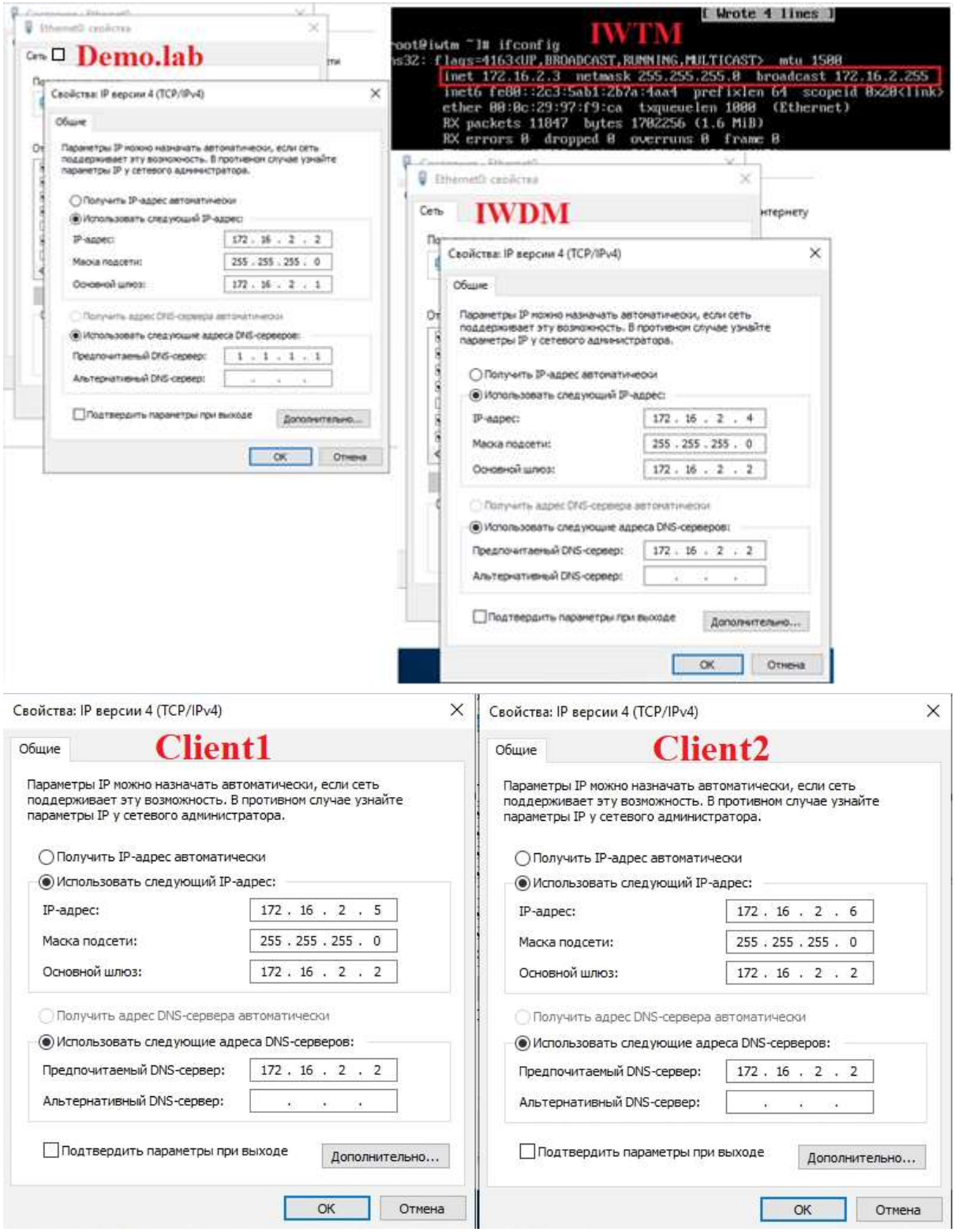
IP-адреса Demo.lab, IWTM, IWDM, Client1, Client2



Задание 1: Настройка контроллера домена

Для удобства работы рекомендуется создать подразделение “Champ” в
корневом каталоге оснастки “Пользователи и компьютеры” AD сервера.

Внутри созданного подразделения “Champ” необходимо создать и настроить
следующих доменных пользователей с соответствующими правами:

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

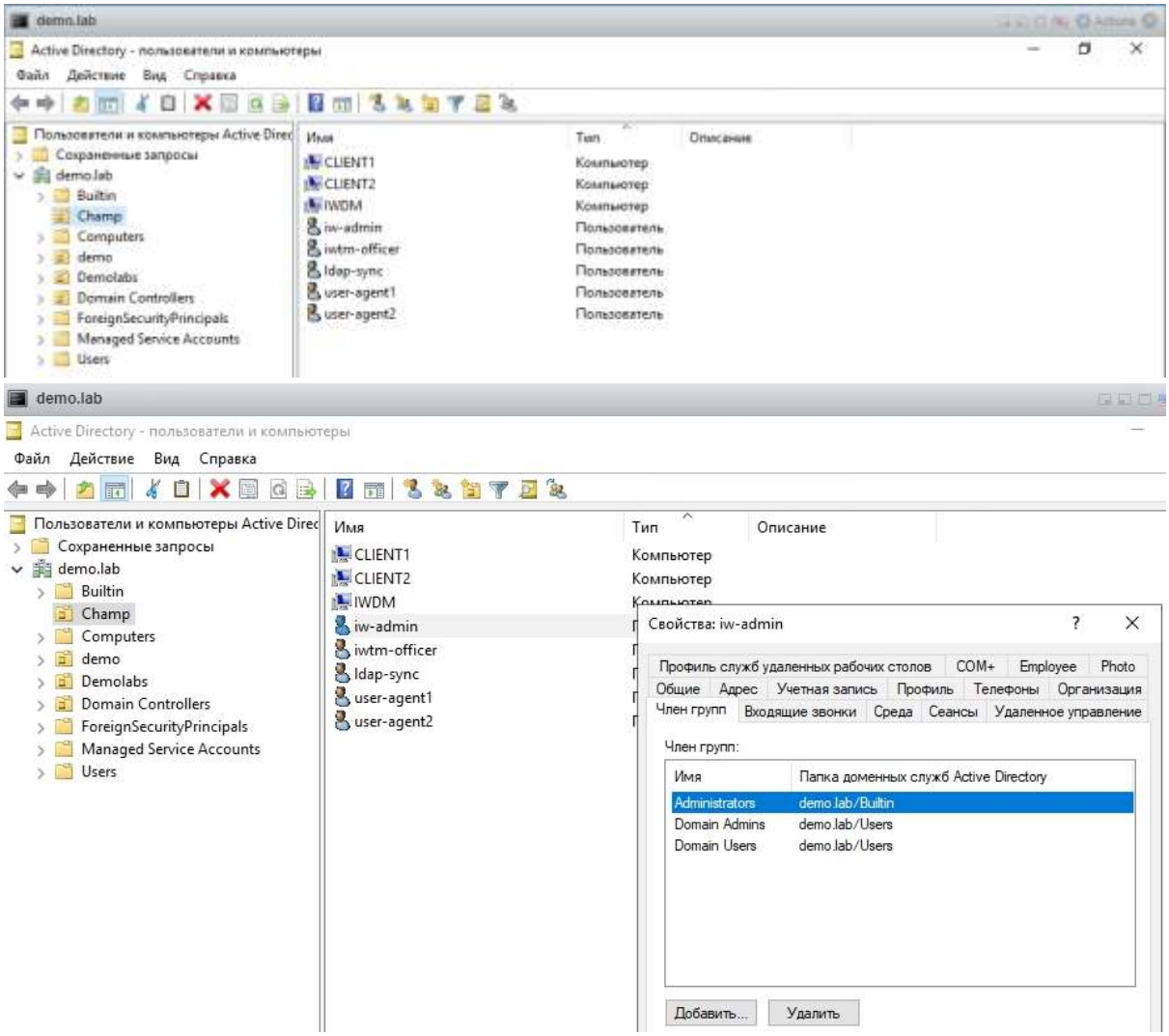
Логин: user-agent2, пароль: xxXX1234, права пользователя домена

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

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

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

Создаем пользователей и добавляем администратору права – Администратора, Администратора Домена (Domain Admin)



Задание 2: Настройка DLP сервера

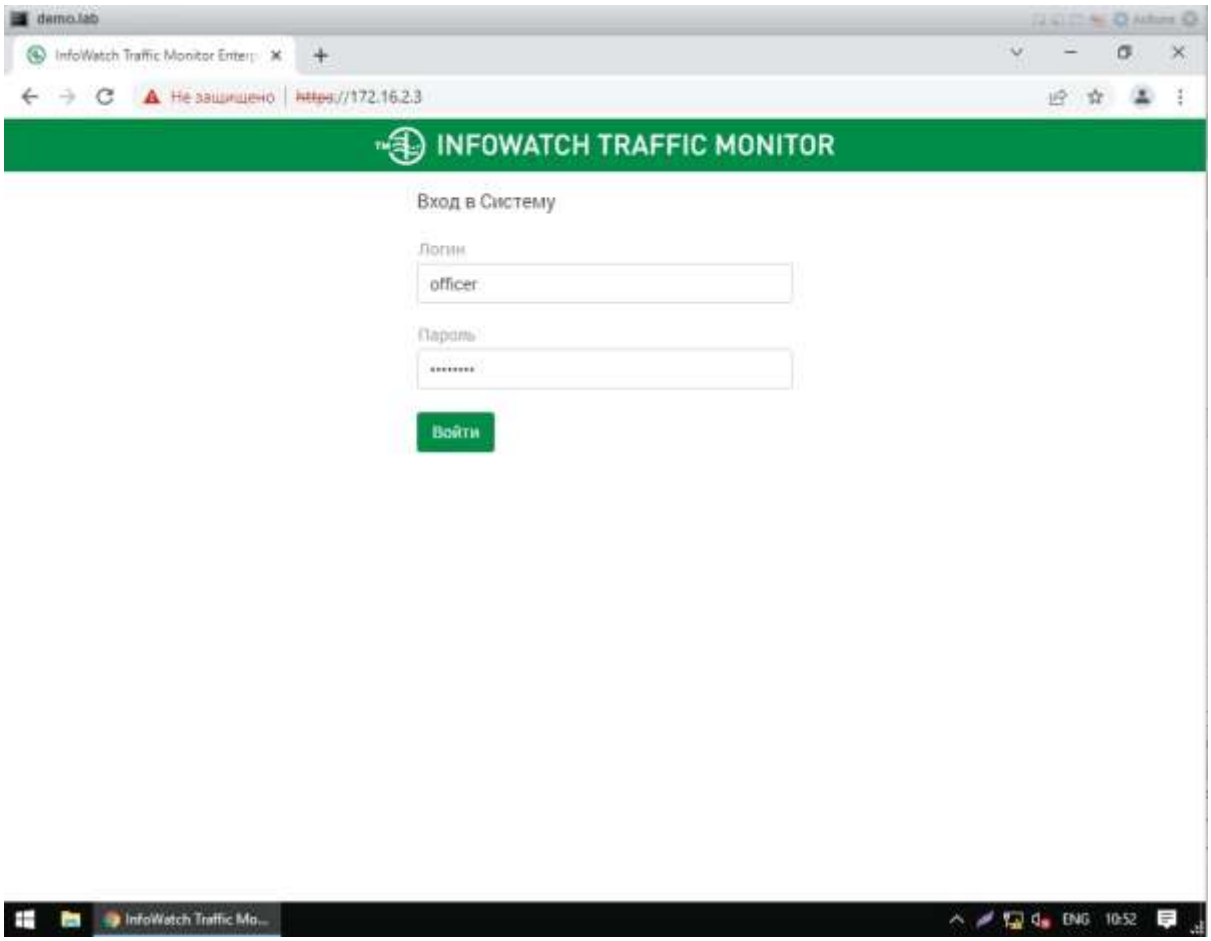
DLP-сервер контроля сетевого трафика уже предустановлен, но не

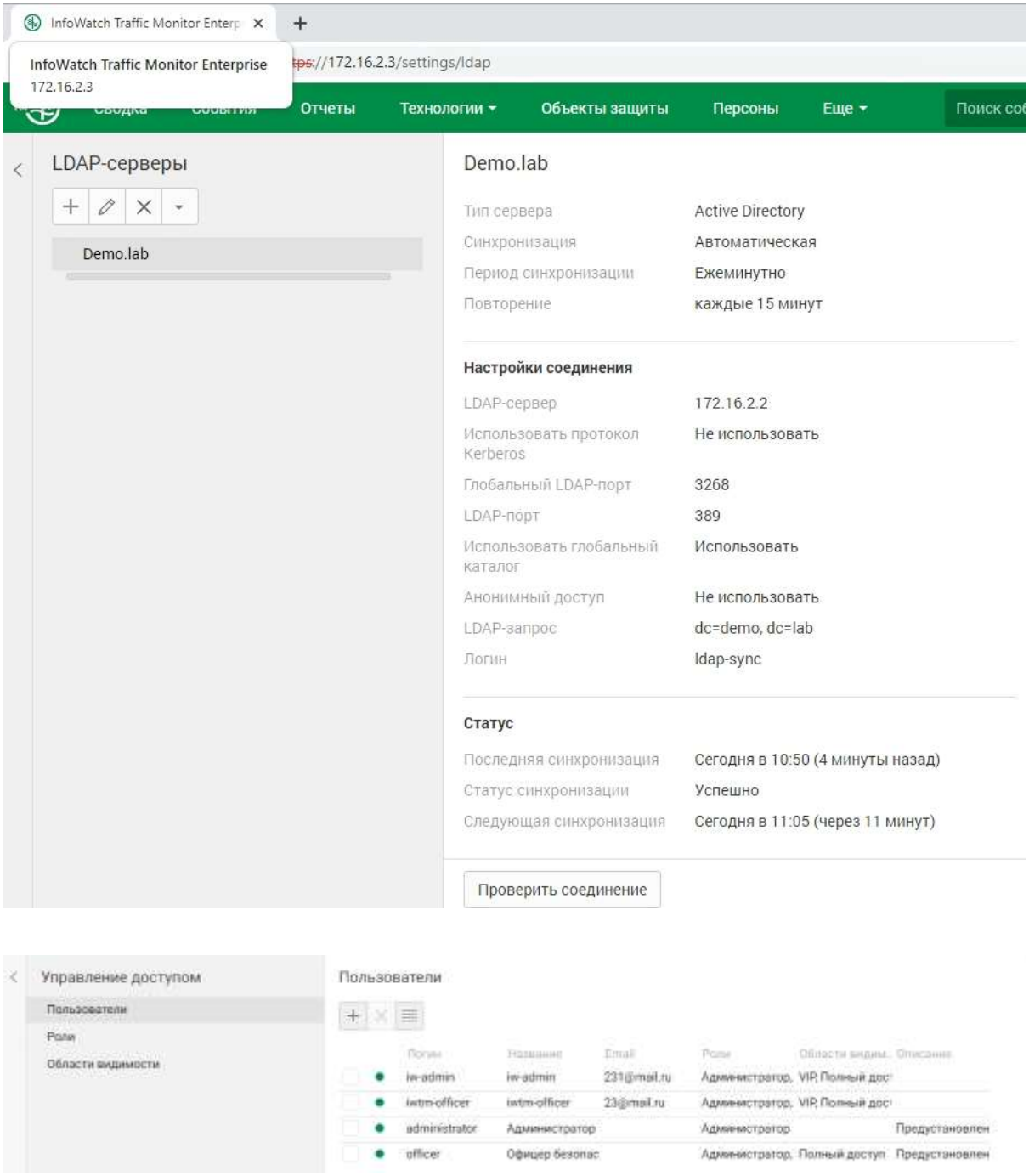
настроен.

Необходимо синхронизировать каталог пользователей и компьютеров
LDAP с домена с помощью ранее созданного пользователя ldap-sync.

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

Запишите IP-адреса, токен, логины и пароли от учетных записей, а также
все прочие нестандартные данные (измененные вами) вашей системы в текстовом
файле «отчет.txt» на рабочем столе компьютера.





Задание 3: Установка и настройка сервера агентского мониторинга

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

Установить базу данных PostgreSQL с паролем суперпользователя xxXX1234.

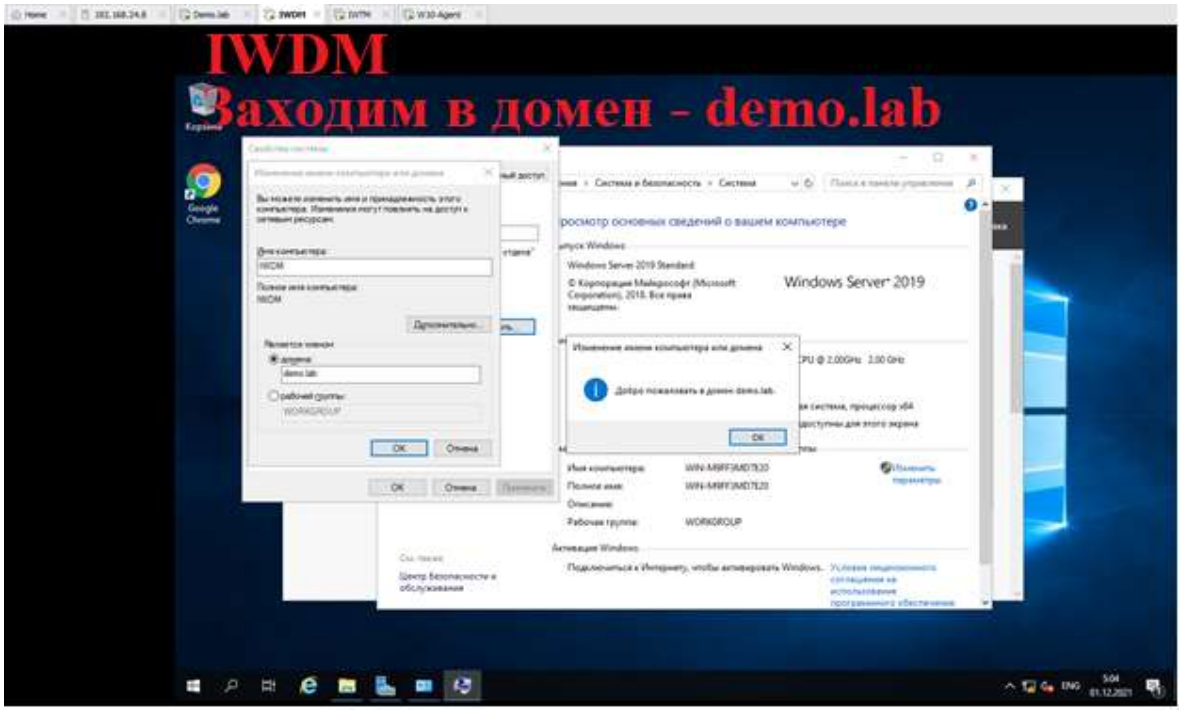
Установить сервер агентского мониторинга с параметрами по умолчанию, подключившись к ранее созданной БД.

При установке сервера агентского мониторинга необходимо установить соединение с DLP-сервером по IP-адресу и токену, но можно сделать это и после установки. При установке настроить локального пользователя консоли
управления: officer с паролем xxXX1234

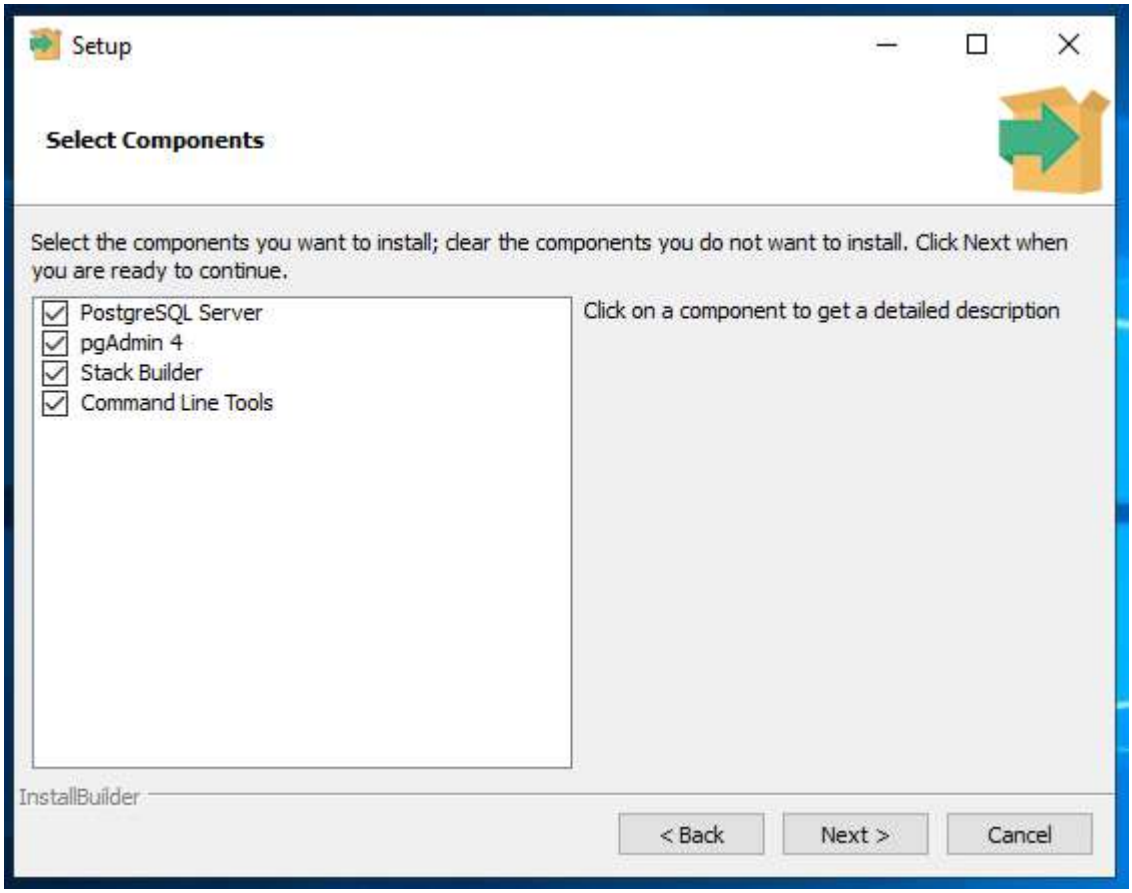
Синхронизировать каталог пользователей и компьютеров с Active Directory.

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

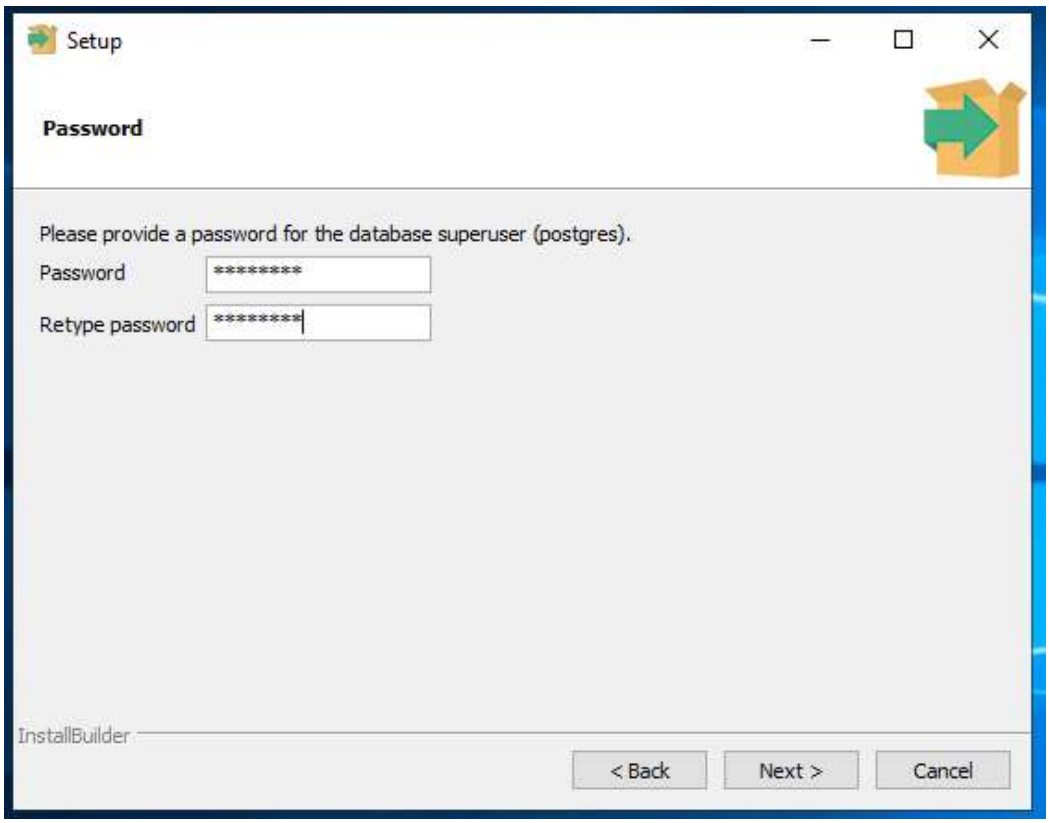
Проверить работоспособность входа в консоль управления без ввода пароля. Если сервер не введен в домен или работает от другого пользователя,
данная опция работать не будет.



