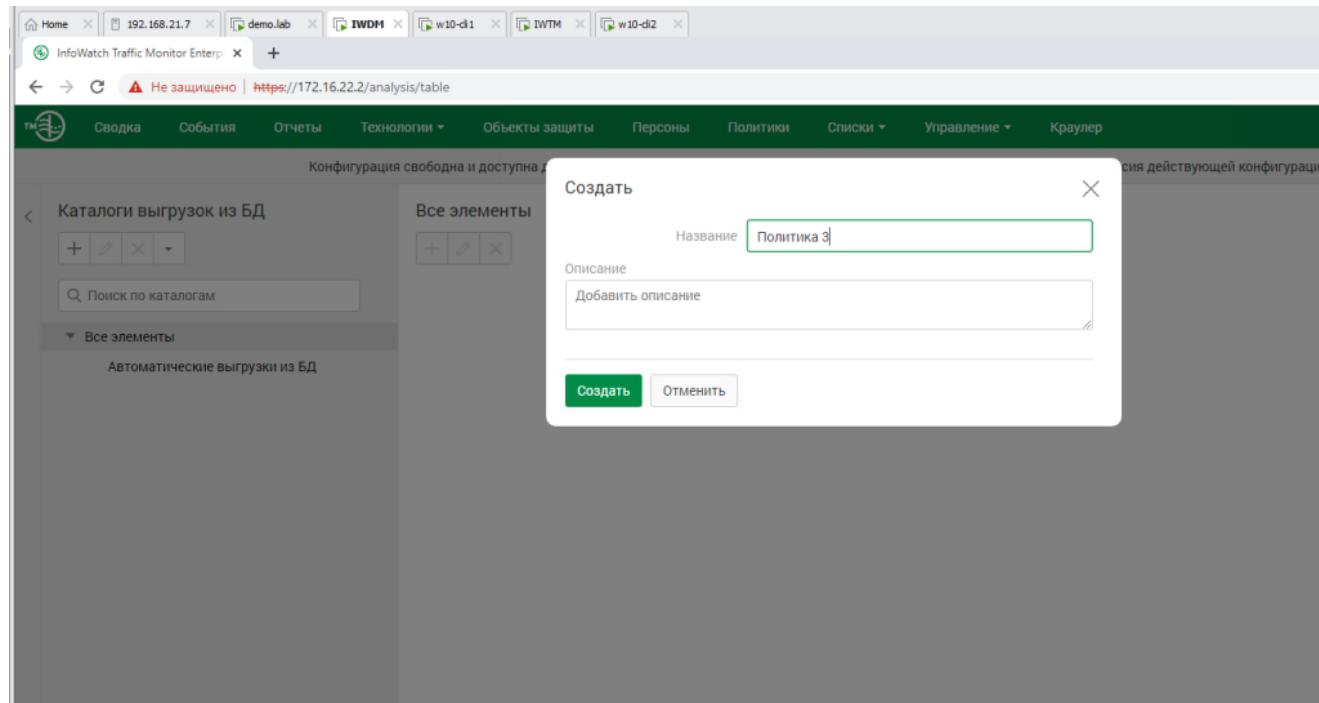
Тег: Политика 6

Для

загрузки выгрузки из БД перейдите в «Технологии» — «Выгрузки 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



Не защищено | <https://172.16.22.2/analysis/table/58B4355B12604492AFA80787078F498B00000000>

Вы редактируете конфигурацию

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 умол...	5+7+10+14+16+18	5

Описание
Введите описание

Создан: 04.05.2022 14:57 Изменен: 04.05.2022 14:57

Сохранить **Обновить** **Отменить**

Не защищено | <https://172.16.22.2/protected/D304764A72AA4AFE986A5D217AC5CB9300000000>

Каталоги объектов защиты

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

Выгрузки из БД

Создать Отменить Создать объект защиты на каждый выбранный элемент

Загрузка технологий

The screenshot shows the InfoWatch Traffic Monitor Enterprise web interface. A modal window titled "Создание объекта защиты" (Create Protection Object) is open. In the background, the main navigation bar includes tabs like "Сводка", "События", "Отчеты", "Технологии", "Объекты защиты", "Персоны", "Политики", "Списки", and "Управление". The "Объекты защиты" tab is active.

The modal window contains the following fields:

- Название:** Политика 3
- Статус:**
- Элементы технологий:** Выгрузка из БД, csv
Выгрузка из Бд
- Условия обнаружения:** Условие по умолчанию
- Добавить условие:** [button]
- Описание:** [text area]

At the bottom of the modal are two buttons: "Создать" (Create) and "Отменить" (Cancel).

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

The screenshot shows the InfoWatch Traffic Monitor Enterprise web interface. The main navigation bar is visible at the top. The "Политики" (Policies) section is active, displaying three data protection policies:

- Политика защиты данных:** Политика на любые данные
Передача Копирование Хранение Работа в приложениях
- Политика 2:** Объект защиты: Политика 2
Передача 1 Копирование Хранение Работа в приложениях
- Политика 1:** Объект защиты: Политика 1
Передача 1 Копирование Хранение Работа в приложениях

To the right, a detailed configuration panel for "Политика защиты данных" is shown:

- Название:** Политика 3
- Период действия:** Всё время
- Статус:**
- Защищаемые данные:** Выбрать
- Описание:** Введите описание
- Information at the bottom: Создан: 04.05.2022 15:01 | Изменен: 04.05.2022 15:01

Сводка События Отчеты Технологии Объекты защиты Персоны Политики Списки Управление Краулер Поиск событий iwtm-officer

Конфигурация свободна и доступна для редактирования. Последний раз конфигурацию редактировали в 04.05.2022 15:03. Версия действующей конфигурации № 22.

Политики

Добавить политику Фильтр

Политики защиты данных:

- Политика 3
Объект защиты: Политика 3
Передача Копирование Хранение Работа в приложениях
Добавить правило
- Политика 2
Объект защиты: Политика 2
Передача 1 Копирование Хранение Работа в приложениях
- Политика 1
Объект защиты: Политика 1
Передача 1 Копирование Хранение Работа в приложениях

Правило передачи

Направление маршрута → В одну сторону ⇡ В оба направления

Тип события Бейс-сообщение: Facebook, ICQ, Mail.Ru Агент, MS Lync, Skype, Telegram, XMPP: Вконтакте, Почта в Браузере, Почта на Клиенте

Компьютеры DEMO-DC DEMOLAB iWDM W10-CLI1

Отправители HR

Получатели Начните вводить текст

Дни действия правила Любой день недели

Часы действия правила 0:00 - 0:00

Действия при срабатывании правила

Отправить почтовое уведомление Начните вводить текст

Назначить событию вердикт Разрешить

Назначить событию уровень нарушения Средний

Назначить событию теги Политика 3

Сохранить Отменить

Политика 7

Компания «Ростелеком» попросила обеспечить защиту от утечки важных данных.

Необходимо создать политику на контроль правила передачи содержащие слова «абонент», «оборудование», «услуга» в 1 сообщении или документе одновременно. Если в документе встречается только по 1 слову из перечисленных — политика срабатывать не должна.

Правило должно срабатывать на сообщения, которые отправляются за пределы компании всеми пользователями, кроме отдела IT, который может отсылать информацию свободно.

Вердикт: разрешить

Уровень нарушения: средний

Тег: Политика 7

Политика 8

Для мониторинга движения анкет необходимо вести наблюдение за анкетами компании за пределы компании, запрещая любую внешнюю передачу