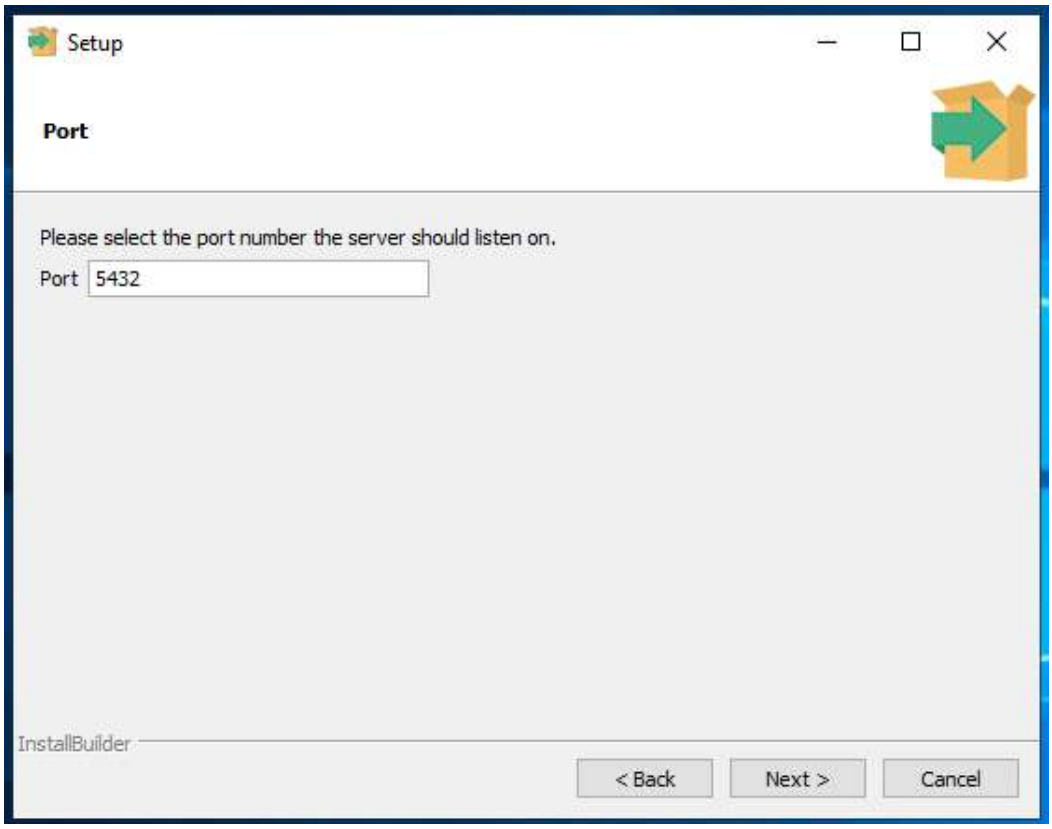
После перезагрузки заходим под iw-admin (без стак билдера)



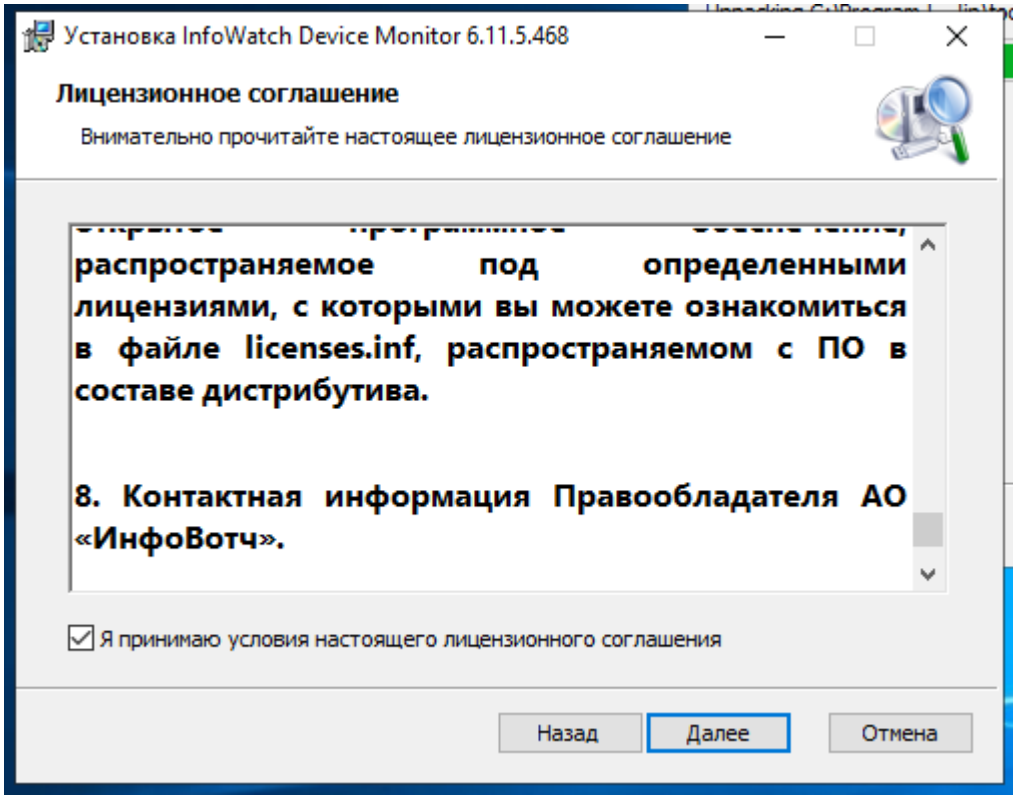
Вводим стандартный пароль



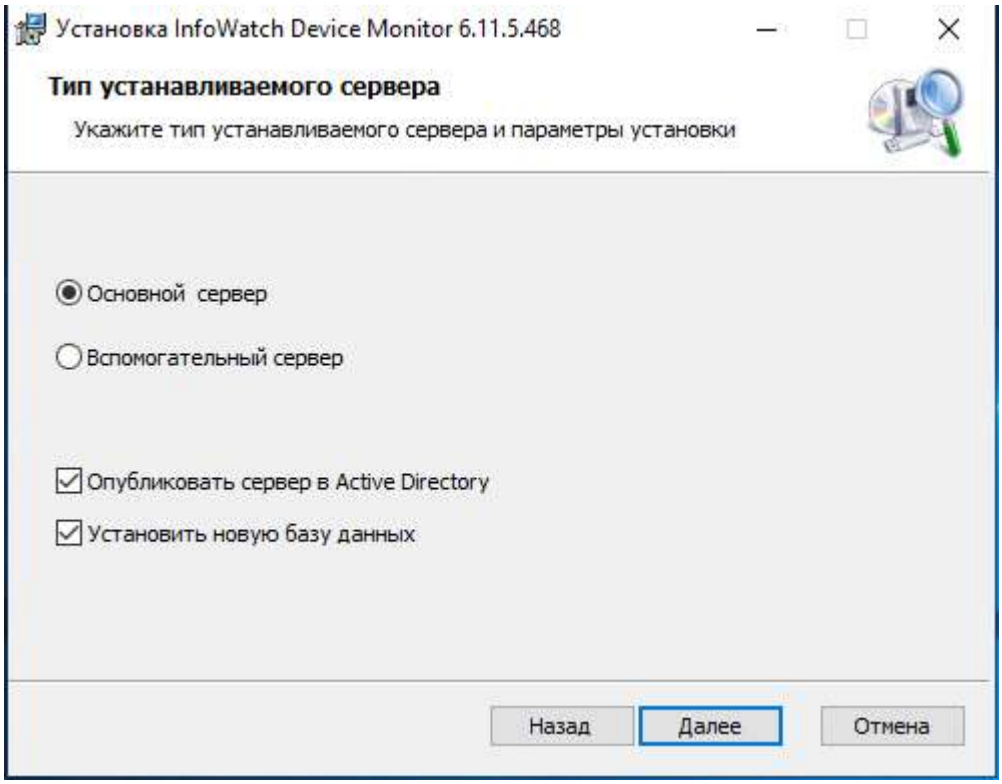
Порт оставляем по умолчанию

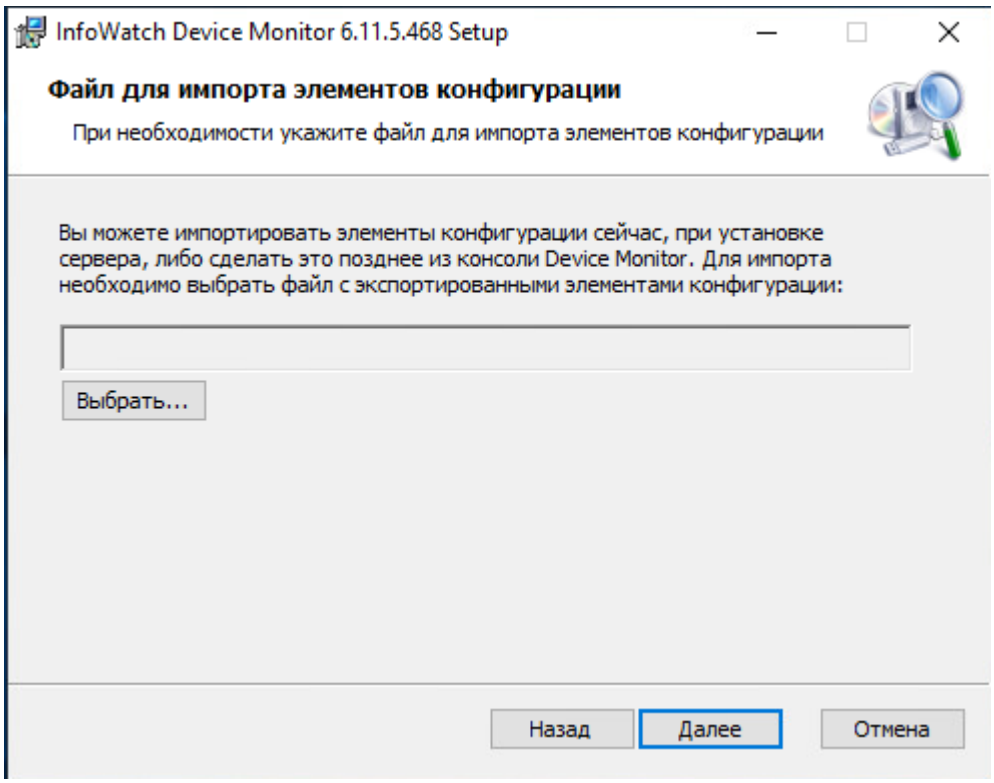


Затем, переходим к установке InfoWatch Device Monitor

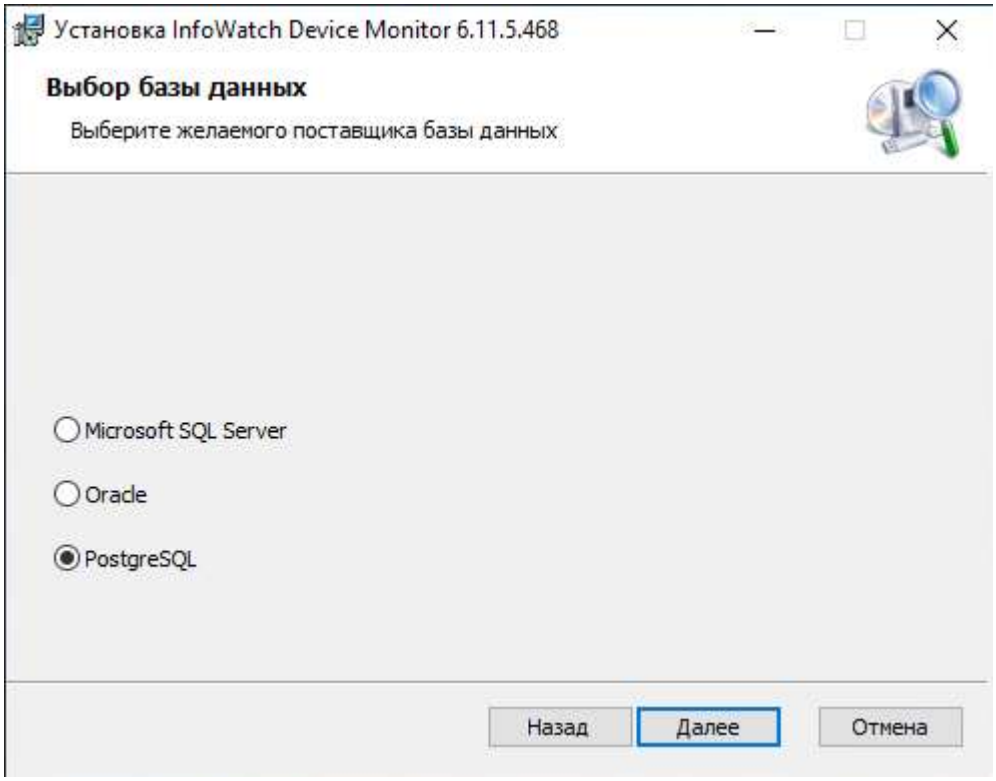


Оставляем галочку на основном сервере

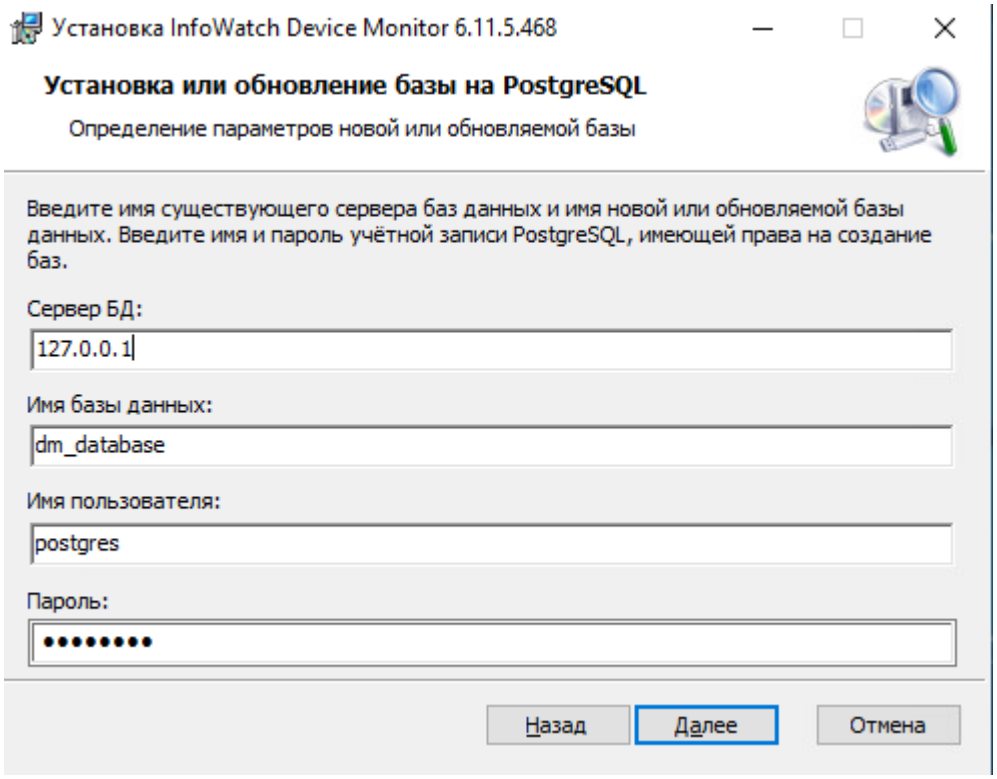




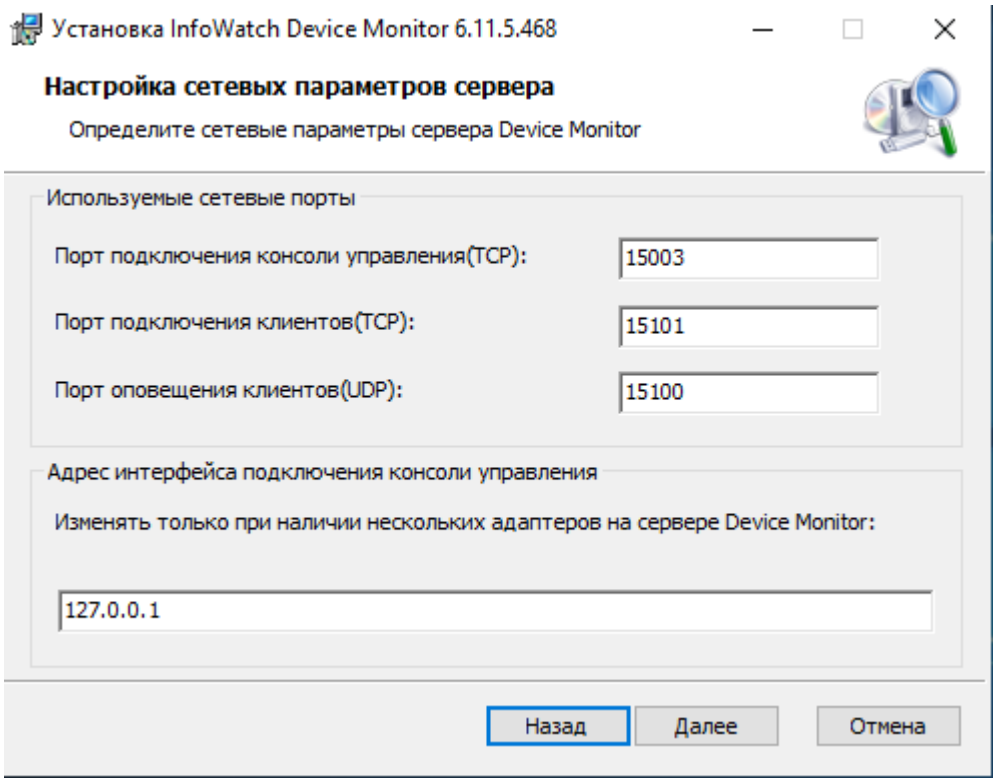
Выбираем базу данных, в нашем случае будет - PostgresSQL



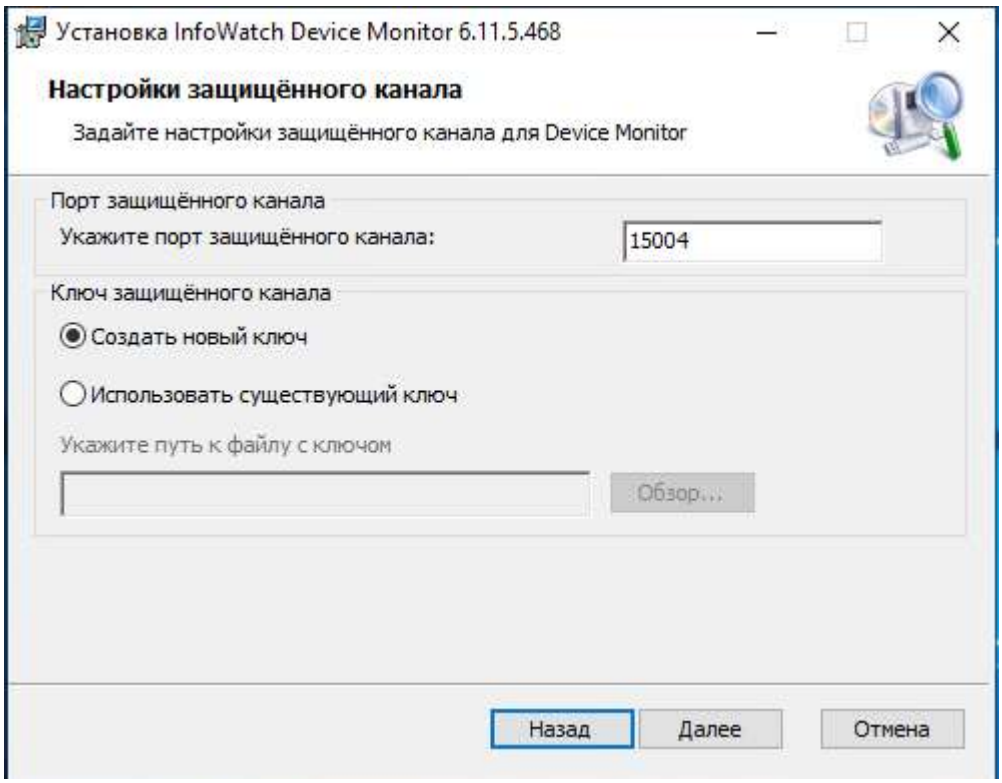
Задаем сервер БД – 127.0.0.1; Имя БД – dm_database, имя пользователя – postgres и стандартный пароль



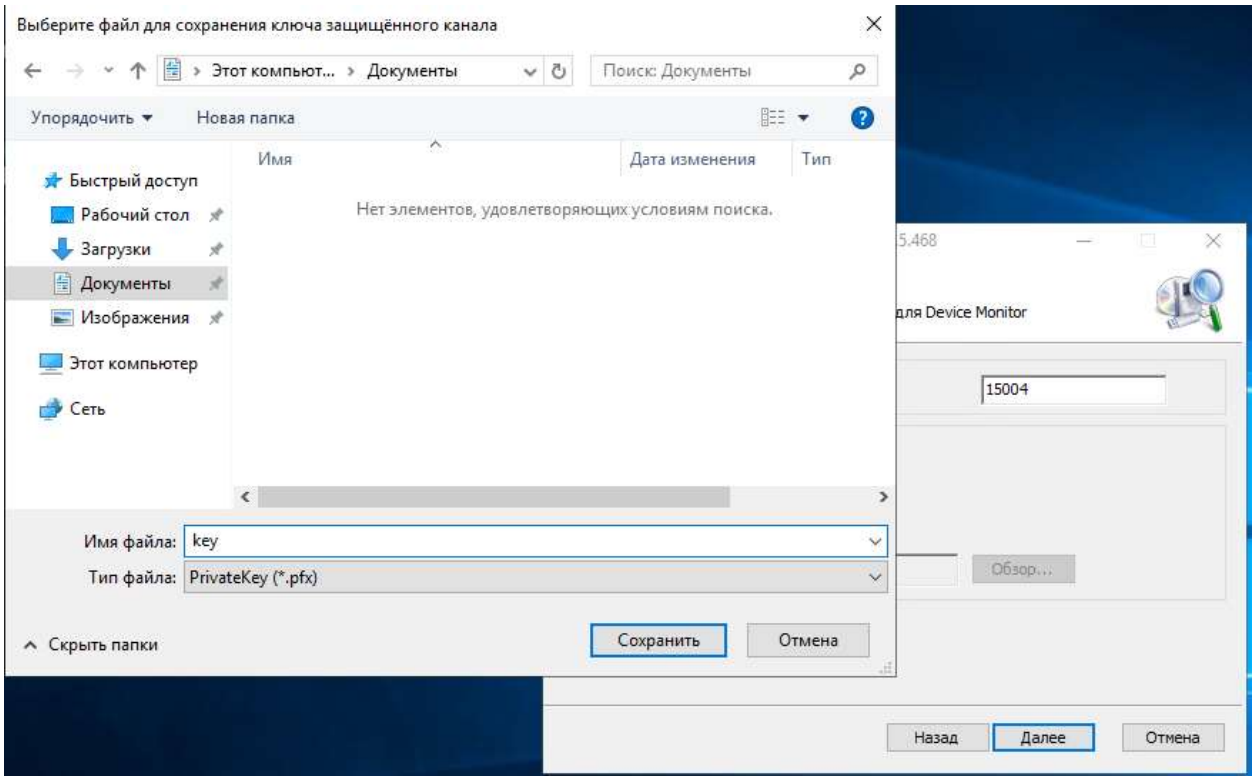
Настраиваем сетевые параметры



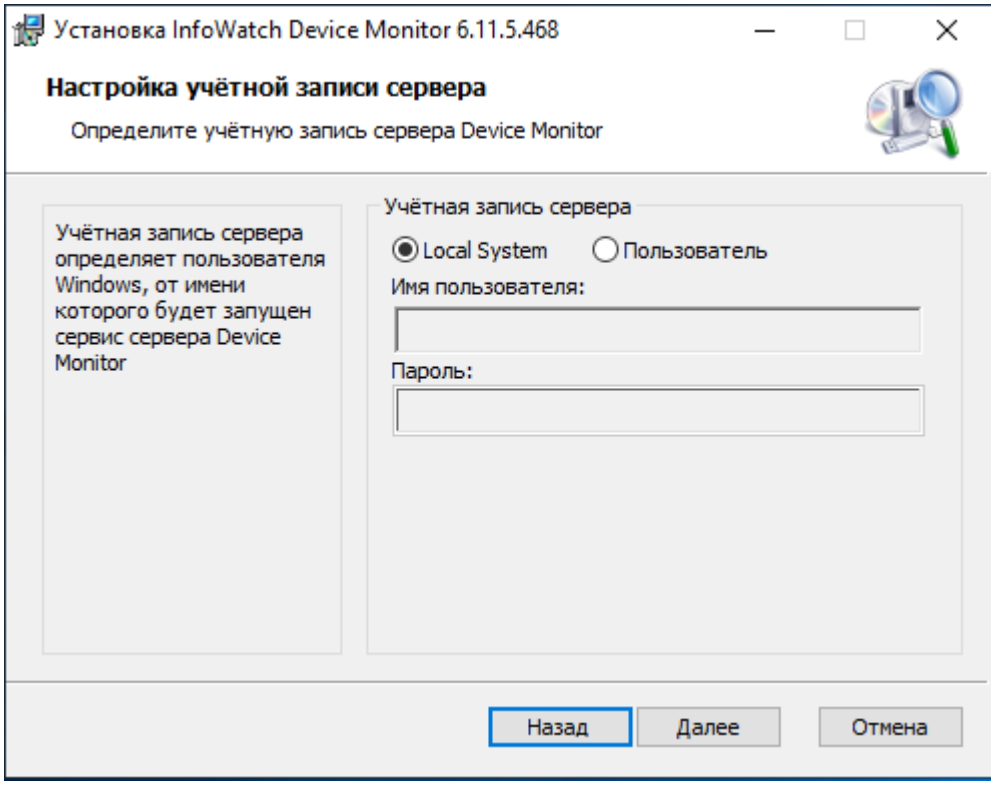
Настраиваем защищённый канал и создаём новый ключ