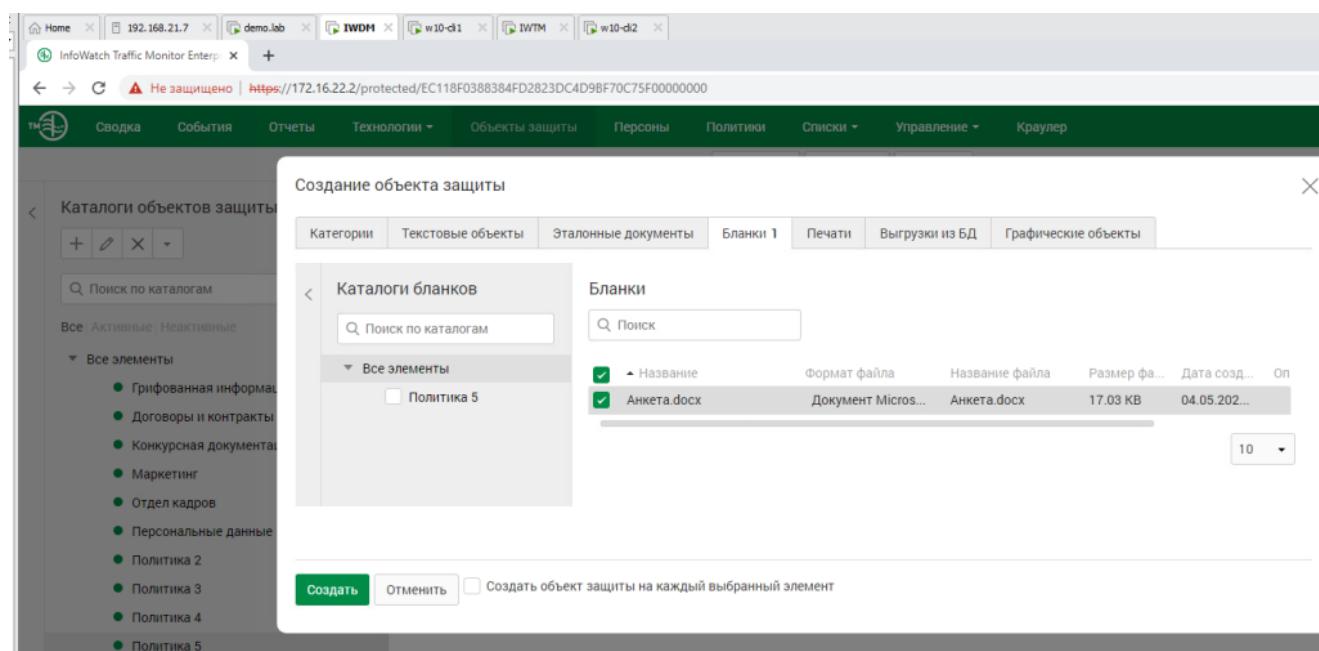
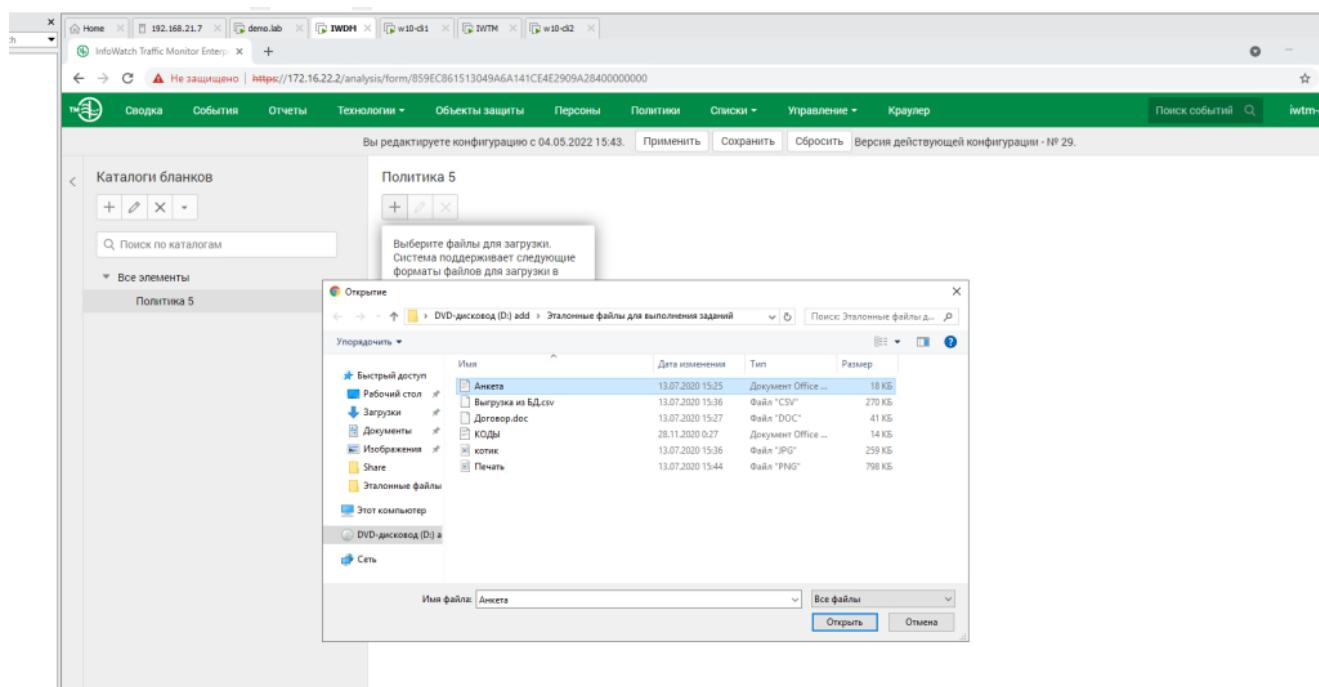
документов в пустых и заполненных бланках. Для настройки используйте файл примера из AdditionalFiles.iso в datastore1.