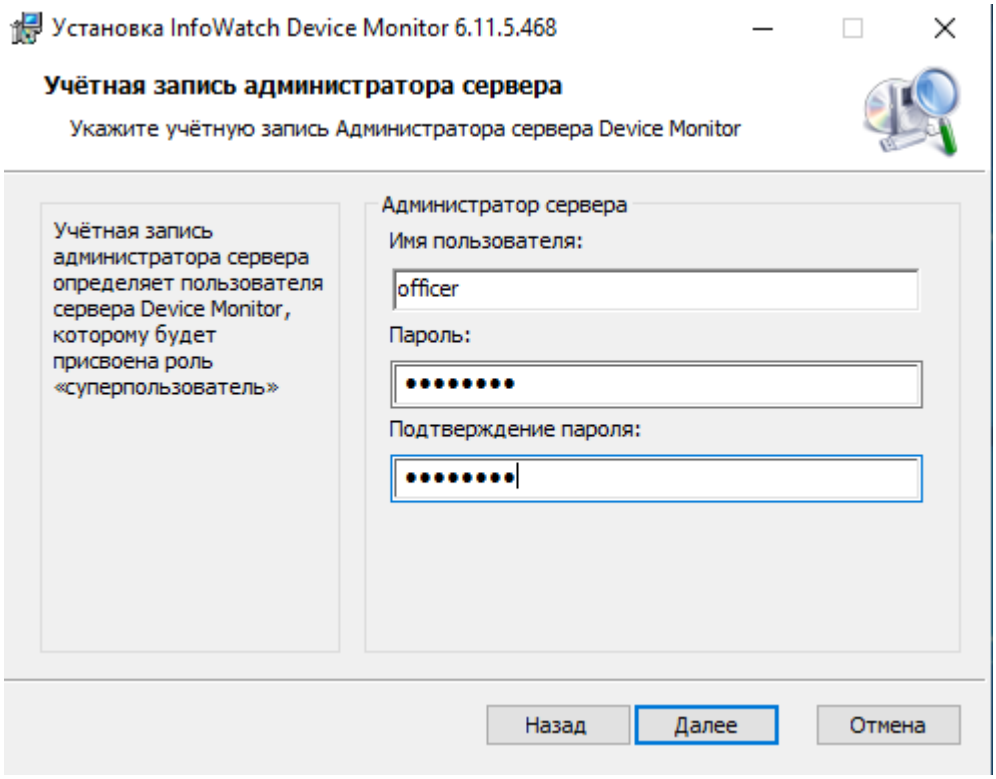
Сохраняем ключ



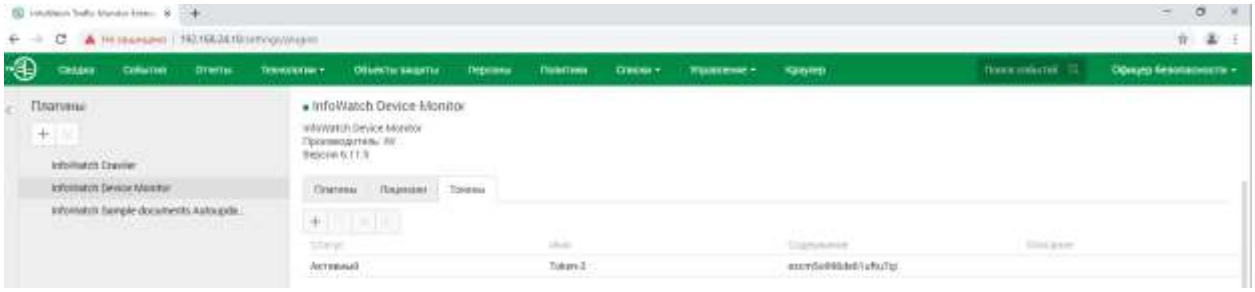
Оставляем локальную учётную запись



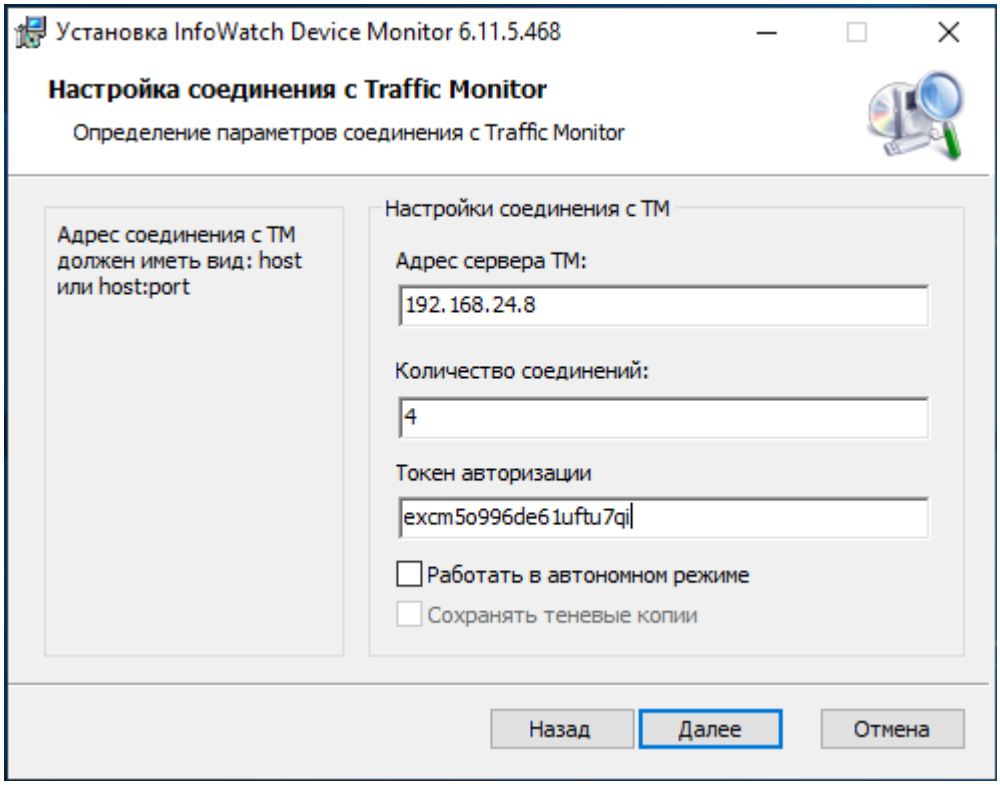
Вводим логин и пароль администратора



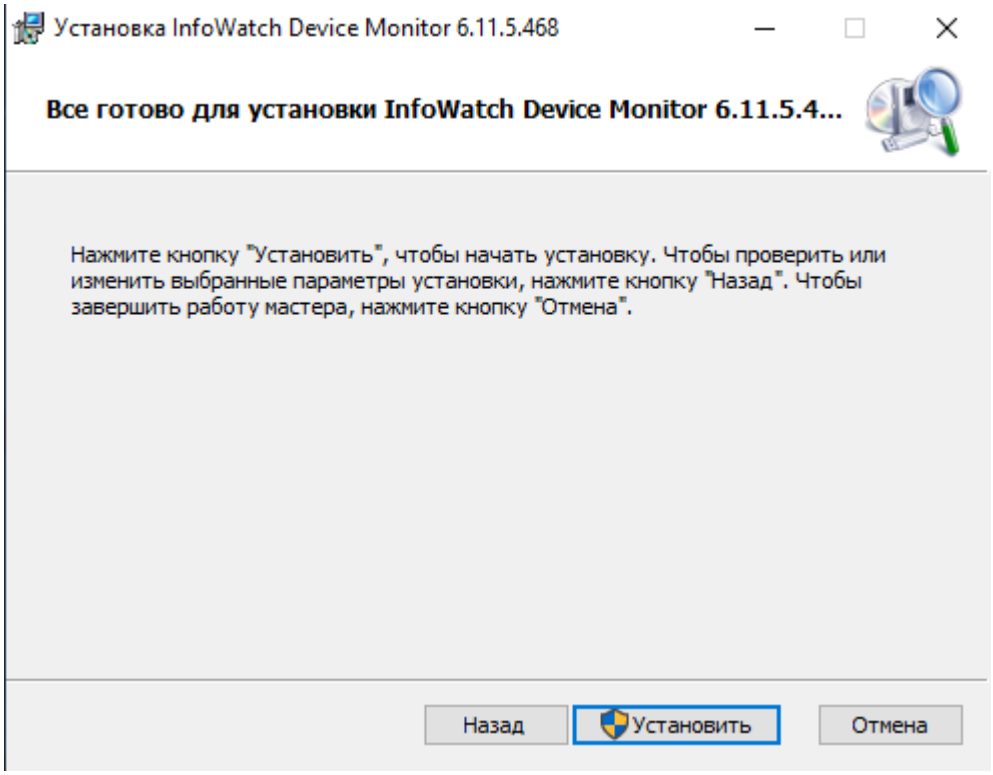
Сморим токен



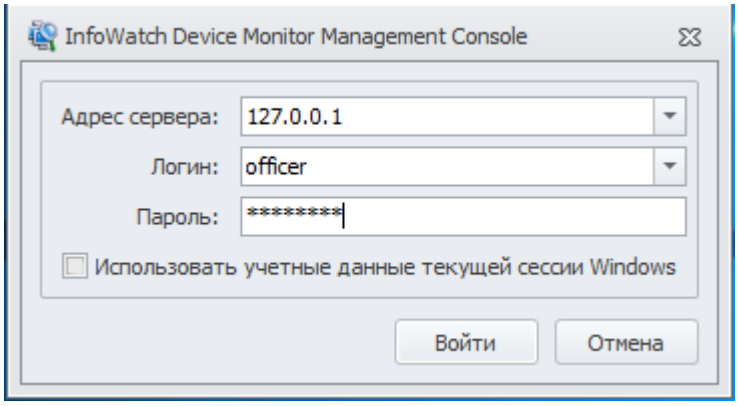
Указываем Ip-адрес IWTM и токен (который только что посмотрели в трафик мониторе)



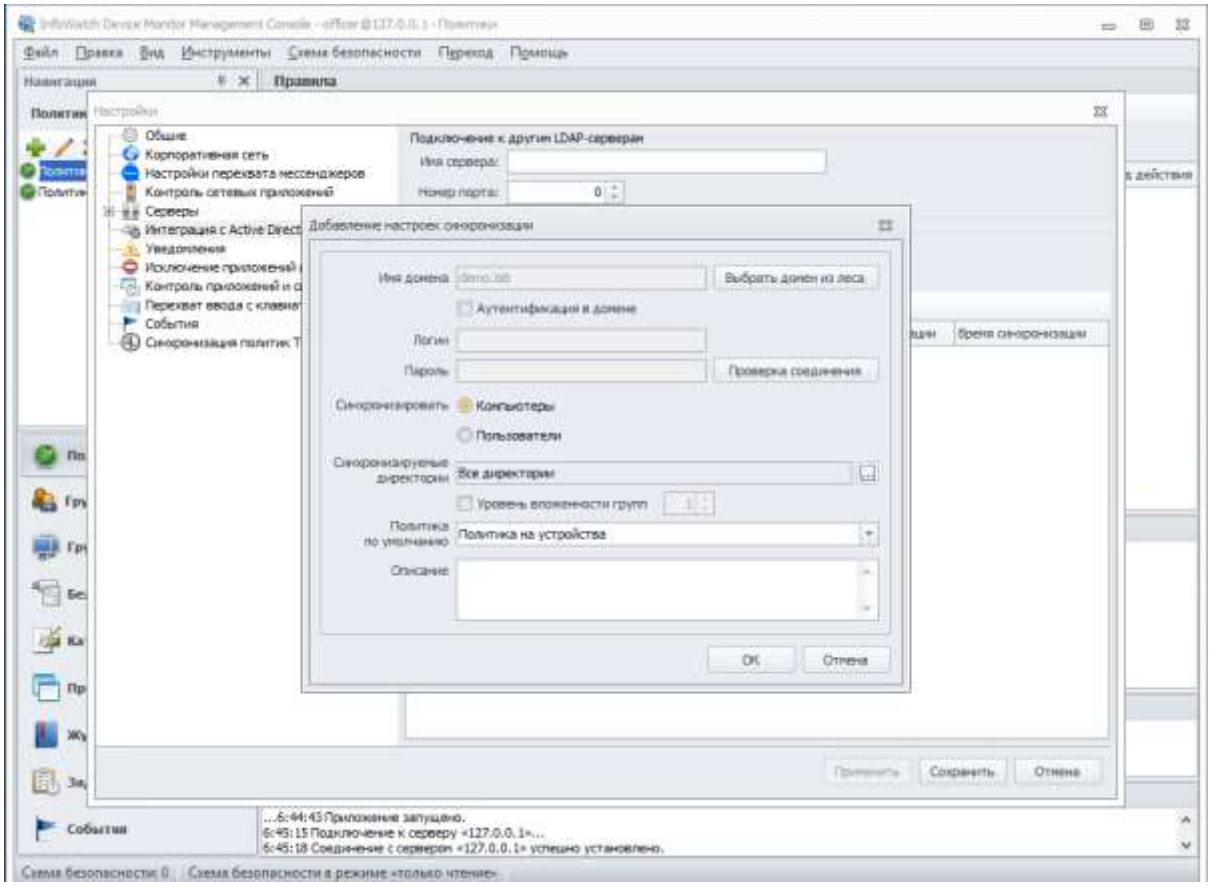
Устанавливаем



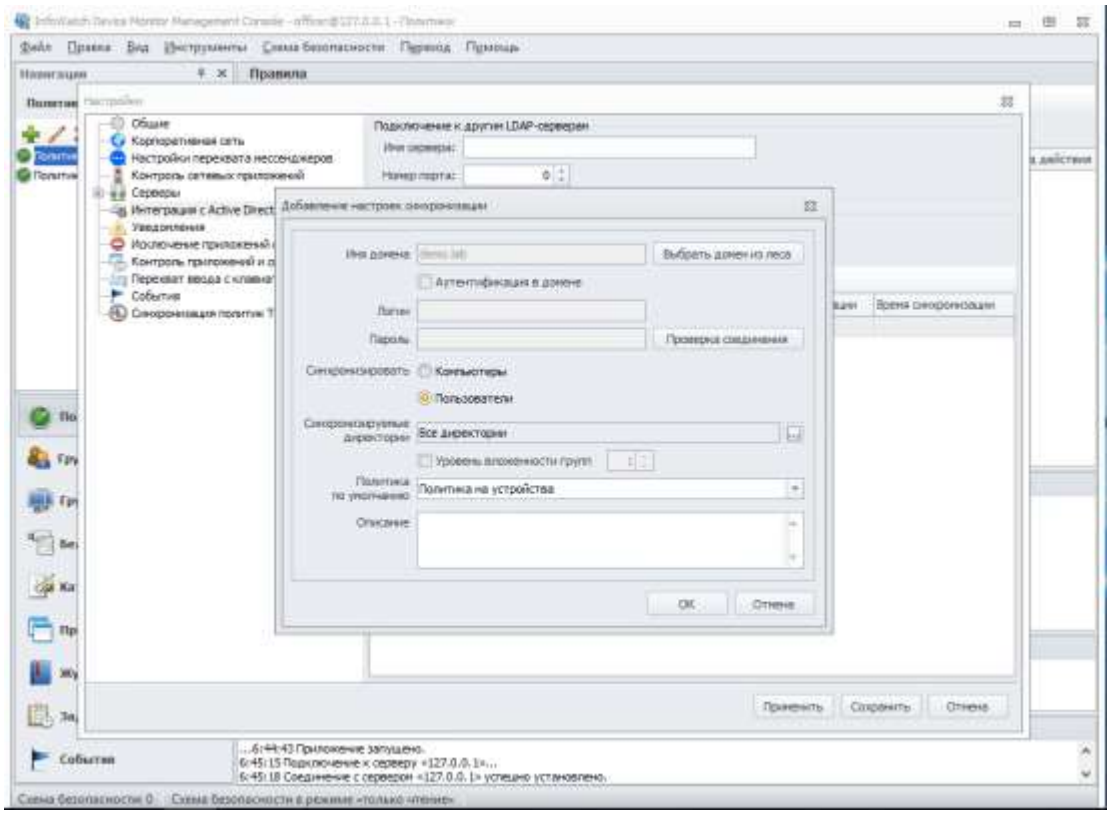
Подключаемся к InfoWatch Device Monitor Management Console



Синхронизуем компьютеры

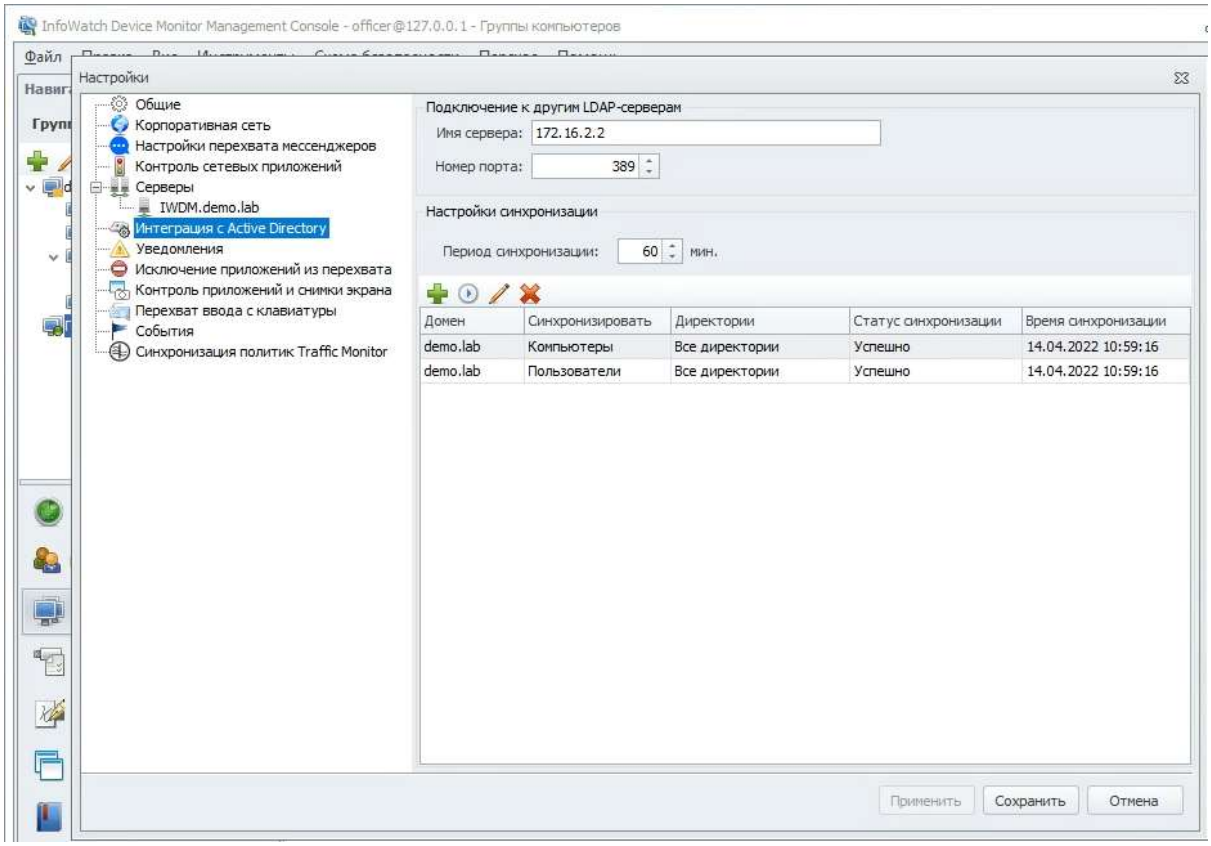


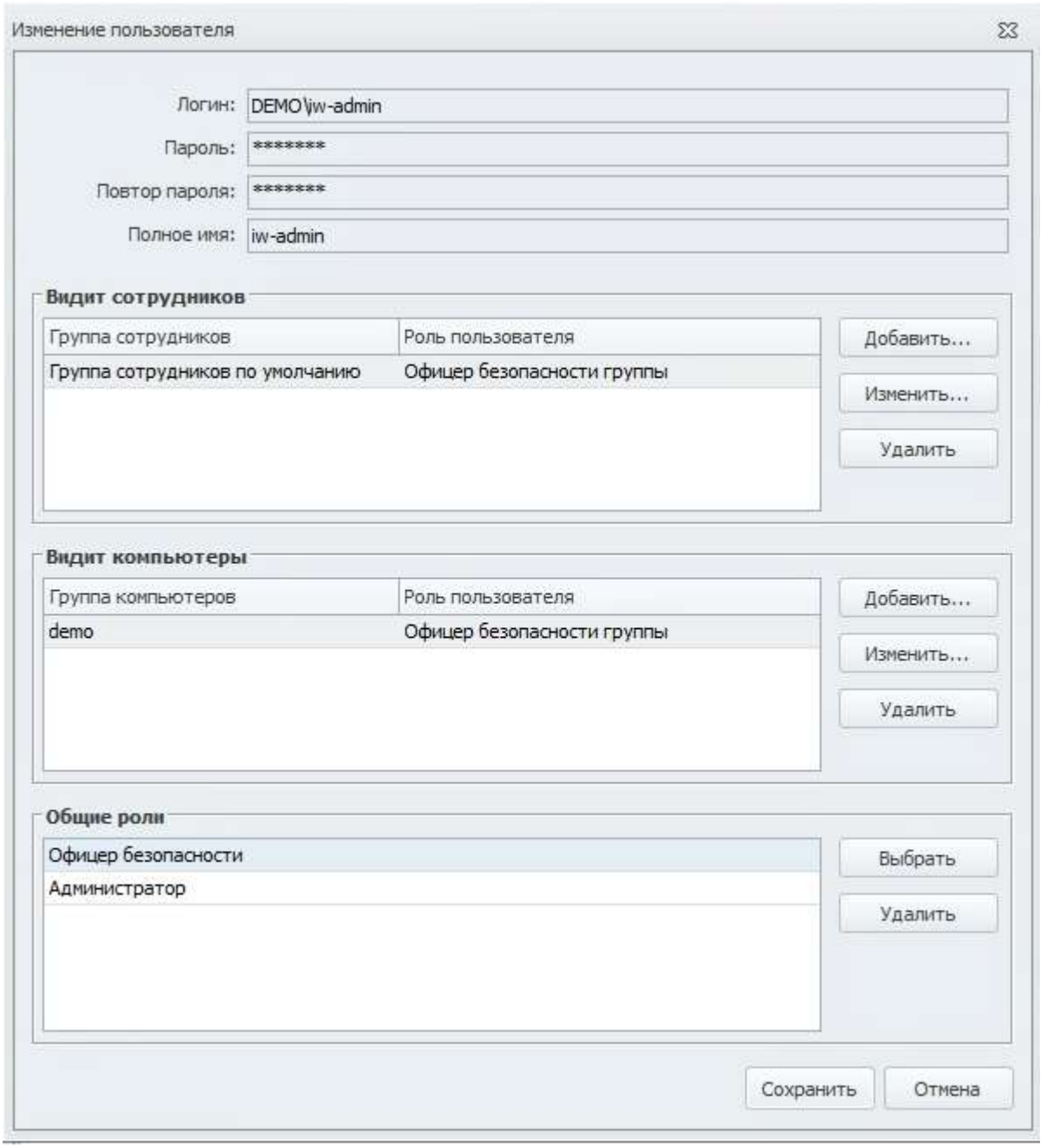
Синхронизуем пользователей

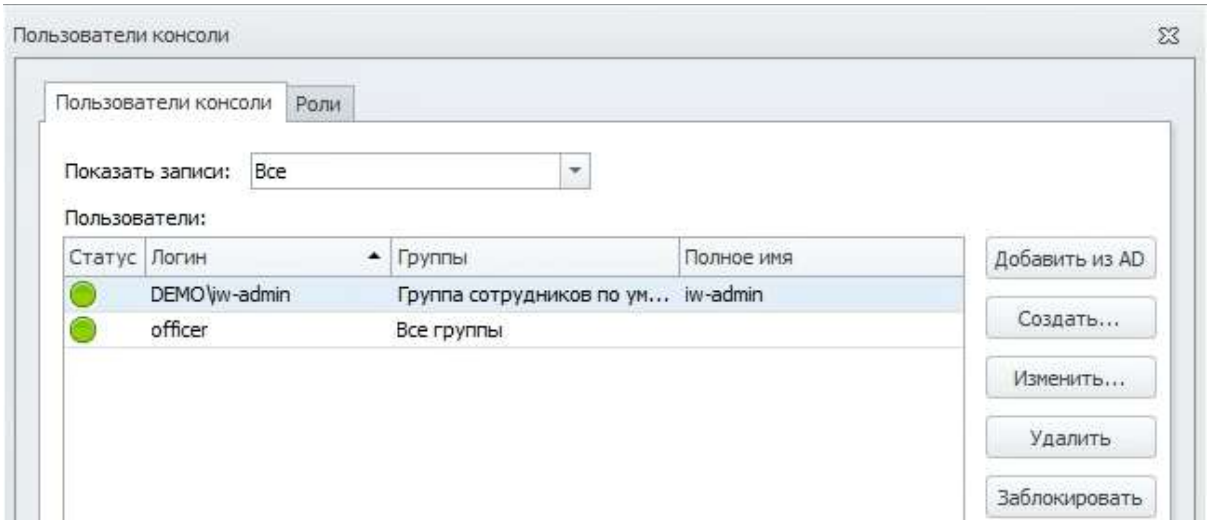


Указываем Ip-адрес сервера demo.lab и порт

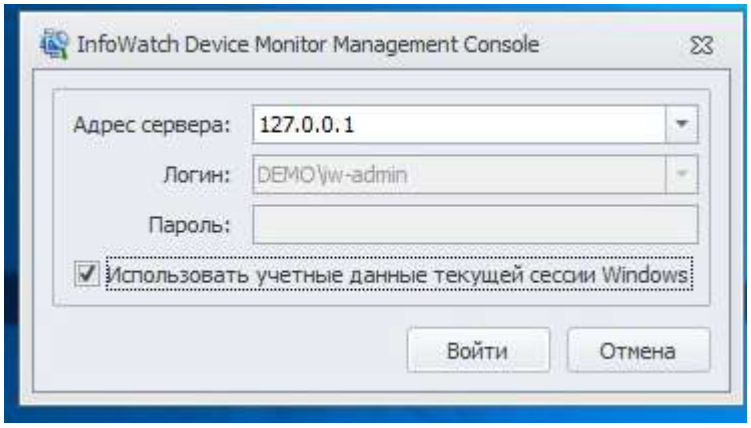
Синхронизация у компьютеров и пользователей


InfoWatch Device Monitor Management Console - officer@127.0.0.1 - Группы компьютеров
Файл
Настройки
Общие
Корпоративная сеть
Настройки перехвата мессенджеров
Контроль сетевых приложений
Серверы
IWDM.demo.lab
Интеграция с Active Directory
Уведомления
Исключение приложений из перехвата
Контроль приложений и снимки экрана
Перехват ввода с клавиатуры
События
Синхронизация политик Traffic Monitor
Подключение к другим LDAP-серверам
Имя сервера: 172.16.2.2
Номер порта: 389
Настройки синхронизации
Период синхронизации: 60 мин.
Домен | Синхронизировать | Директории | Статус синхронизации | Время синхронизации
demo.lab | Компьютеры | Все директории | Успешно | 14.04.2022 10:59:16
demo.lab | Пользователи | Все директории | Успешно | 14.04.2022 10:59:16
Применить
Сохранить
Отмена


Изменение пользователя
Логин: DEMO\jw-admin
Пароль: *******
Повтор пароля: *******
Полное имя: iw-admin
Видит сотрудников
Группа сотрудников
Роль пользователя
Группа сотрудников по умолчанию
Офицер безопасности группы
Добавить...
Изменить...
Удалить
Видит компьютеры
Группа компьютеров
Роль пользователя
demo
Офицер безопасности группы
Добавить...
Изменить...
Удалить
Общие роли
Офицер безопасности
Администратор
Выбрать
Удалить
Сохранить
Отмена


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

Настройка беспарольного входа



Задание 4: Установка агента мониторинга на машине нарушителя

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

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

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

Установить агент мониторинга:

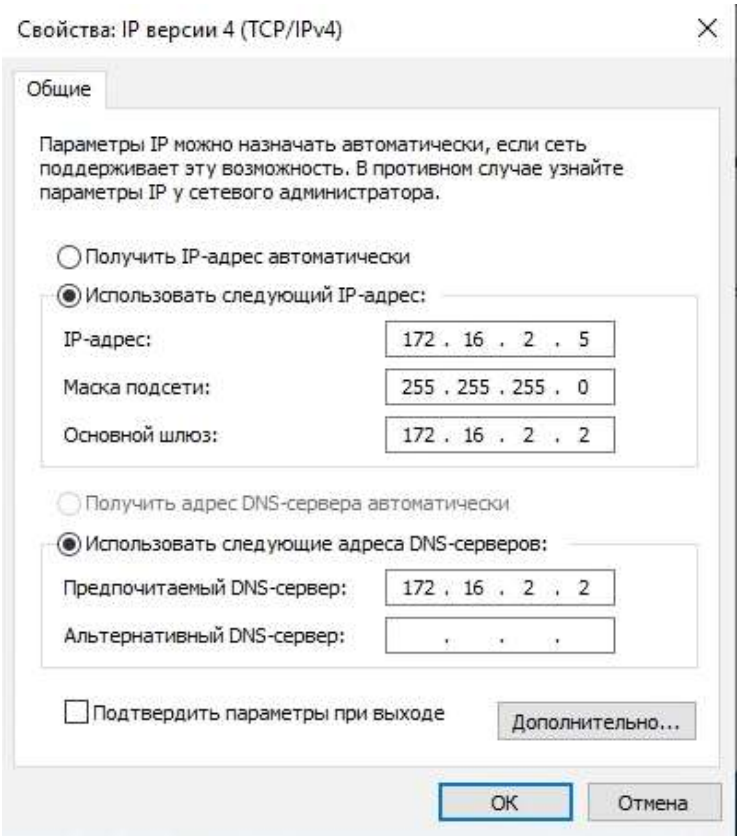
На машину 1 с помощью задачи первичного распространения с сервера агентского мониторинга.

На машину 2 с помощью групповых политик домена.

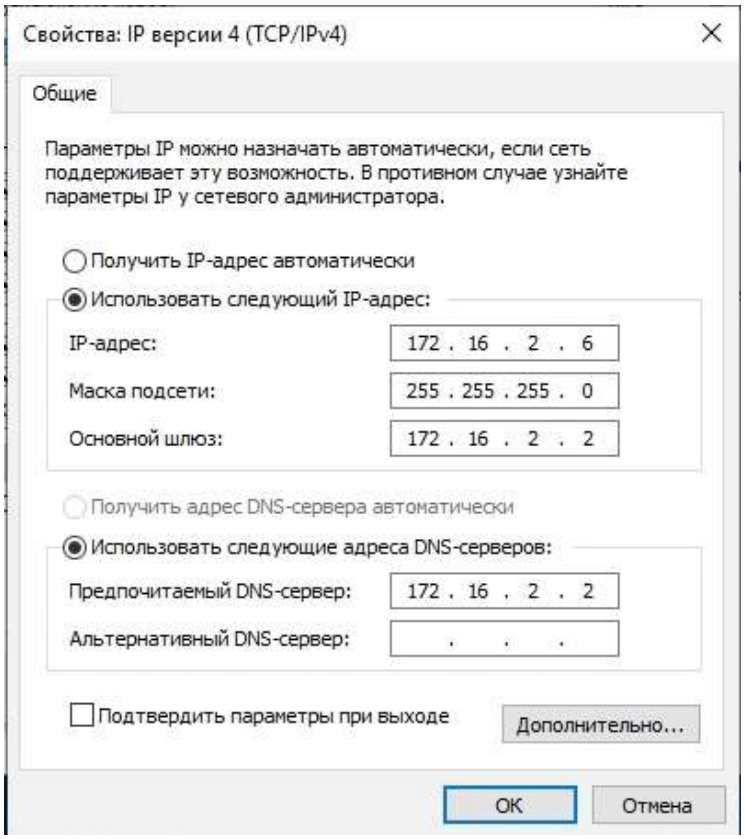
Необходимо создавать отдельные объекты групповых политик на каждое задание и делать снимки экрана для подтверждения создания и выполнения политик.