Генеральный директор и совет директоров могут обмениваться данной информацией совершенно свободно.

Вердикт: разрешить

Уровень нарушения: средний

Тег: Политика 8



The screenshot shows the 'Создание объекта защиты' (Create Protection Object) dialog box. The 'Название' (Name) field is set to 'Политика 5'. The 'Статус' (Status) switch is turned on. The 'Элементы технологий' (Technology Elements) tab is selected. A single item, 'Анкета.docx', is listed under 'Условие обнаружения' (Detection Condition). Below the dialog, the main interface shows a catalog of protection objects, including 'Грифованная информация', 'Договоры и контракты', and 'Конкурсная документация'.

The screenshot displays the 'Политики' (Policies) section. It lists four existing policies: 'Политика защиты данных', 'Политика 4', 'Политика 3', and 'Политика 2'. Each policy entry includes details like 'Передача', 'Копирование', 'Хранение', and 'Работа в приложениях'. To the right, a detailed view of 'Политика защиты данных' is shown, including its name ('Политика 5'), period ('Все время'), status, and associated objects ('Политика 5').

The screenshot shows the 'Политики' (Policies) section again. It highlights a policy entry for 'Любой отправитель, кроме Komarov V. Fedosej, BUD'. The 'Исполнители' (Performers) section lists 'Направление маршрута' (Route direction), 'Получатели' (Recipients), 'Компьютер' (Computer), and 'Действия' (Actions). The 'Действия' section includes icons for 'Копирование' (Copy), 'Хранение' (Storage), and 'Работа в приложениях' (Work in applications).

Политика 9

Пользователи стали часто обмениваться ссылками и файлами, в связи с этим необходимо блокировать передачу (а где это невозможно — просто контролировать) файлов формата .mp4 и ссылок формата чатов IRC. Ложных срабатываний быть не должно.

Вердикт: Заблокировать

Уровень нарушения: средний

Тег: Политика 9

Политика 10

Было замечено, что сотрудники компании стали получать множество рекламных сообщений электронной почты, из-за чего возникла необходимость отследить утечку баз email адресов сотрудников. В связи с этим необходимо детектировать сообщения, содержащие адреса электронной почты.

Важно, чтобы в одном сообщении содержалось минимум 2 адреса (т. к. в противном случае будут детектироваться все почтовые сообщения)!

Возможные домены первого уровня: ru, org и прочие. Детектирование только частей адресов (например @mail.ru) недопустимо.