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

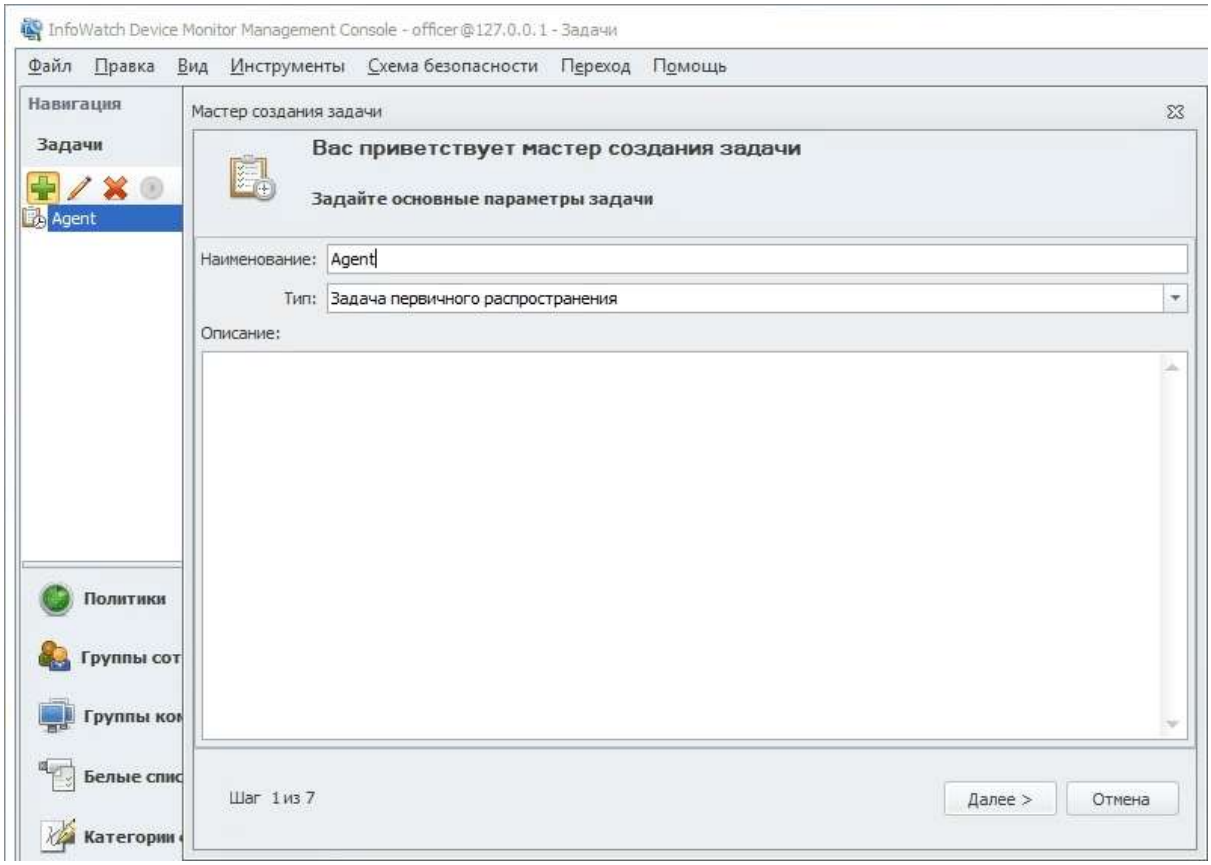
Клиент1



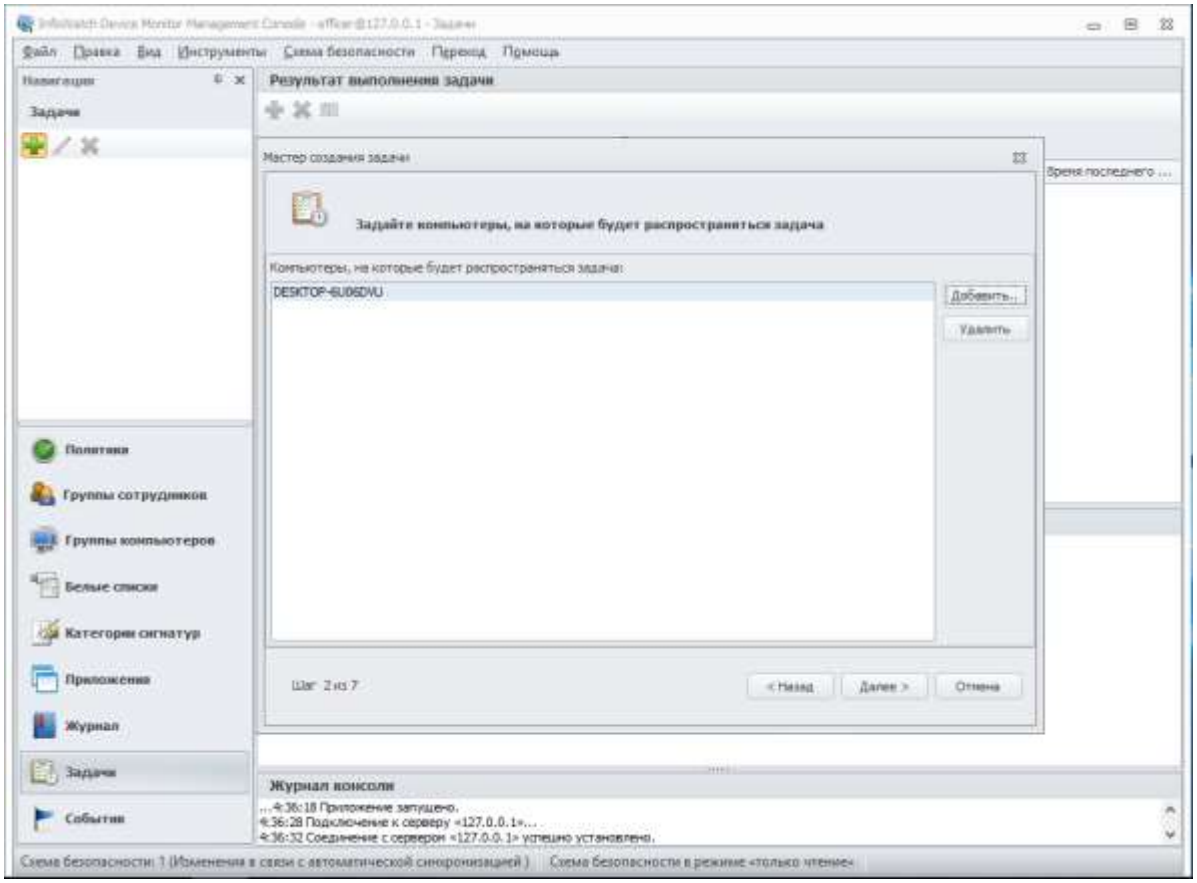
Клиент2



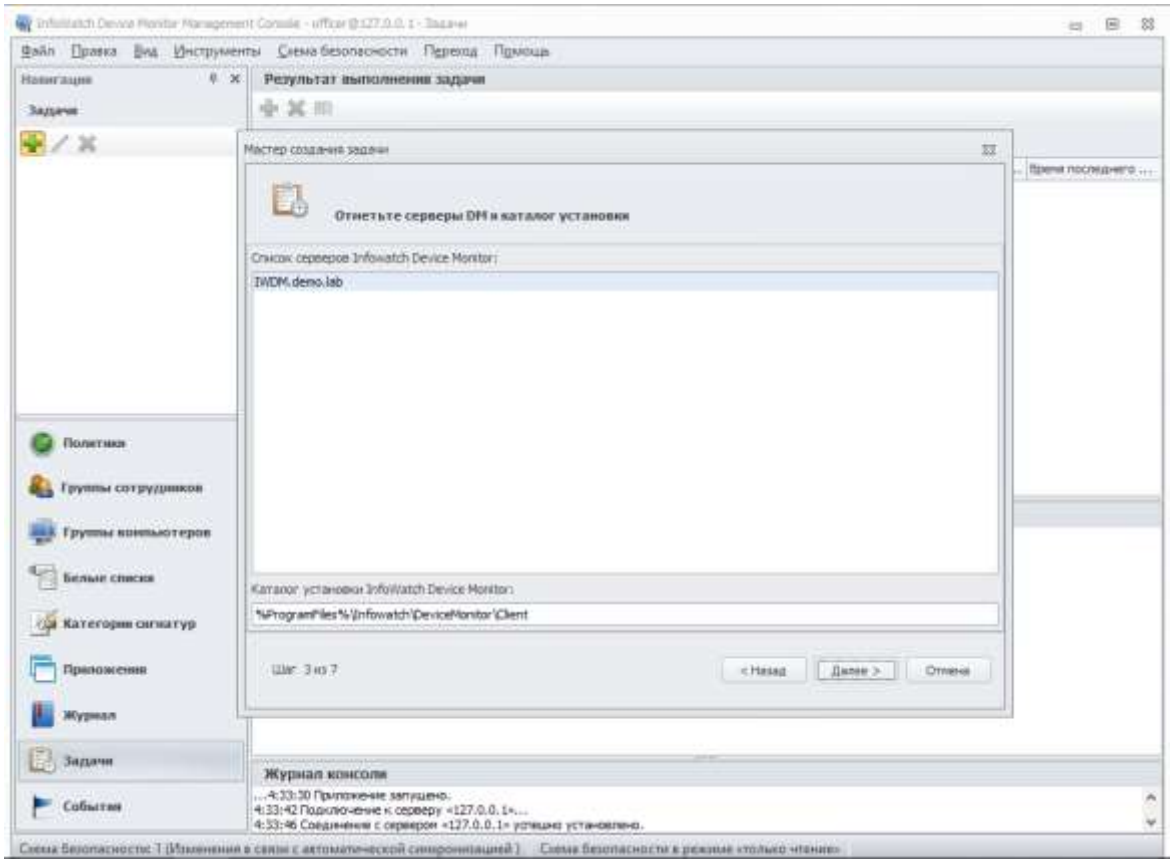
Создаем новую задачу

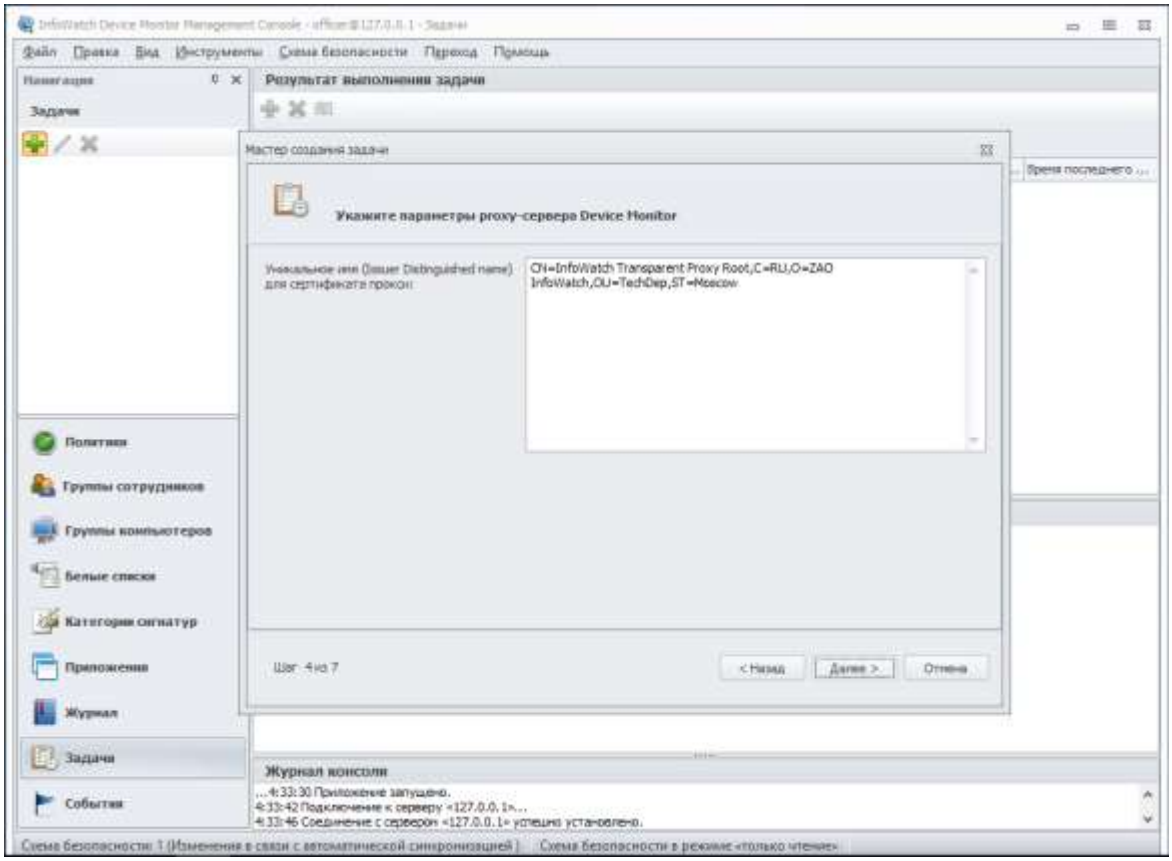


Выбираем компьютер агента

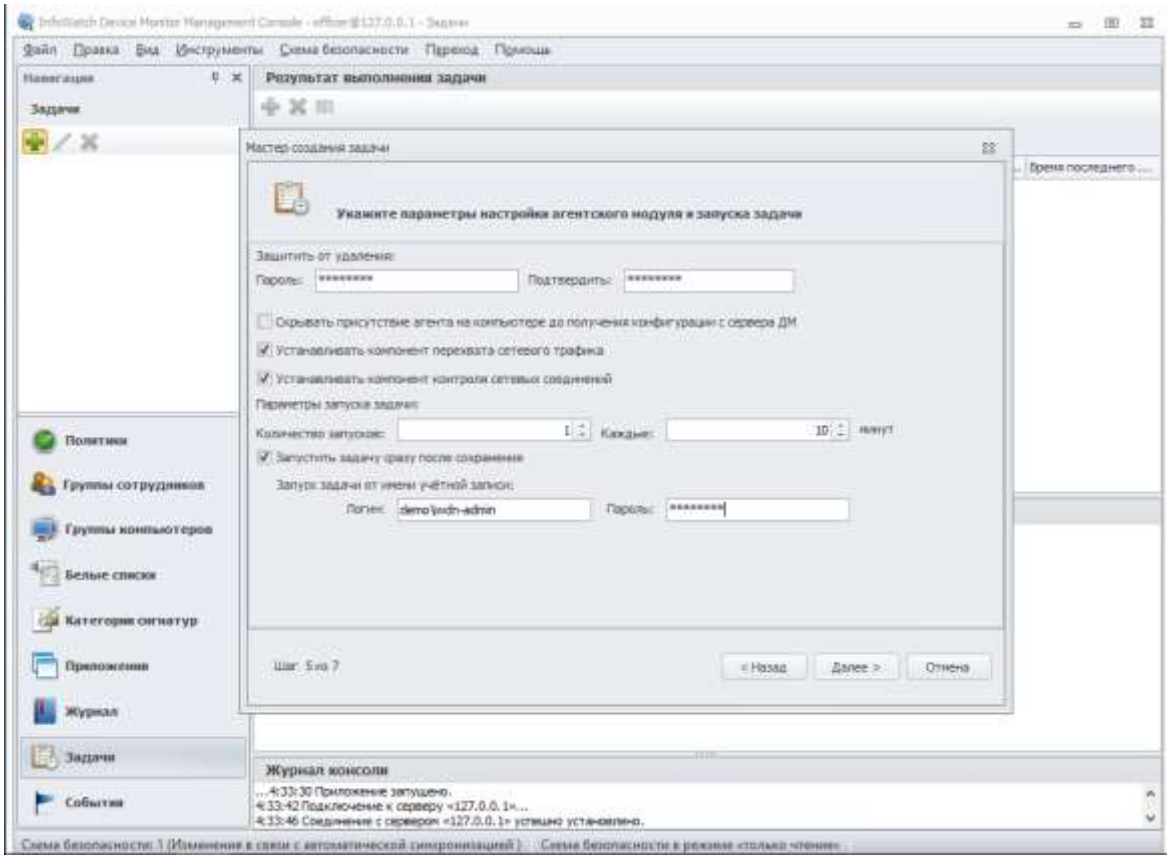


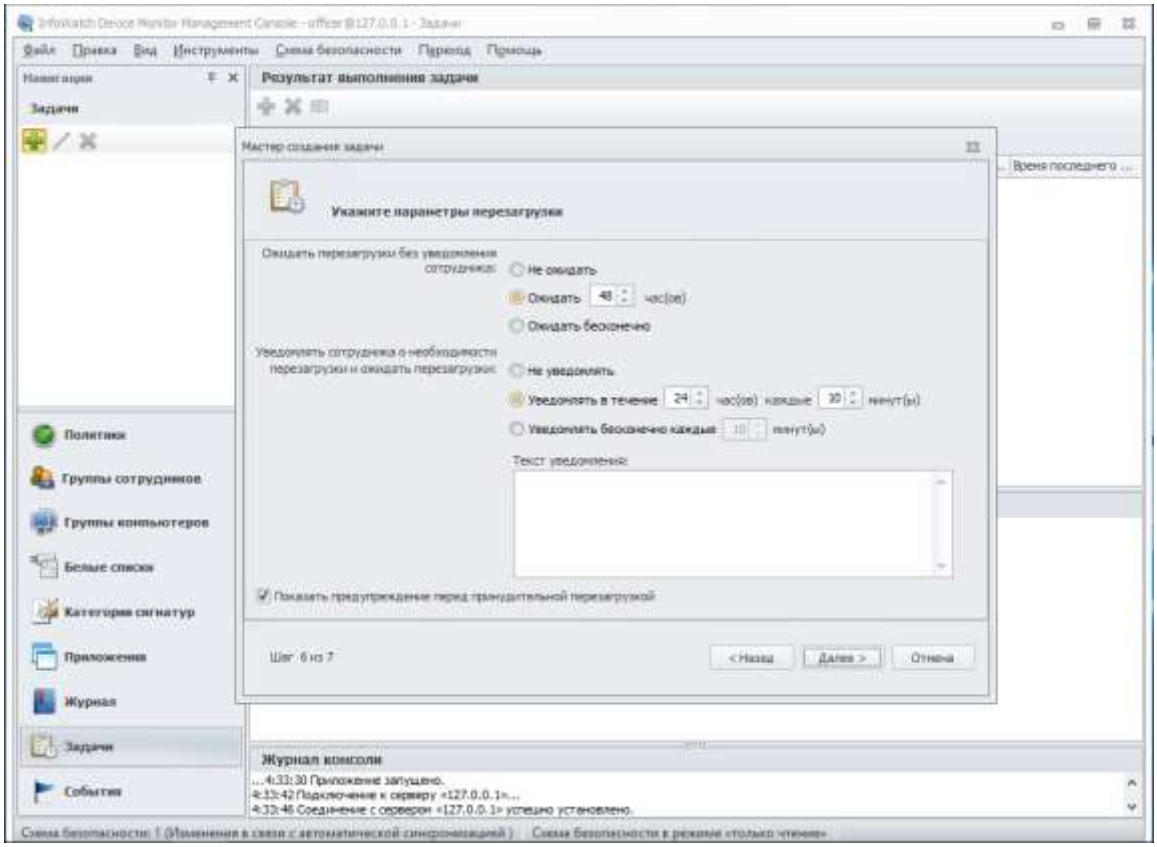
Выбираем наш сервер IWDM



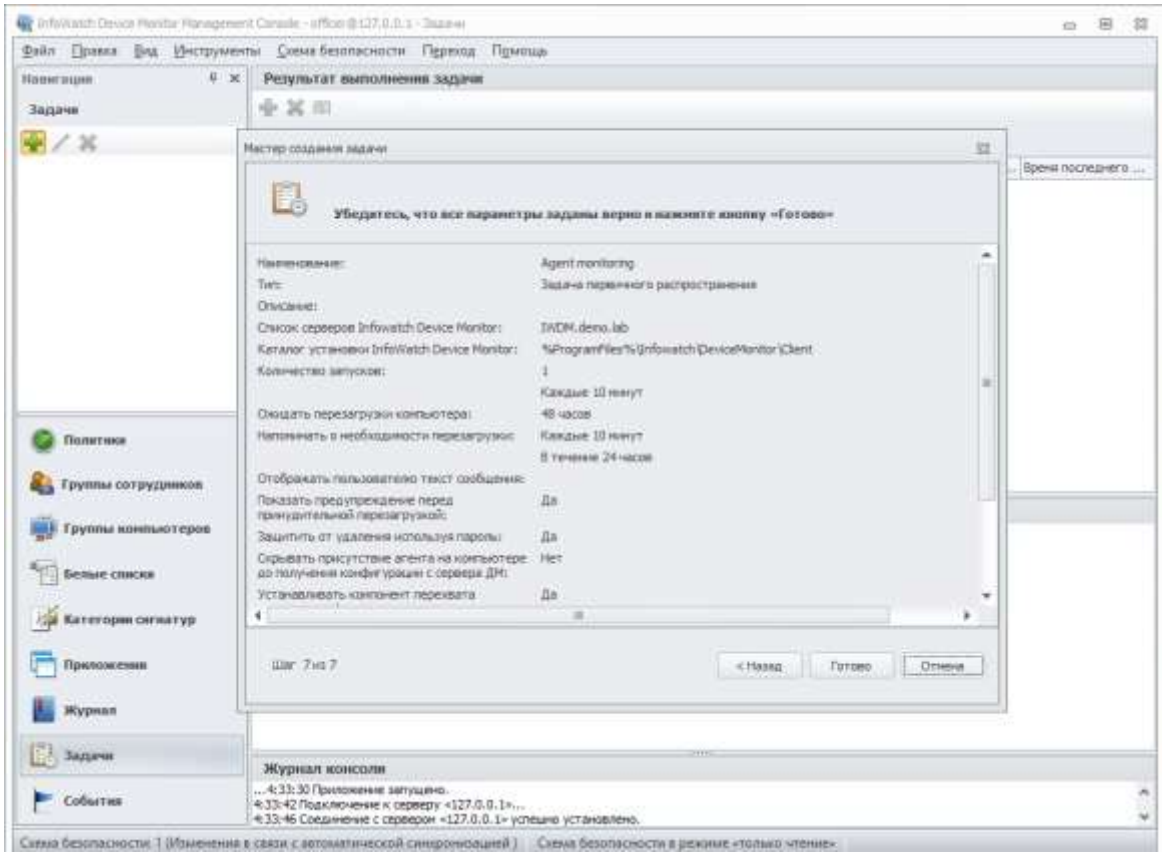


Вводим пароль, и учётную запись от которой будет запускаться задача

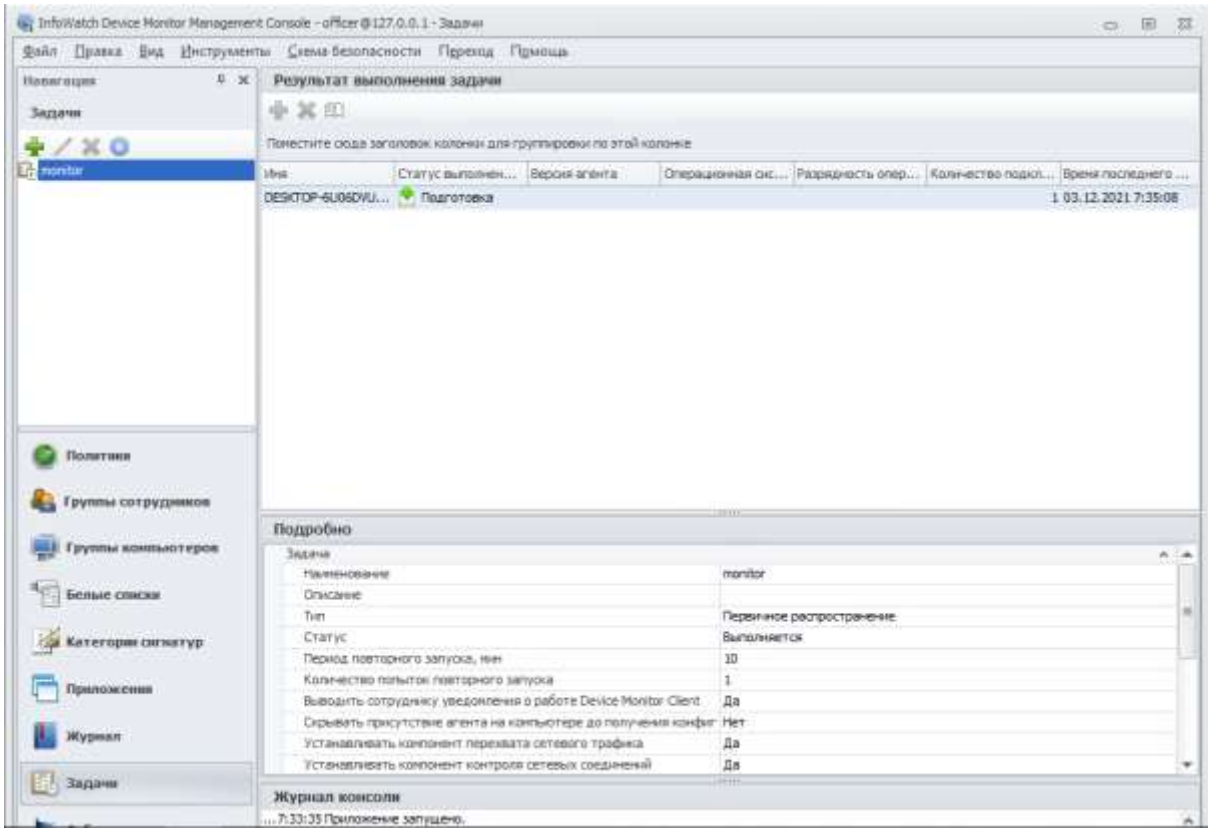




Готово

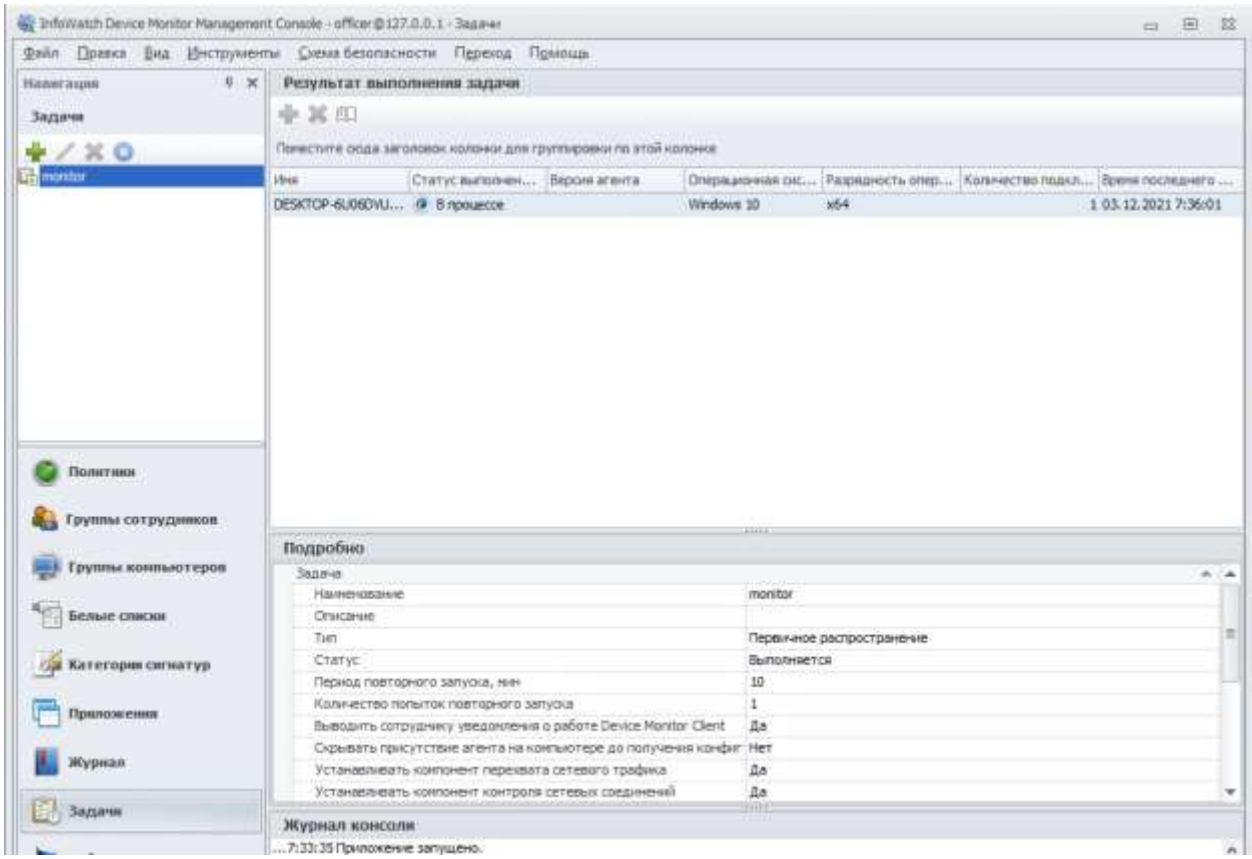


Ожидаем подготовку

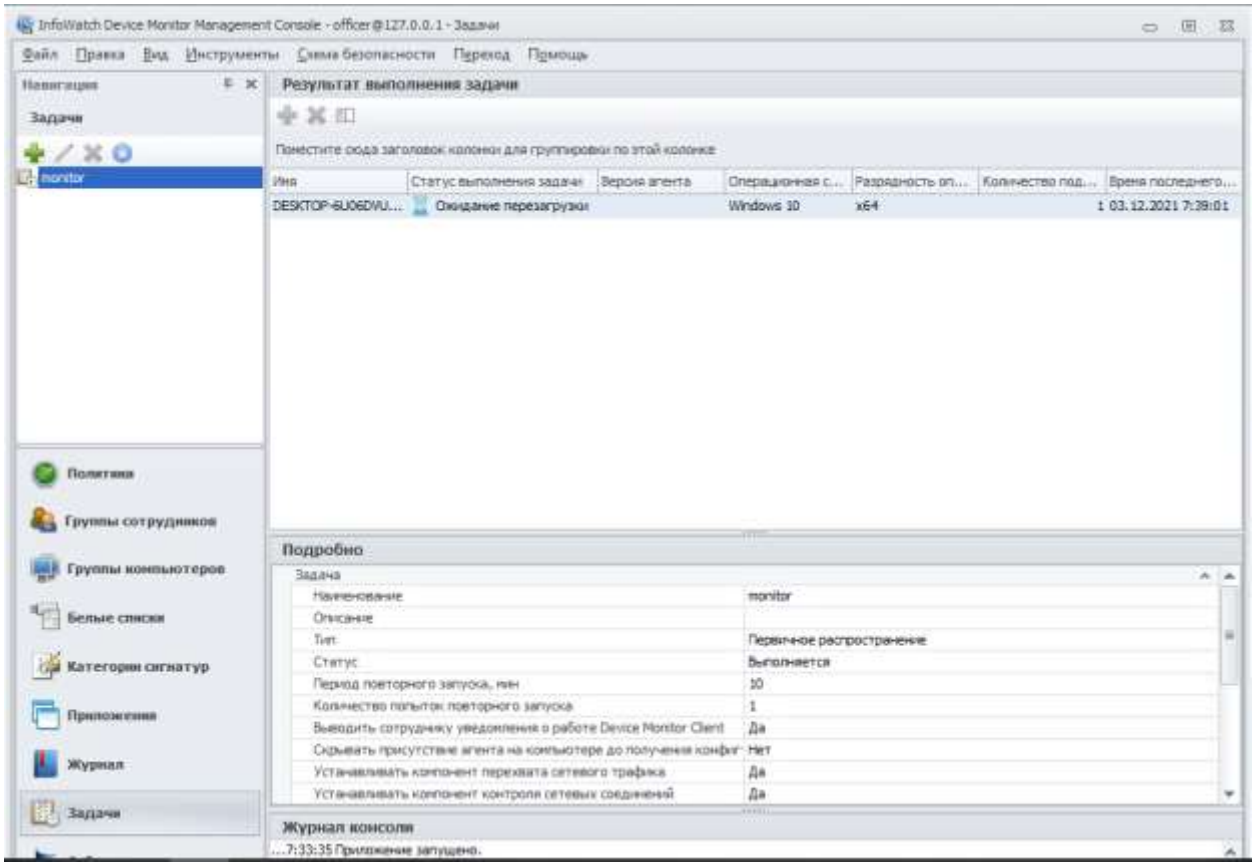


Не забываем у компьютеров Клиент1 и Клиент2 включить сетевое обнаружение!