Вердикт: разрешить

Уровень нарушения: высокий

Тег: Политика 10

Политика 11

В связи с разгильдяйством сотрудников, передающих свои пароли коллегам с помощью почты и сообщений, необходимо предотвратить передачу любых стандартизованных паролей для информационной системы в открытом виде любыми отправителями и получателями как внутри, так и за пределы компании.

Стоит учесть, что пароли могут передаваться любым указанным способом: социальные сети и прочие ресурсы (в браузере), мессенджеры, почта, флешки.

Необходимо также контролировать наличие паролей в сетевых каталогах.

Стоит учесть, что так как генерацией паролей занимается отдел ИТ, то пользователи отдела могут рассыпать пароли пользователям совершенно свободно, но только внутри компании.

Стандартизованные форматы паролей (кириллица): 6 букв – 1 знак !?
#\$/^/_& – 2–4 цифры – 4 буквы – 2–3 знака !?#\$^/_& (например,
ПаРоль#67рКнЕ!?)

Вердикт: разрешить

Уровень нарушения: средний

Тег: Политика 11

Политика 12

Необходимо контролировать передачу архивов, файлы таблиц только за пределы компании.

Вердикт: разрешить

Уровень нарушения: низкий

Тег: Политика 12

Описание модуля 4:

Задание 1: Контроль доступа

Необходимо создать пользователя DLP системы с определенными правами просмотра и редактирования.

Управление доступом

Роли

Название: auditor

Сводка

- Просмотр панелей
- Редактирование панелей
- Удаление панелей

События

- Полное управление запросами
- Выполнение запросов и просмотр событий
- Выгрузка событий
- Изменение решения пользователя
- Изменение тегов объекта

Сохранить Отменить



Создание роли

Удаление запросов

Отчеты

- Полное управление отчетами
- Просмотр и выполнение отчетов
- Редактирование отчетов
- Удаление отчетов
- Выгрузка отчетов

Технологии

Категории

- Просмотр категорий
- Редактирование категорий
- Удаление категорий

Активация Windows

Создание роли

[Просмотр форматов файлов](#)

Управление

LDAP-синхронизация

Просмотр LDAP-серверов

Редактирование LDAP-серверов

Удаление LDAP-серверов

Запуск синхронизации

Управление доступом

Пользователи

Просмотр пользователей

Редактирование пользователей

Удаление пользователей

Назначение ролей для пользователей

Активация Windows

Лицензия активирована. Для активации Windows, перейдите в

Настройки безопасности и активируйте Windows.

The screenshot shows the 'User Management' section of the application. On the left, there's a sidebar with 'Сводка', 'События', 'Отчеты', 'Технологии', 'Объекты защиты', 'Персоны', 'Политики', 'Еще', 'Поиск событий', 'Выгрузки', and a user 'iwtm-officer'. The 'Пользователи' tab is selected under 'Управление доступом'. In the center, there's a table showing users: 'iwtm-o' (Admin, Full), 'admin' (Admin, Admin), and 'officer' (Officer, Admin, Full). A 'Create User' form is open on the right, with fields for 'Логин' (auditor), 'Статус' (Активен), 'Email' (auditor@demo.lab), 'Полное имя' (auditor), 'Роли' (auditor), 'Области видимости' (Полный доступ), 'Описание' (Описание), 'Пароль' (redacted), and 'Подтверждение пароля' (redacted). A note at the bottom says: 'Активация Windows' and 'Чтобы активировать Windows, перейдите в Настройки безопасности и активируйте Windows.' A green bar at the bottom says 'Приложение'.