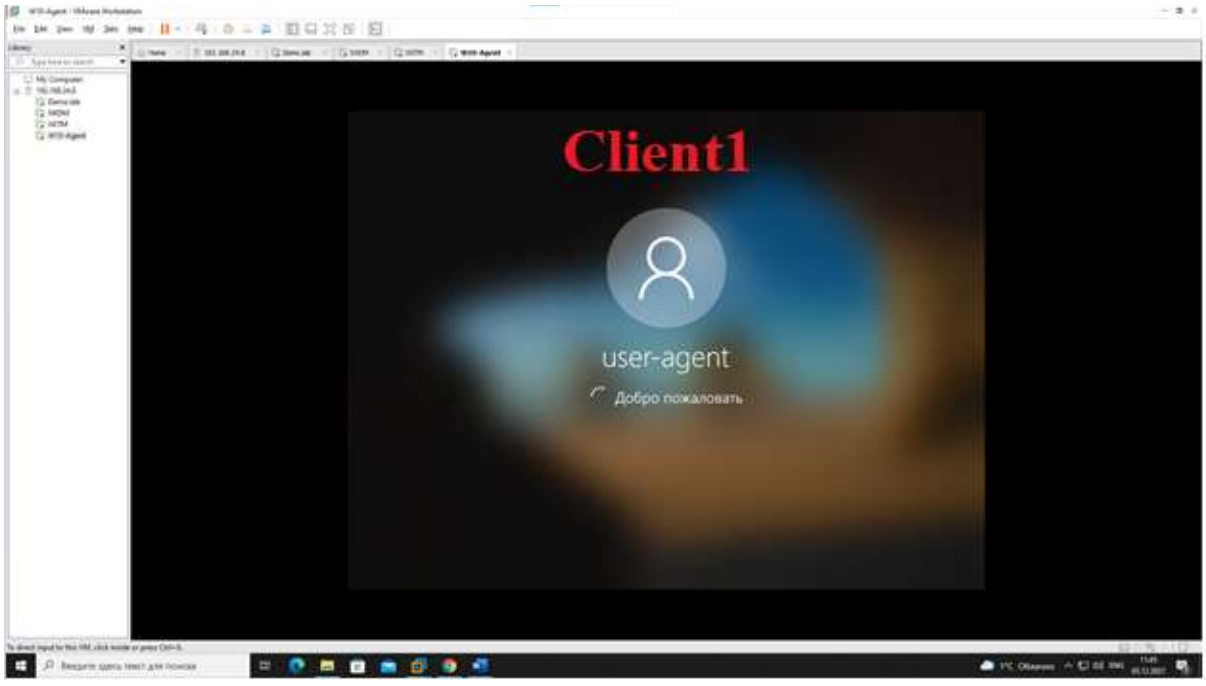
Ожидаем в процессе



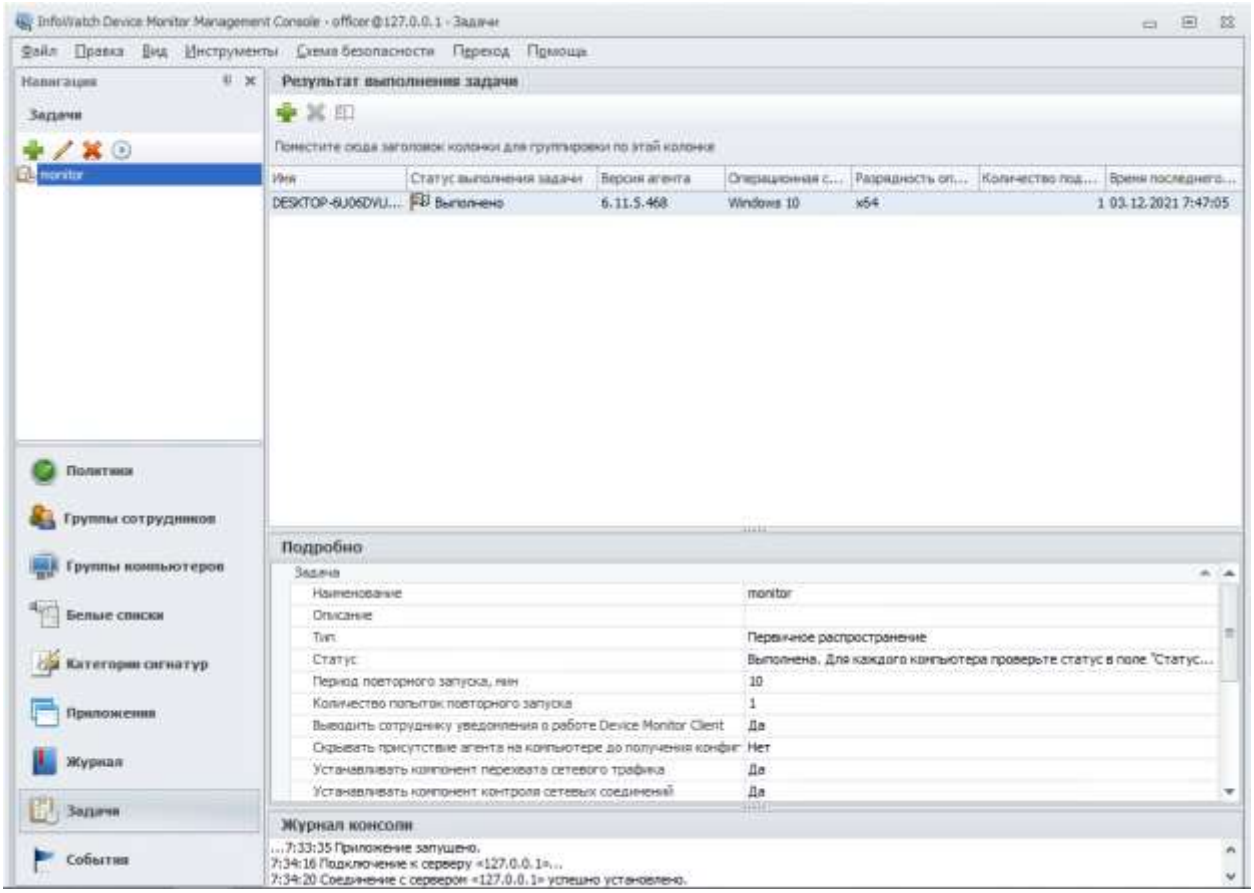
Компьютер агента ожидает перезагрузки

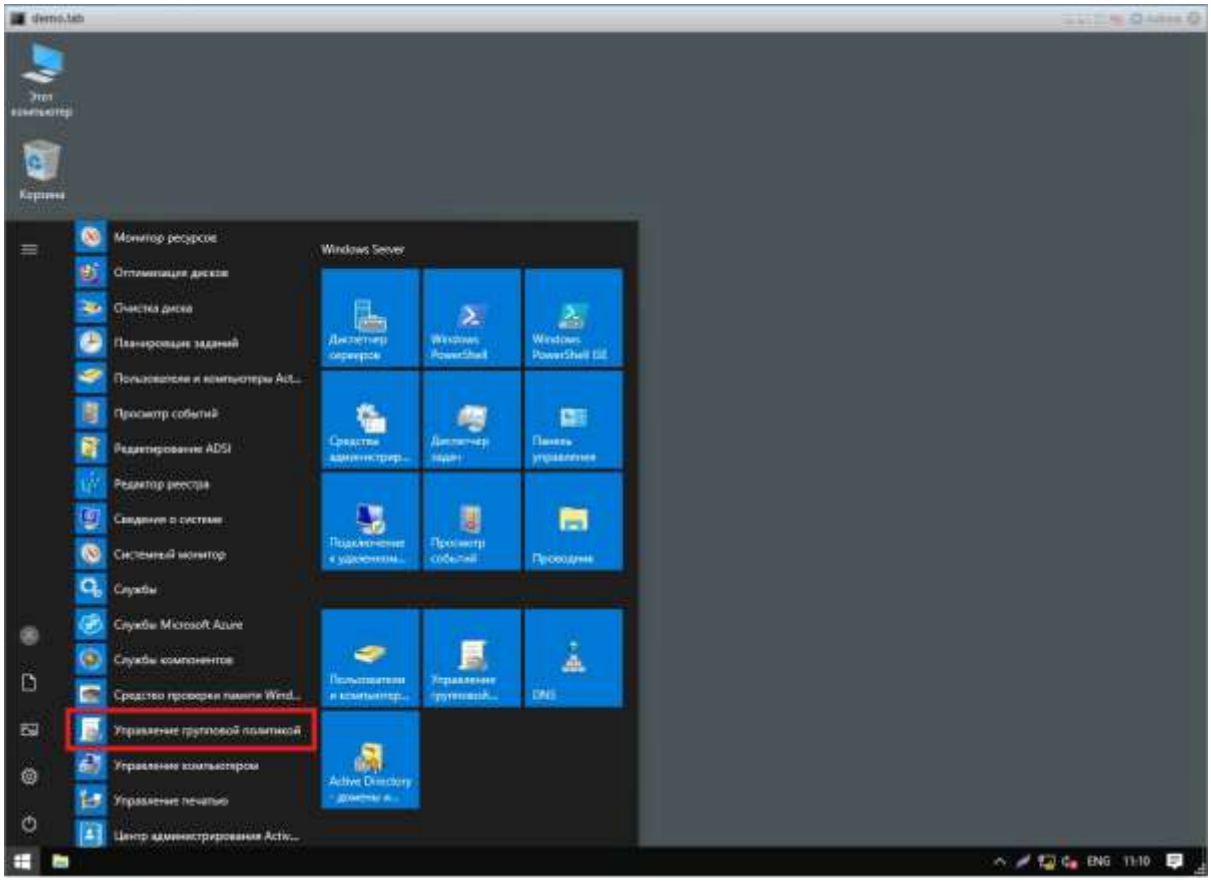


Перезагружаем компьютер агента, и заходим под пользователя

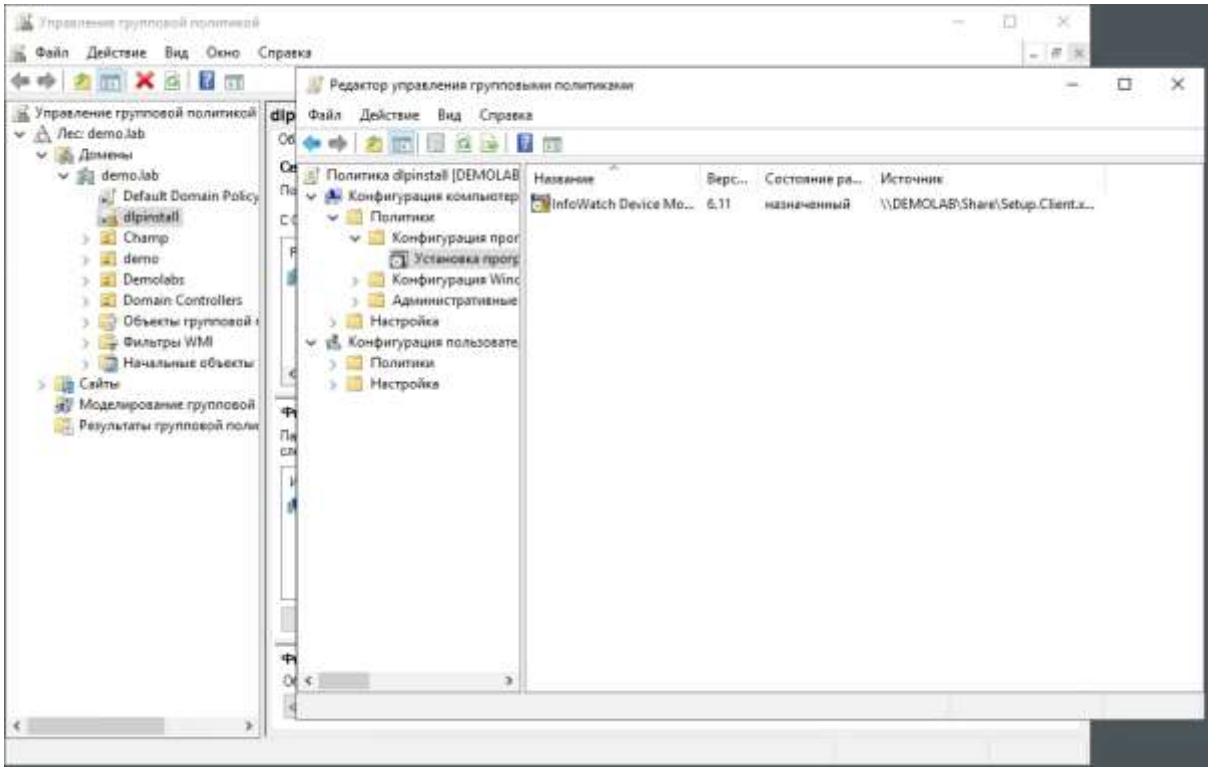


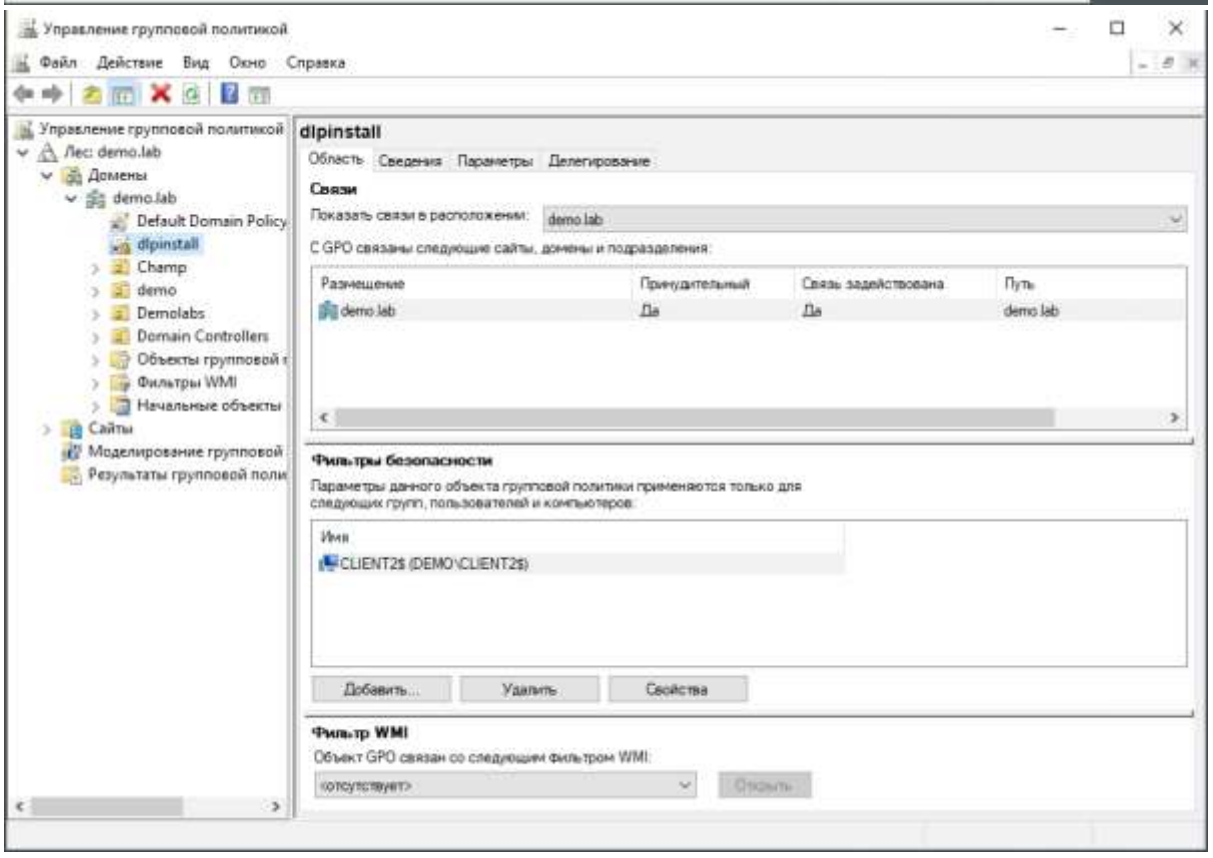
Возвращаемся на компьютер IWDM и смотрим статус выполнения задачи – выполнено

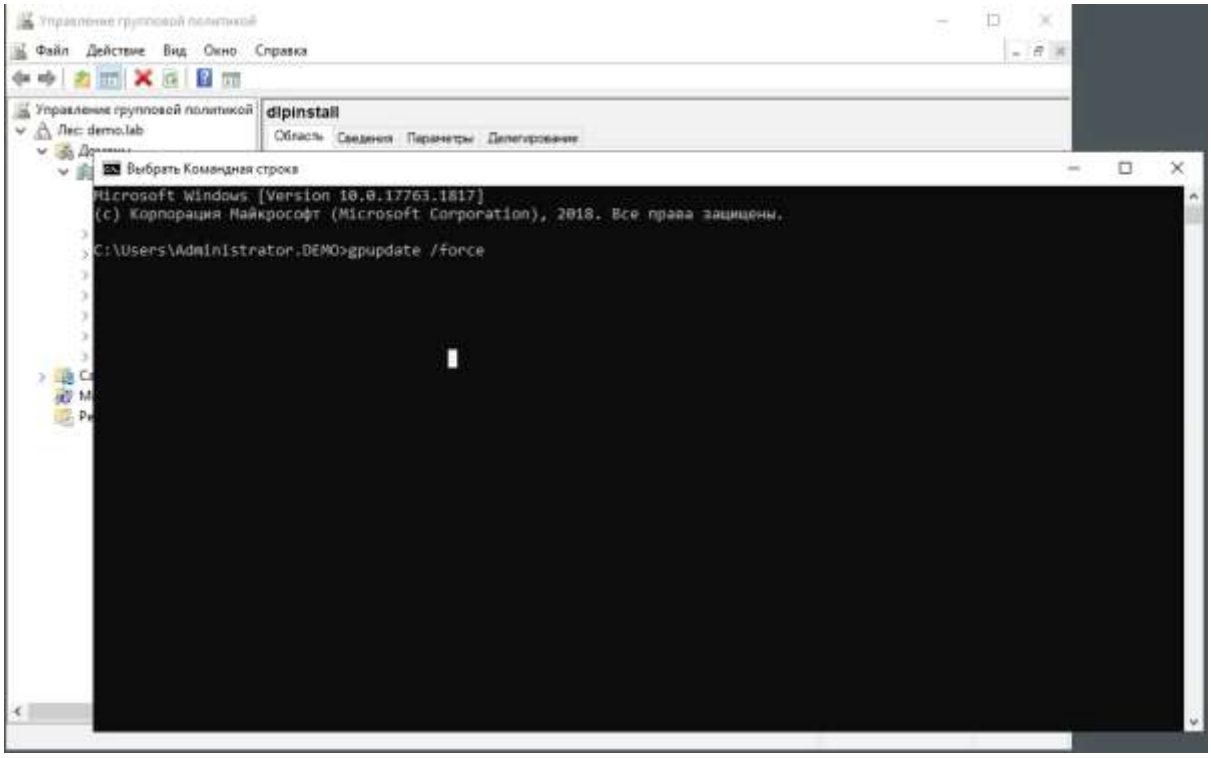




Файл установки выбираем 64 бита


Управление групповой политикой
Файл Действие Вид Окно Справка
Редактор управления групповыми политиками
Файл Действие Вид Справка
Название
Верс...
Состояние ра...
Источник
InfoWatch Device Mo...
6.11
назначенный
\\DEMOLAB\Share\Setup.Client.x...
Управление групповой политикой
Лес: demo.lab
Домены
demo.lab
Default Domain Policy
dlpinstall
Champ
demo
Demolabs
Domain Controllers
Фильтры WMI
Начальные объекты
Сайты
Моделирование групповой
Результаты групповой поли
Политика dlpinstall [DEMOLAB
Конфигурация компьютер
Политики
Настройка
Конфигурация пользовате


Управление групповой политикой
Файл Действие Вид Окно Справка
dlpinstall
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
Да
Да
demo.lab
Фильтры безопасности
Параметры данного объекта групповой политики применяются только для следующих групп, пользователей и компьютеров:
Имя
CLIENT2$ (DEMO\CLIENT2$)
Добавить...
Удалить
Свойства
Фильтр WMI
Объект GPO связан со следующим фильтром WMI:
<отсутствует>
Открыть
Управление групповой политикой
Лес: demo.lab
Домены
demo.lab
Default Domain Policy
dlpinstall
Champ
demo
Demolabs
Domain Controllers
Фильтры WMI
Начальные объекты
Сайты
Моделирование групповой
Результаты групповой поли



После этого перезапускаем компьютер – Клиент2

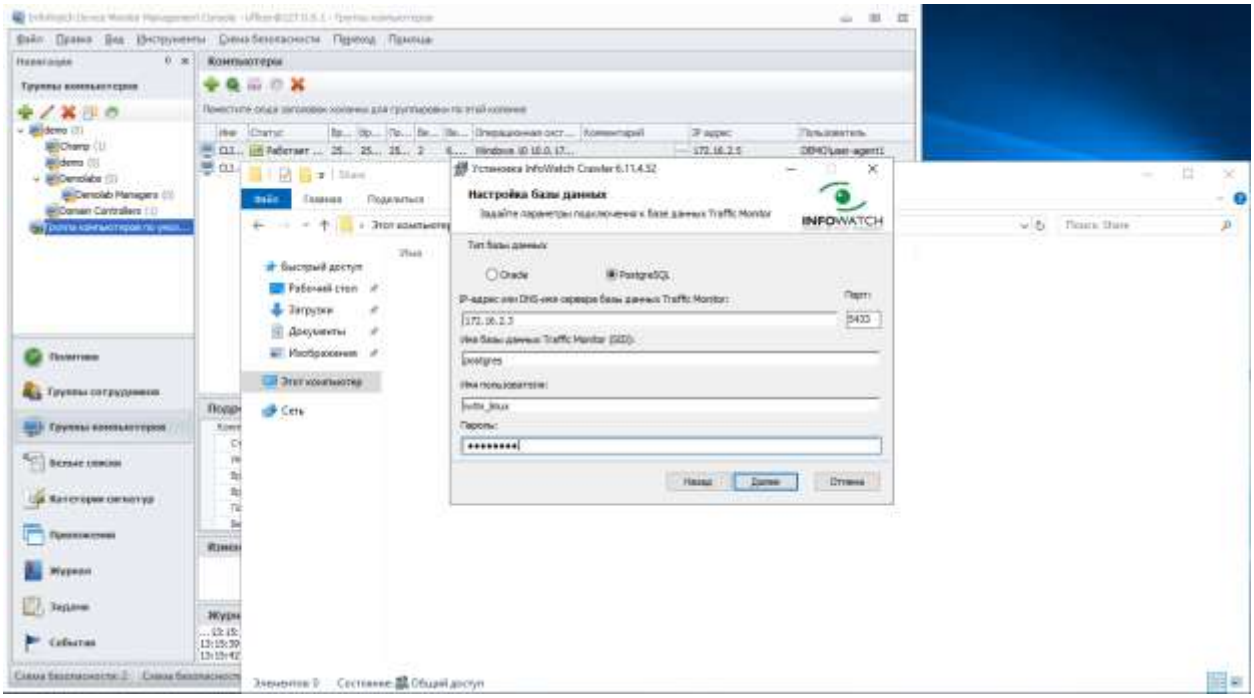
Необходимо создать общий каталог Share в корне диска сервера IWDM и установить права доступа на запись и чтение для всех пользователей домена.

Крауль – ДЕЛАТЬ В ПОСЛЕДНЮЮ ОЧЕРЕДЬ

Задание 5: Установка и настройка подсистемы сканирования сетевых ресурсов.

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

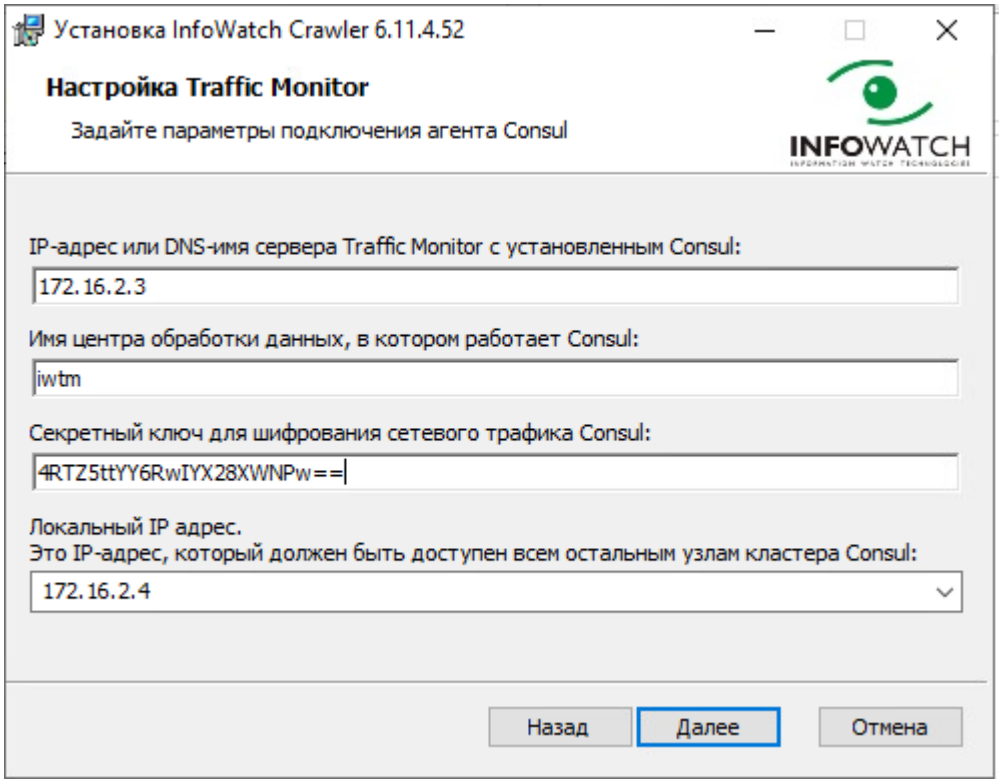
Необходимо настроить подсистему сканирования сетевых ресурсов на автоматическое ежедневное сканирование только ранее созданного каталога. Для работы подсистемы может потребоваться редактирования конфигурационных
файлов (для устранения предупреждения).




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

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

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

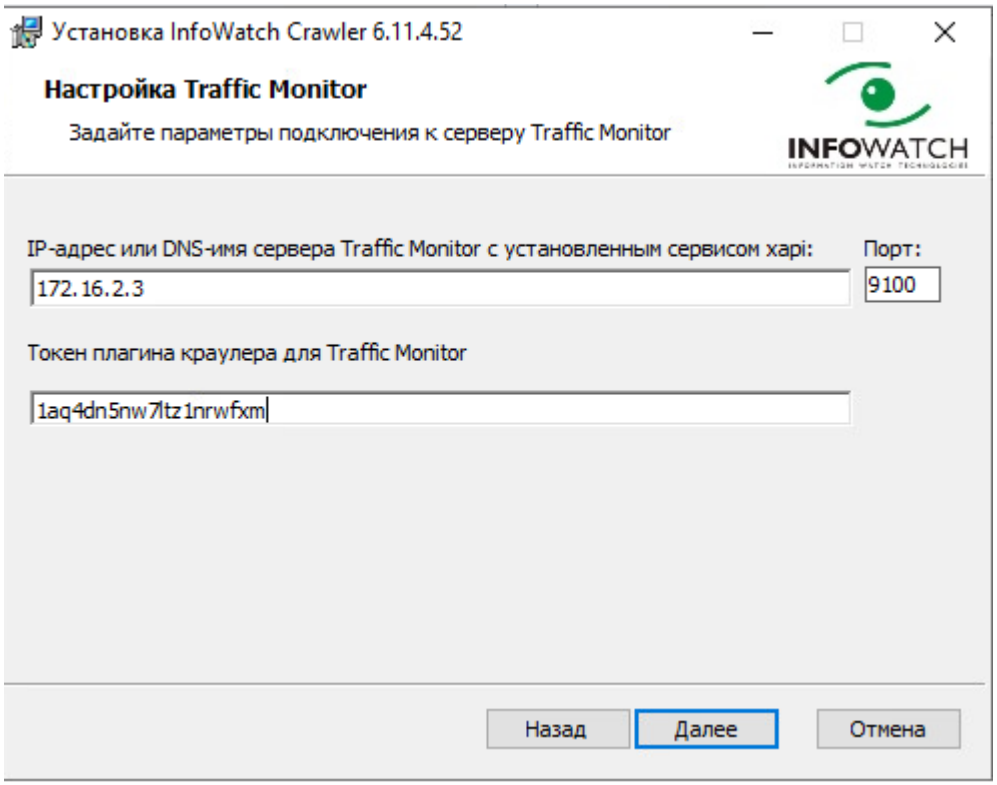


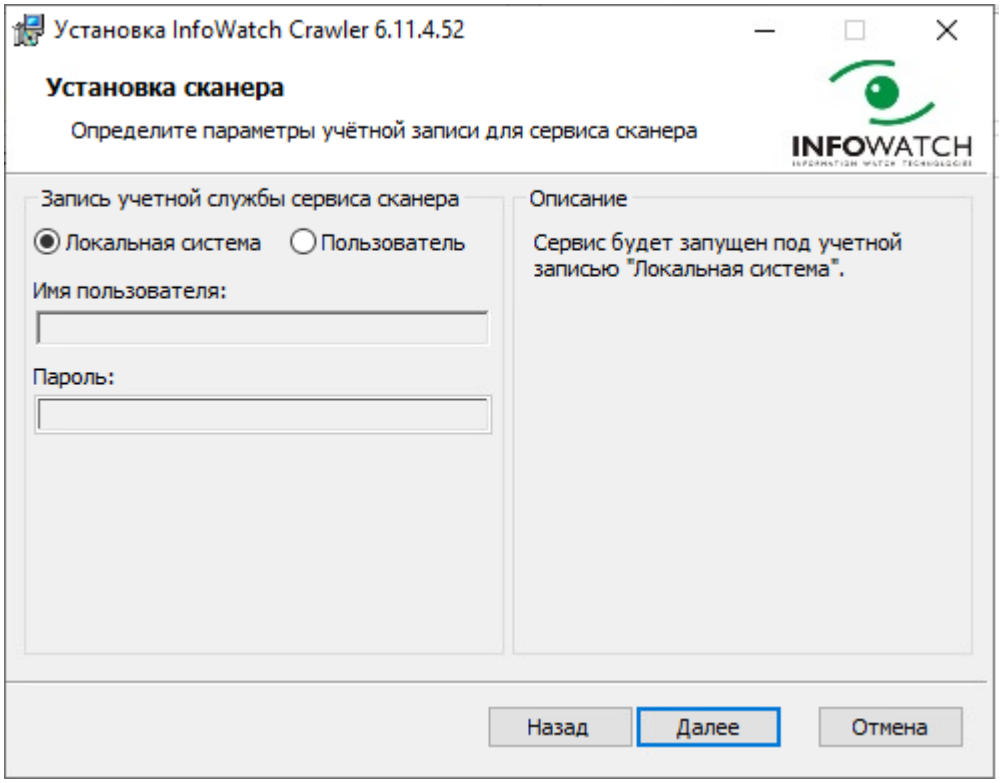
Статус	Имя	Содержание
Активный	Token-2	1aq4dn5nw7ltz1nrwfxm

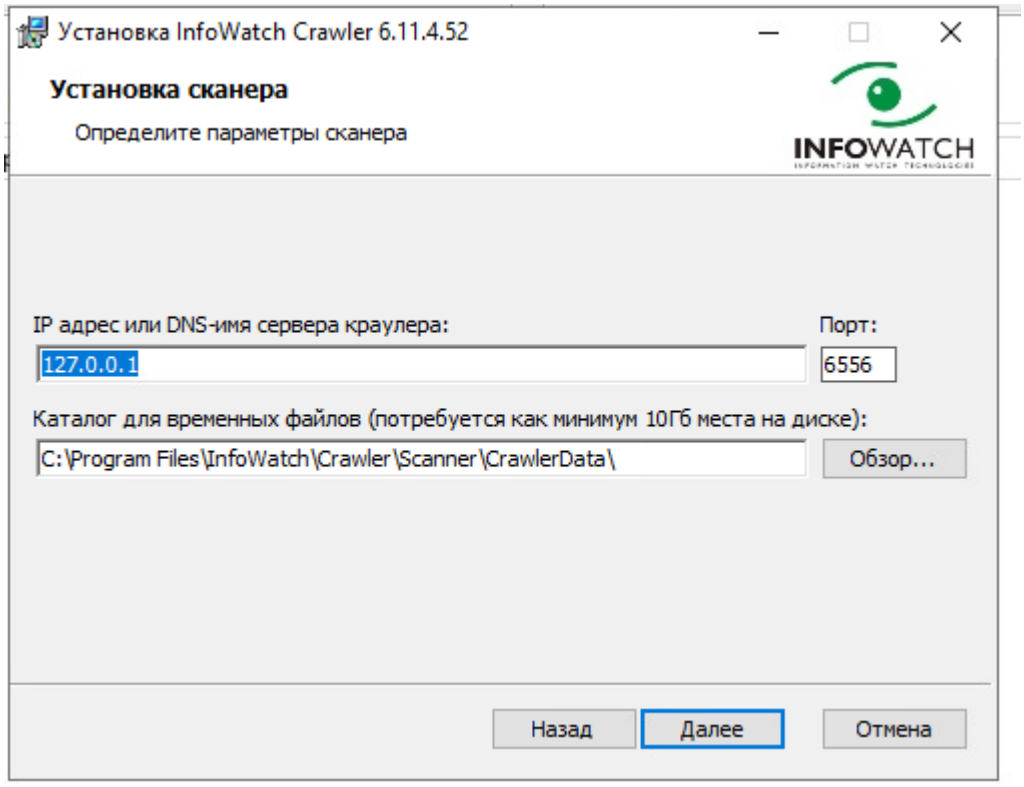
```
[root@iwtm etc]# cd /opt/iw/tm5/etc
```