Задание 2: Сводки

Создайте новые вкладки сводки «Чемпионат» и «Дополнительные сводки» в разделе «Сводка»

Сводка

Сводка за последние 7 дней

Динамика нарушений за период

Без учета правил ▾

Добавление новой панели

Название: Чемпионат

Сохранить Отменить

Сводка

Сводка за последние 7 дней

Чемпионат >

Добавление новой панели

Название: Дополнительные сводки

Сохранить Отменить

Задание 3: Виджеты Создайте в сводке 4 виджета:

1. Выборка по событиям краулеров за 3 дня
2. Выборка по политикам с технологиями: графические объекты, печати, эталонные документы за последнюю неделю
3. Статистика по политикам за текущий месяц
4. Топ нарушителей за последние 30 дней

Выберите тип статистики

Динамика нарушений за период

Показывает динамику нарушений в соответствии с выбранными типами нарушений для выбранного временного периода

Добавить виджет

Топ нарушителей

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

Добавить виджет

Количество нарушений за период

Закрыть

Активация Windows
Активизация Windows, перейти

Сводка

+ Сводка за последние 7 дней Чемпионат X Дополнительные сводки

Общие настройки виджета

Название:	Топ нарушителей
Интервал обновления:	Каждые 15 минут
Период:	Последние 30 дней
Количество нарушителей:	10
Группы:	Введите название группы
Статусы:	Выберите статус
<input type="button" value="Сохранить"/> <input type="button" value="Отменить"/>	

Сводка События Отчеты Технологии ▾ Объекты защиты Персоны Политики Еще ▾ Помощь Поиск событий iwtm-officer ▾

Добавить виджет Выгрузить

Сводка

+ Сводка за последние 7 дней
Топ нарушителей
Без учета правил ▾

Для выбранного

Выберите тип статистики

Добавить виджет

Статистика по политикам
Показывает количество нарушений по политикам в разрезе активностей персоны для выбранного периода

Добавить виджет

Статистика по объектам защиты
Показывает количество нарушений по объектам защиты в разрезе уровней нарушений для выбранного периода

Закрыть

Активация Windows
Активируйте Windows, перейдите в раздел "Параметры".



Сводка

+	Сводка за последние 7 дней	Чемпионат ×	Дополнительные сводки
-------------------	----------------------------	-----------------------------	-----------------------

Общие настройки виджета

Название	По политикам
Интервал обновления:	Не обновлять ▾
Период:	Текущий месяц ▾
Политики	Начните вводить текст +
Сохранить Отменить	

Сводка

Выберите тип статистики

Сводка за последние 7 дней

По политикам

Статистика по политикам

Политики

Для выбранного

Добавить виджет

Подборка

Показывает события для выбранной подборки

Добавить виджет

Динамика статусов за период

Показывает динамику статусов для выбранного периода времени

Закрыть

Активация Windows

Активация Windows

чтобы активировать Windows, перенесите "Гарантию Windows"...

Добавить 2

Далее переходим во вкладку «события» и создаем запрос. Выставляем тип запроса — обычный. Удаляем не нужные вкладки и добавляем свои (дата перехвата — последние 3 дня, перехватчик — выбрать краулер.) Пишем сверху название — краулер за 3 дня. Сохраняем.

Во вкладке «сводка» — чемпионат. Выбираем подборку и нажимаем редактировать (маленькая стрелочка вниз в правом верхнем углу виджета). Выбираем ранее созданную подборку (краулер за 3 дня) и пишем вверху название «краулер за 3 дня» и сохраняем.

Далее снова переходи во вкладку «события» создаем новый запрос (первые вариант из трех). В запросах удаляем вторую и третью строку, а в первой выставляем — последние 7 дней. и добавляем запрос –технологии. Редактируем этот запрос. Выбираем графические объекты — все, кроме этого также добавляем печати и эталонные документы. Вверху пишем название — Выборка по технологиям. Сохраняем.

Переходим во вкладку «сводка»–чемпионат. Выбираем подборку и редактируем. Название — выборка по технологиям. выбираем созданную подборку — выборка по технологиям и сохраняем.

Задание 4

Необходимо создать виджет в разделе сводка во вкладке «Дополнительные сводки» отображающий события с высоким уровнем угрозы на правила копирования за последние 7 дней.

Зафиксировать скриншотом конструктора выборки.

Задание 5

Необходимо создать виджет в разделе «Сводка», вкладка «Дополнительные сводки» для отображения нарушений только от обоих компьютеров нарушителей (виртуальных машин) со средним и высоким уровнем угрозы за последние 3 дня.

Зафиксировать скриншотом конструктор выборки.