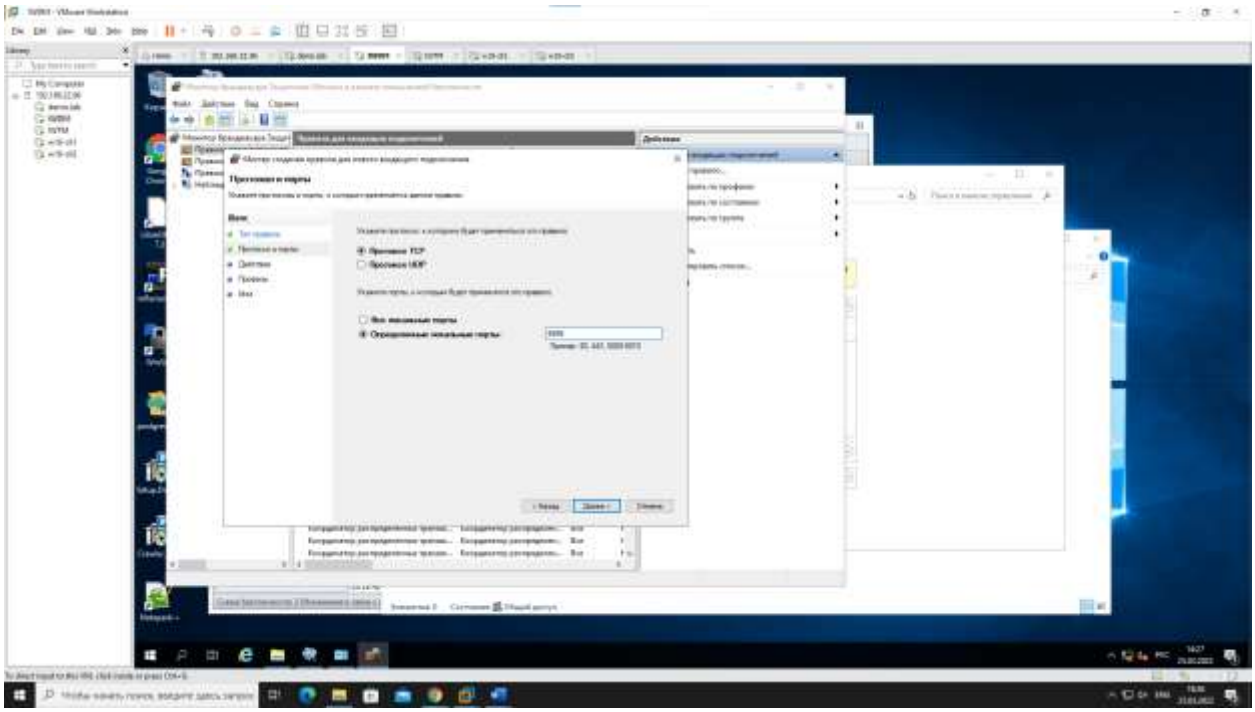
```
[root@iwtm etc]# nano web.conf
```

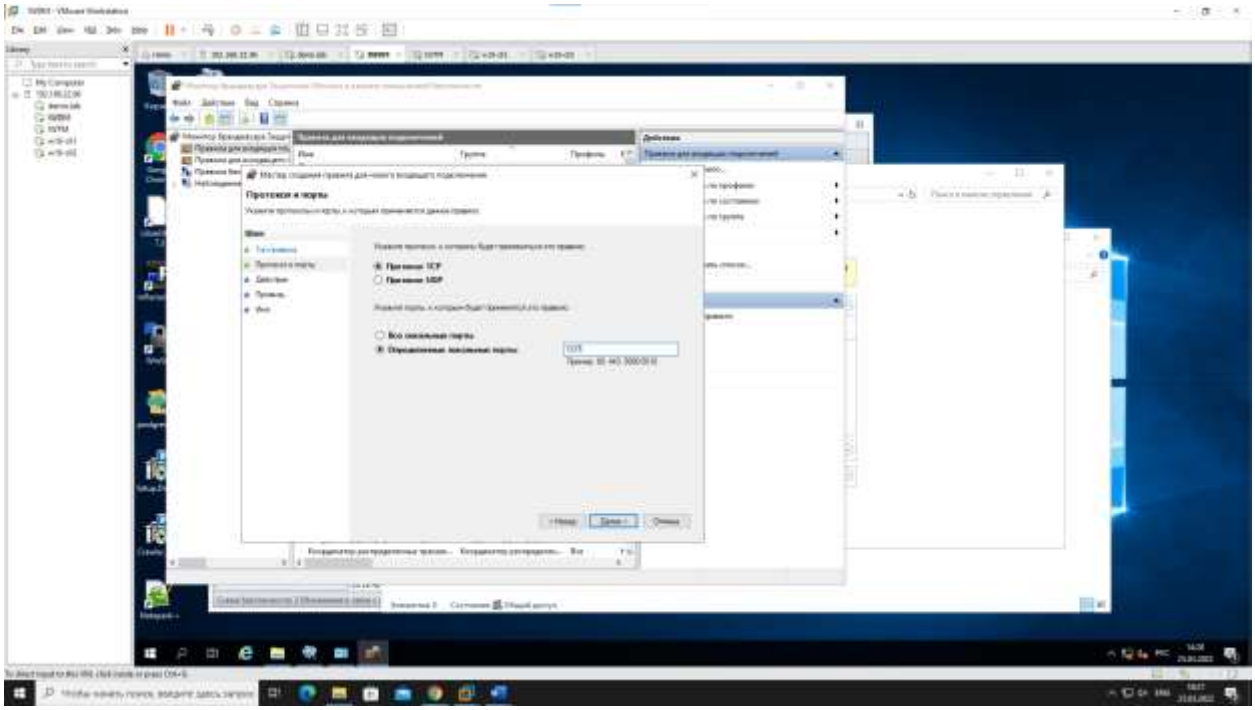
```
    },
    "crawler": {
        "enabled": 1
    },
```


Установка InfoWatch Crawler 6.11.4.52
Настройка Traffic Monitor
Задайте параметры подключения к серверу Traffic Monitor
INFOWATCH
IP-адрес или DNS-имя сервера Traffic Monitor с установленным сервисом xapi:
Порт:
172.16.2.3
9100
Токен плагина краулера для Traffic Monitor
1aq4dn5nw7ltz1nrwfxm
Назад
Далее
Отмена


Установка InfoWatch Crawler 6.11.4.52
Установка сканера
Определите параметры учётной записи для сервиса сканера
INFOWATCH
Запись учетной службы сервиса сканера
Локальная система
Пользователь
Имя пользователя:
Пароль:
Описание
Сервис будет запущен под учетной записью "Локальная система".
Назад
Далее
Отмена

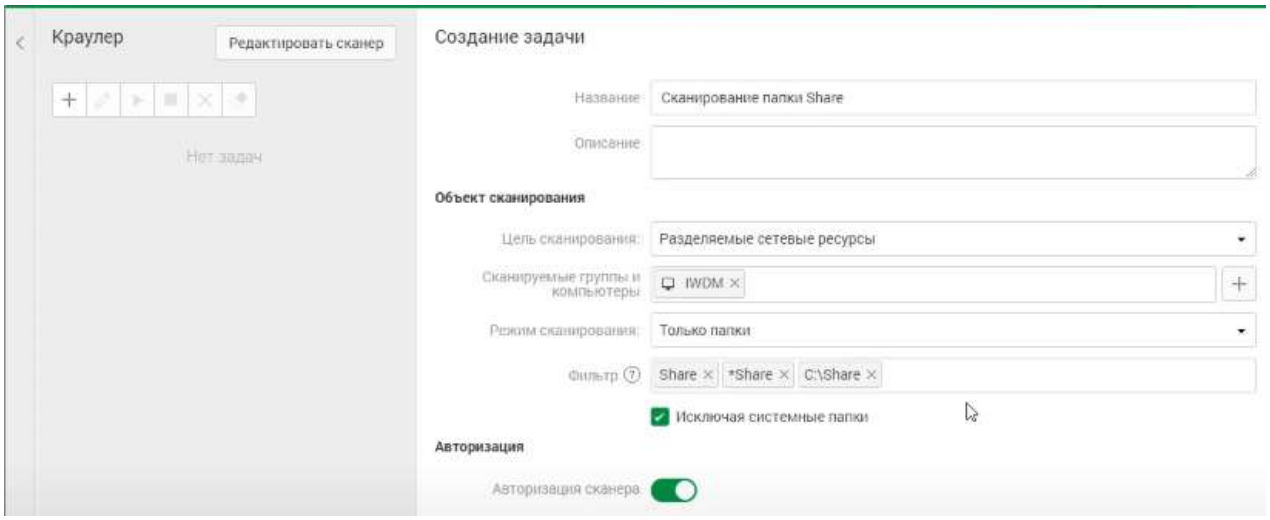

Установка InfoWatch Crawler 6.11.4.52
Установка сканера
Определите параметры сканера
INFOWATCH
IP адрес или DNS-имя сервера краулера:
Порт:
127.0.0.1
6556
Каталог для временных файлов (потребуется как минимум 10Гб места на диске):
C:\Program Files\InfoWatch\Crawler\Scanner\CrawlerData\
Обзор...
Назад
Далее
Отмена





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

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



Расписание:

Период сканирования: Ежедневно

Начало действия: 13/05/2022

Время: 0:00

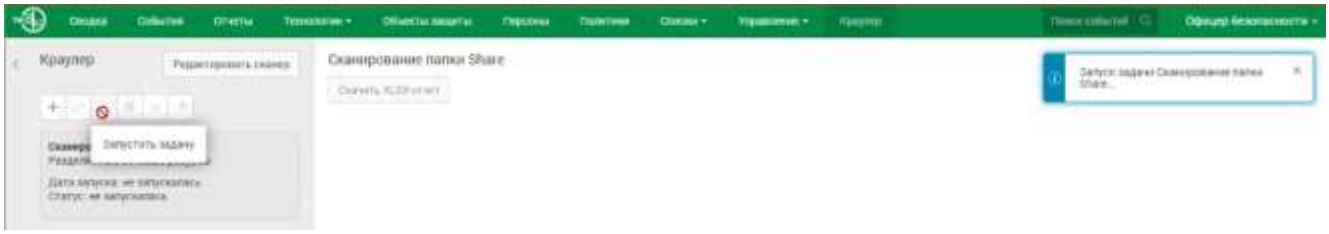
Искать файлы

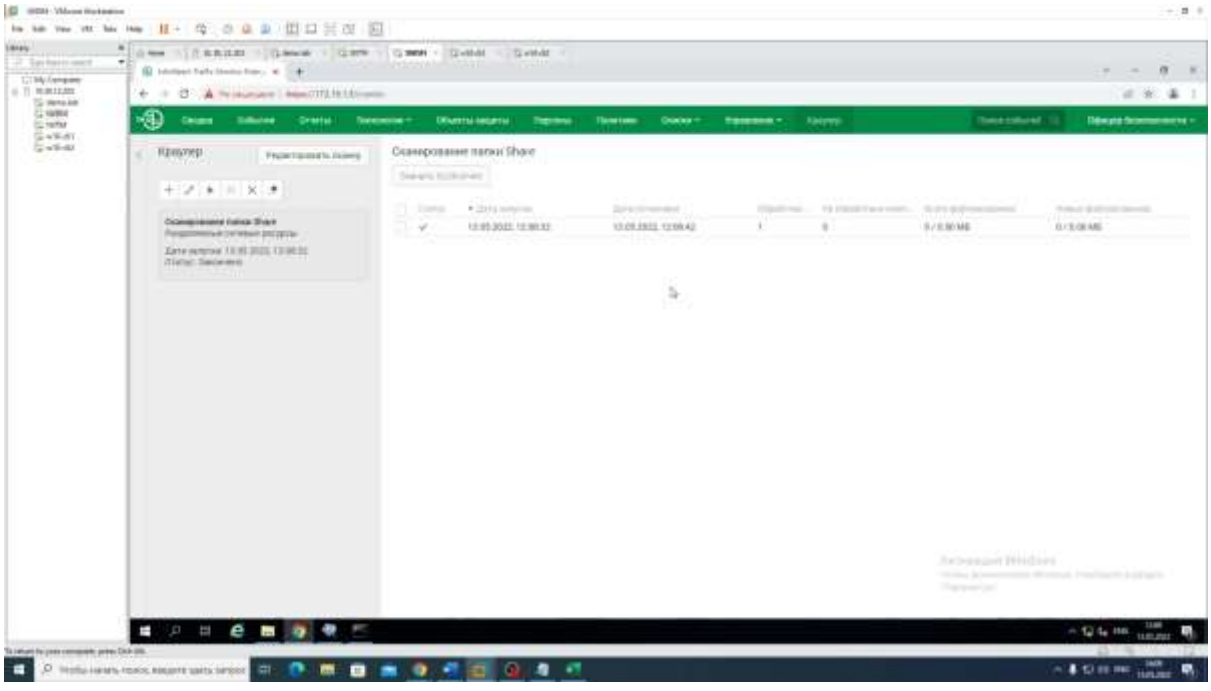
Минимальный размер (КБ): 0

Максимальный размер (КБ):

Фильтры файлов (маски): *.doc × *.docx × *.xls × *.xlsx × *.ppt × *.pptx × *.odt × *.ods × *.odp × *.pdf × *.rtf × *.tnef × *.htm × *.html × *.xml × *.txt × *.emf ×

Сохранить Отменить

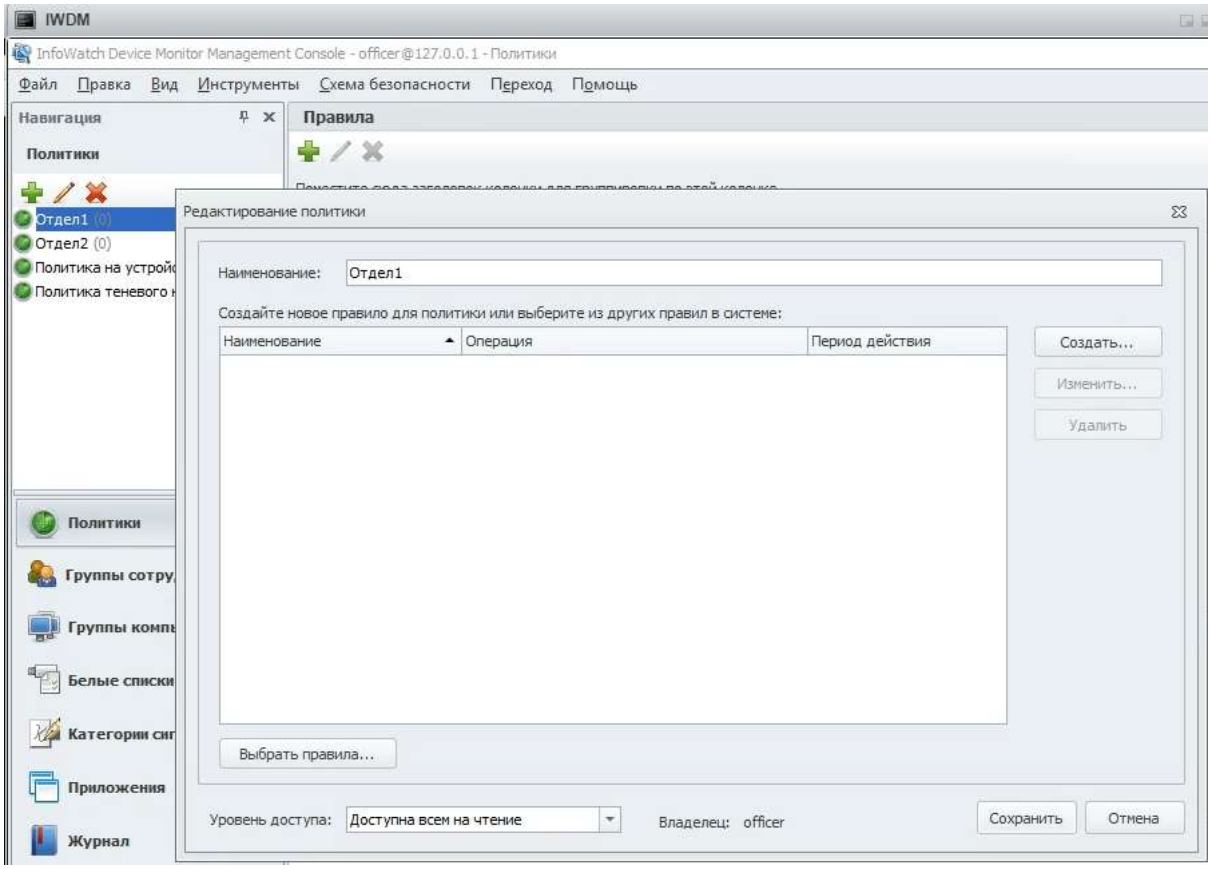


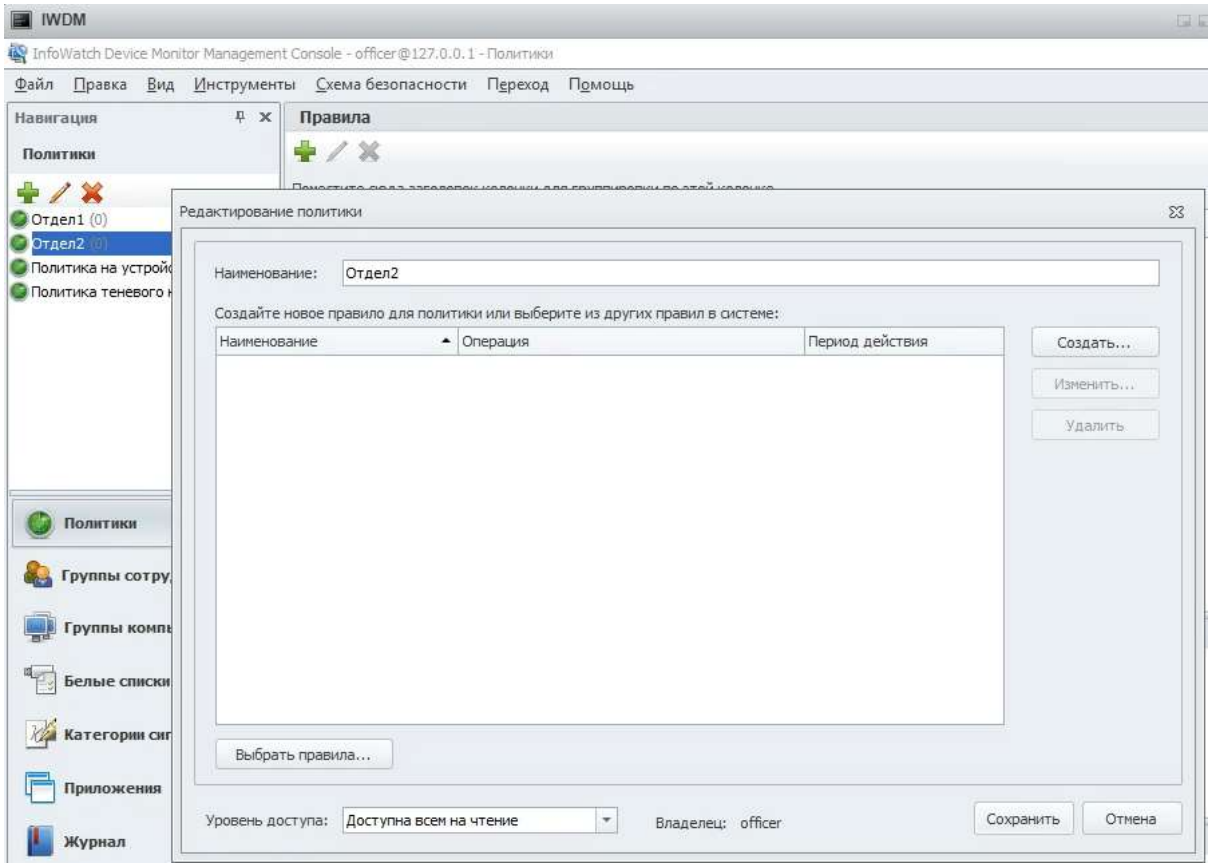


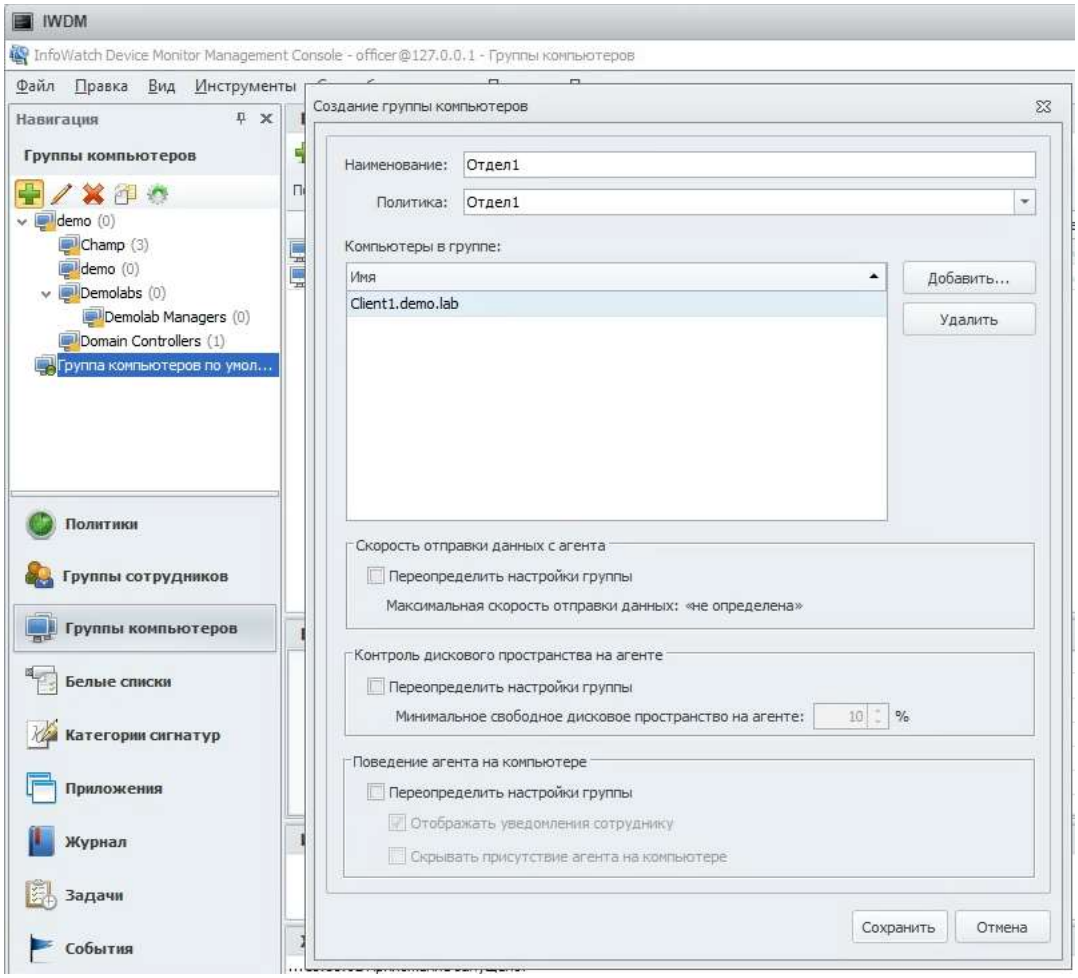
Модуль 2.

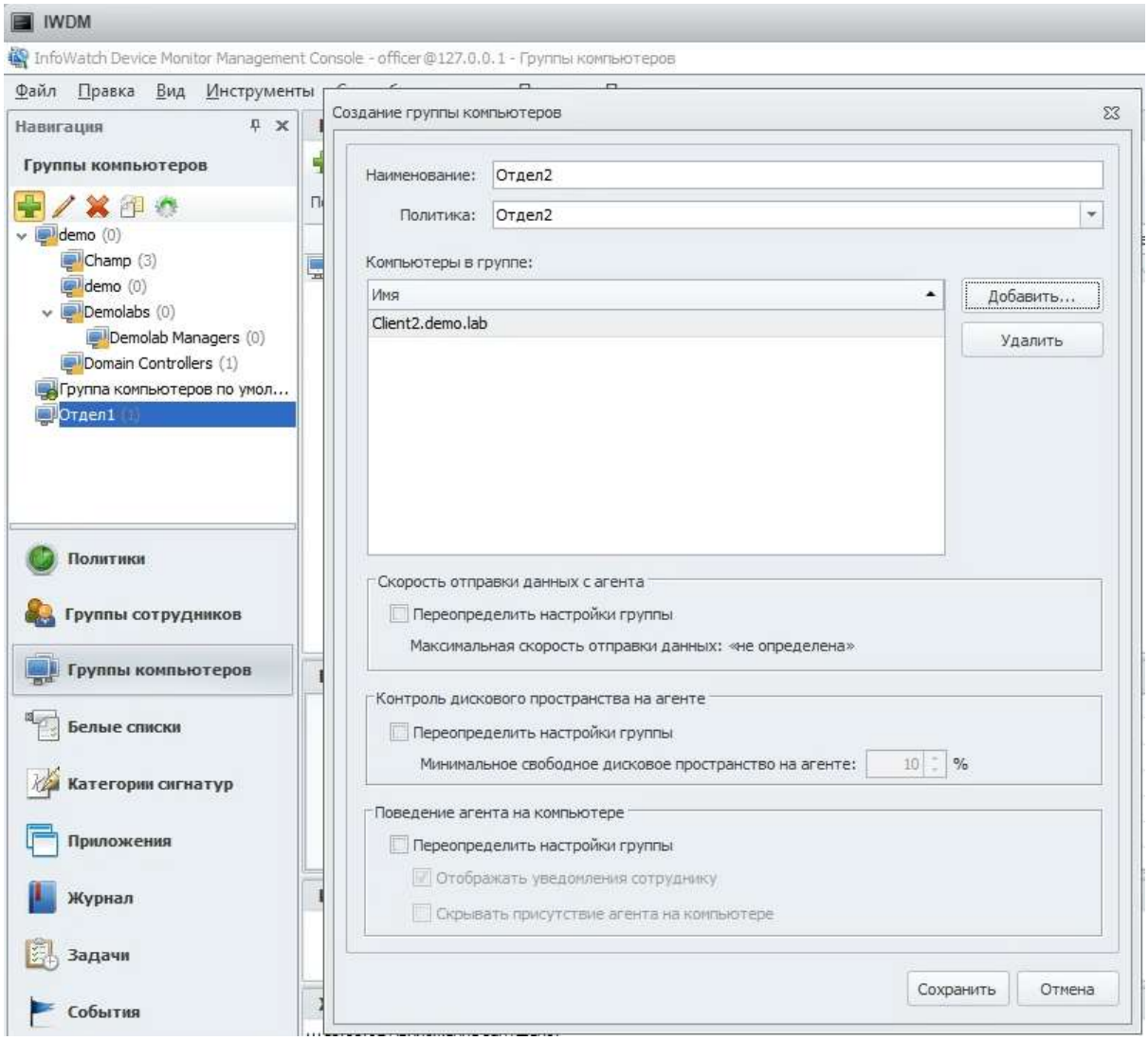
Задание 1

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




IWDM
InfoWatch Device Monitor Management Console - officer@127.0.0.1 - Политики
Файл Правка Вид Инструменты Схема безопасности Переход Помощь
Навигация
Политики
Правила
Отдел1 (0)
Отдел2 (0)
Политика на устройс
Политика теневого к
Редактирование политики
Наименование: Отдел2
Создайте новое правило для политики или выберите из других правил в системе:
Наименование
Операция
Период действия
Создать...
Изменить...
Удалить
Выбрать правила...
Уровень доступа: Доступна всем на чтение
Владелец: officer
Сохранить
Отмена
Политики
Группы сотру
Группы компь
Белые списки
Категории сиг
Приложения
Журнал


IWDM
InfoWatch Device Monitor Management Console - officer@127.0.0.1 - Группы компьютеров
Файл Правка Вид Инструменты
Навигация
Группы компьютеров
demo (0)
Champ (3)
demo (0)
Demolabs (0)
Demolab Managers (0)
Domain Controllers (1)
Группа компьютеров по умол...
Создание группы компьютеров
Наименование: Отдел1
Политика: Отдел1
Компьютеры в группе:
Имя
Client1.demo.lab
Добавить...
Удалить
Скорость отправки данных с агента
Переопределить настройки группы
Максимальная скорость отправки данных: «не определена»
Контроль дискового пространства на агенте
Переопределить настройки группы
Минимальное свободное дисковое пространство на агенте: 10 %
Поведение агента на компьютере
Переопределить настройки группы
Отображать уведомления сотруднику
Скрывать присутствие агента на компьютере
Сохранить
Отмена
Политики
Группы сотрудников
Группы компьютеров
Белые списки
Категории сигнатур
Приложения
Журнал
Задачи
События

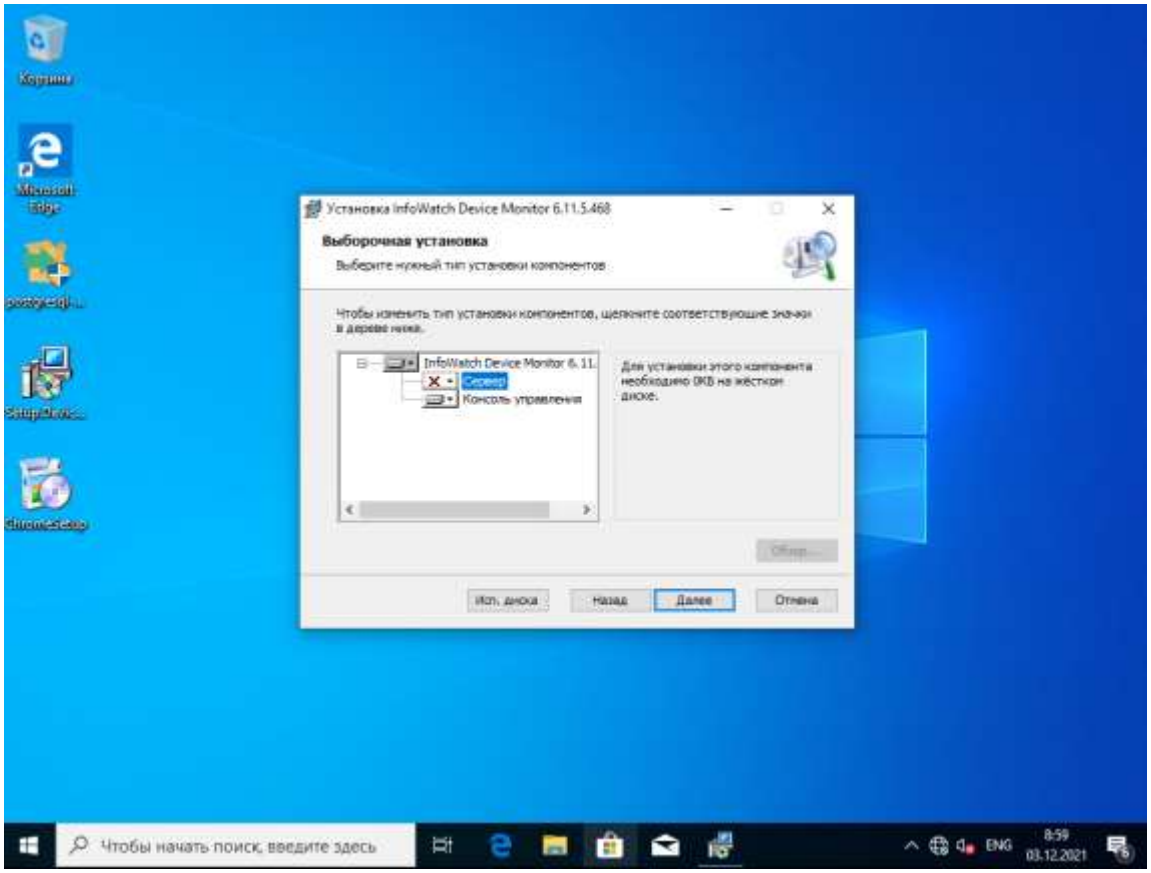


Задание 2

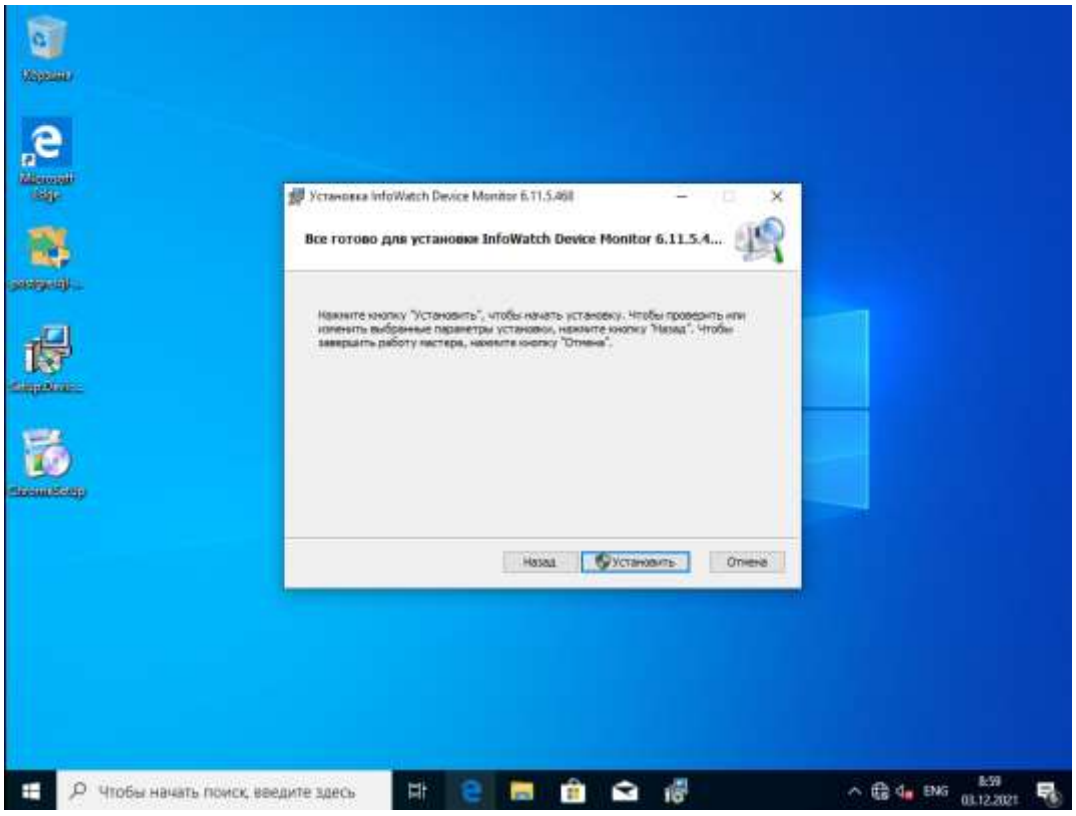
Для удобства работы офицера безопасности необходимо установить дополнительную консоль управления сервером агентского мониторинга на машину W10-agent1 для удаленного доступа к серверу агентского мониторинга.

Следующие правила создаются в политике «Отдел1».

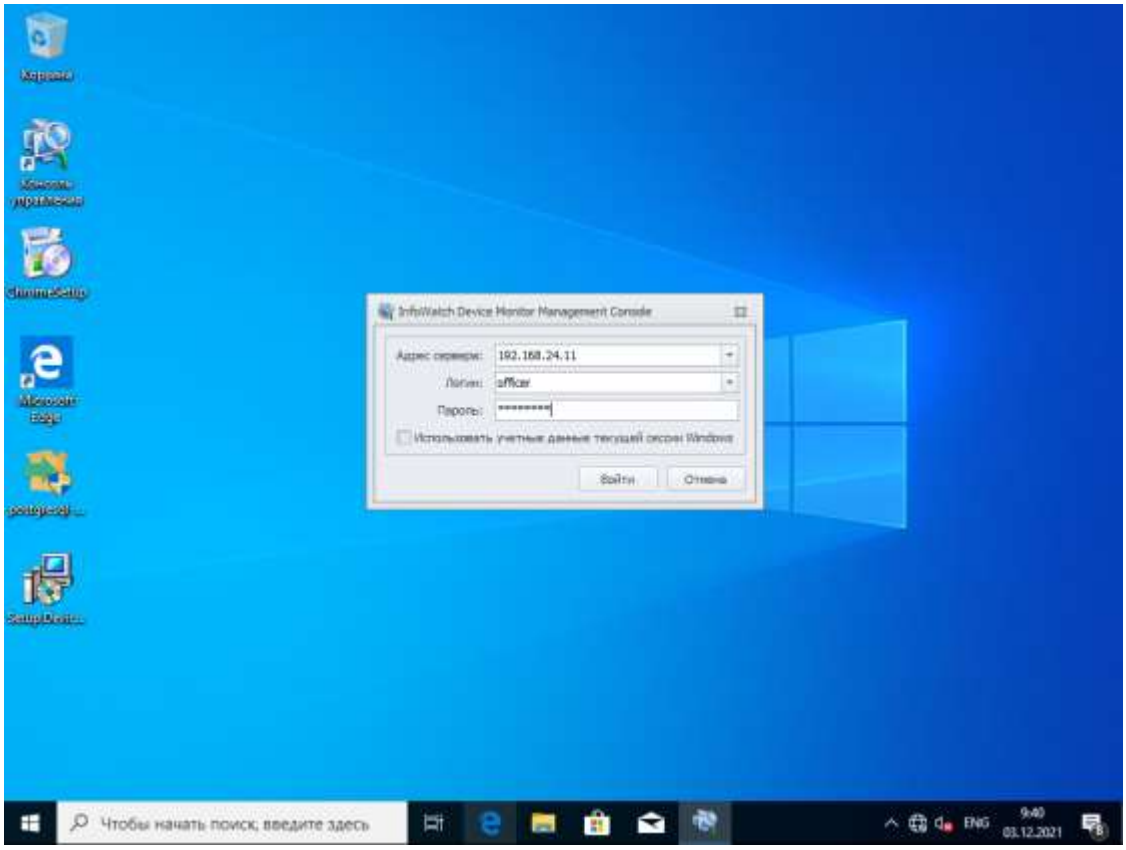
Убираем сервер, оставляем только консоль управления

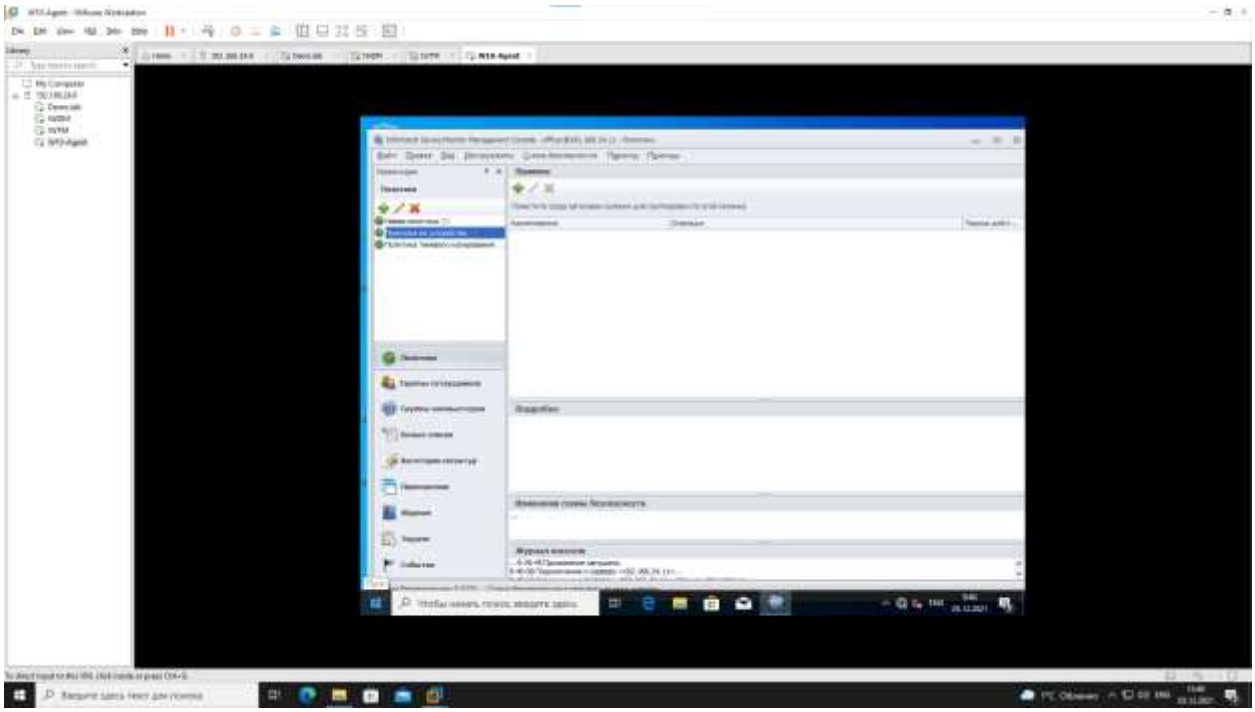


Установили InfoWatch Device Monitor



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


InfoWatch Device Monitor Management Console
Адрес сервера:
192.168.24.11
Логин:
officer
Пароль:
Использовать учетные данные текущей сессии Windows
Войти
Отмена
Чтобы начать поиск, введите здесь
ENG
9:40
03.12.2021



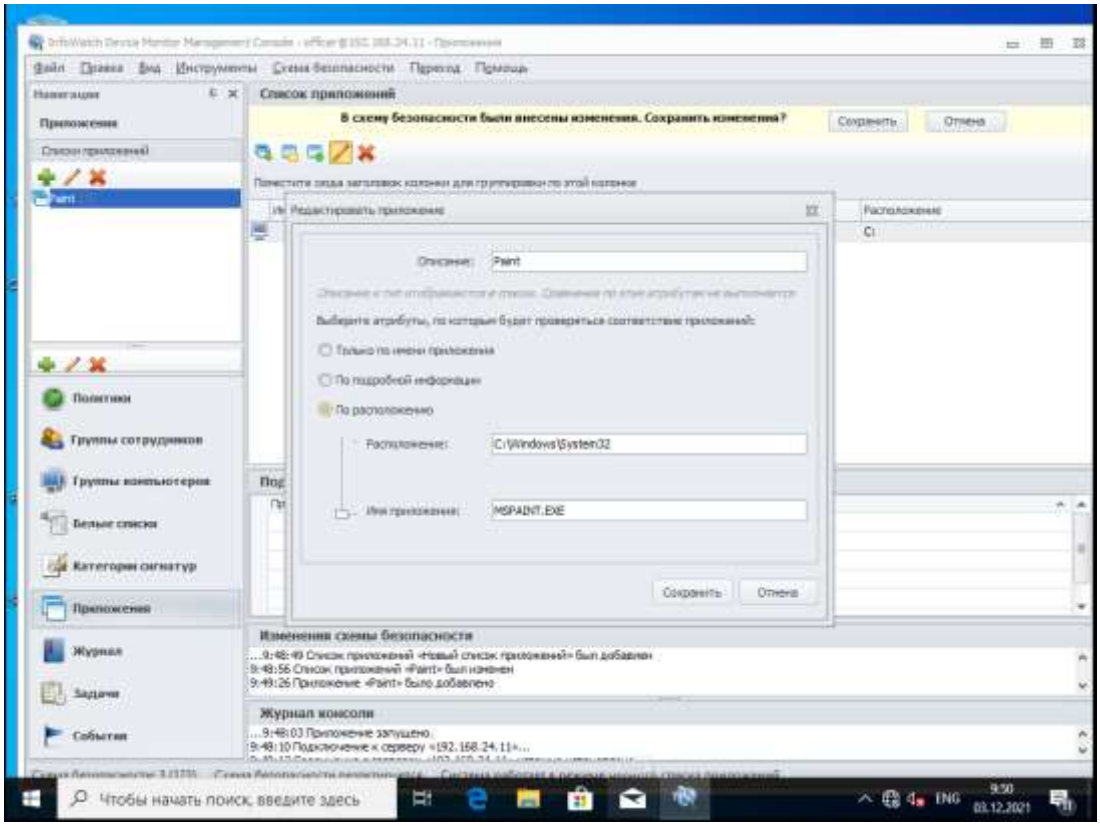
Следующие правила создаются в политике «Отдел1»

Правило 1

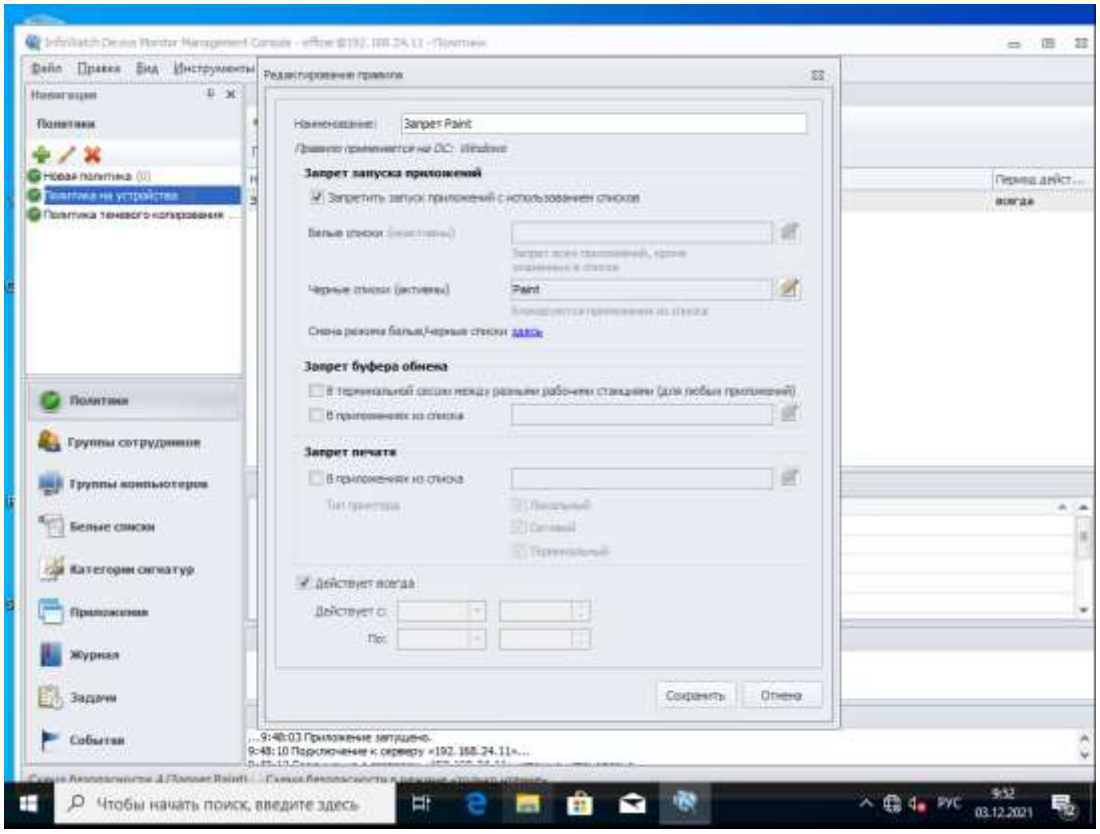
Необходимо запретить пользоваться Microsoft Paint, так как участились случаи подделки печатей компании.

Проверить работоспособность и зафиксировать выполнение скриншотом.

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



Переходим в политики, далее переходим в редактирование правил



Зафиксировать скриншотами необходимо!

Правило 2

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

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

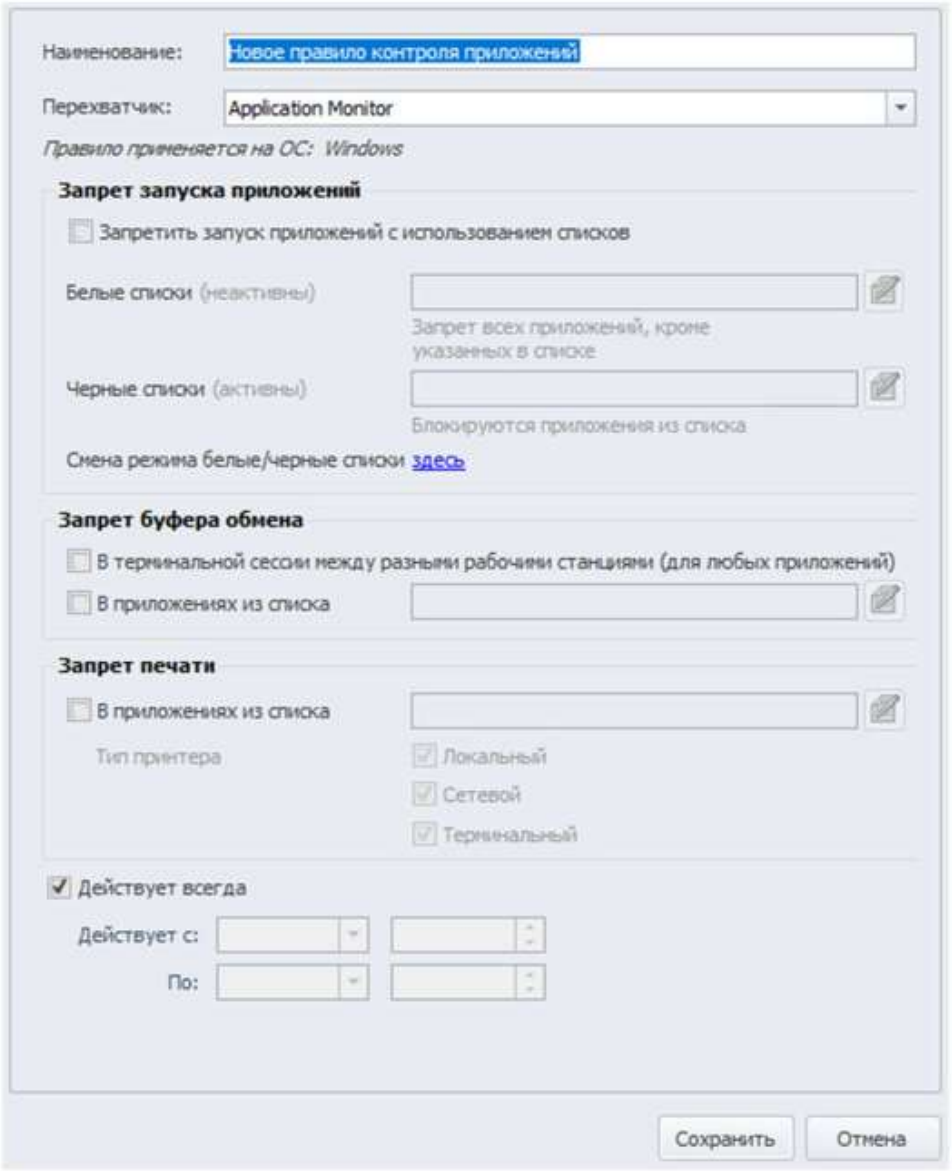
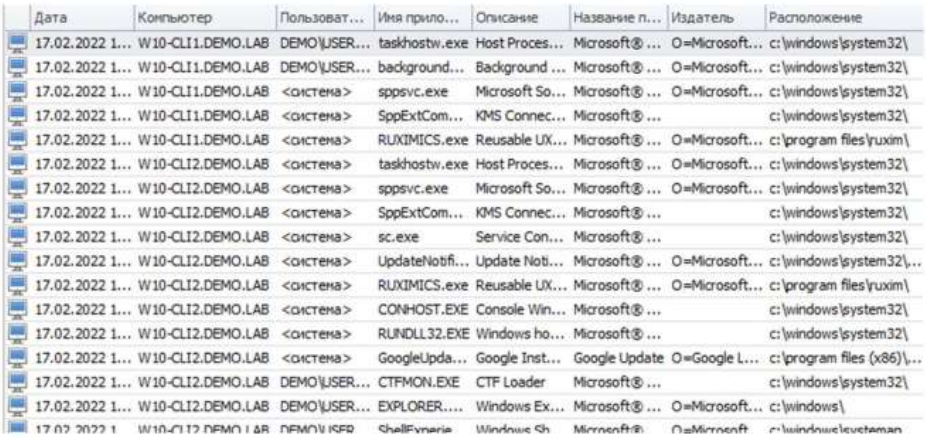


Рисунок 57 – «Создание правила»

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



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

Рисунок 58 – «Протокол приложений»

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

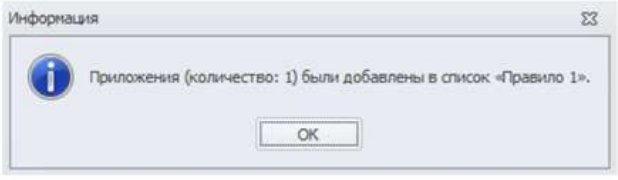


Рисунок 59 – «Успешное добавление приложения»

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

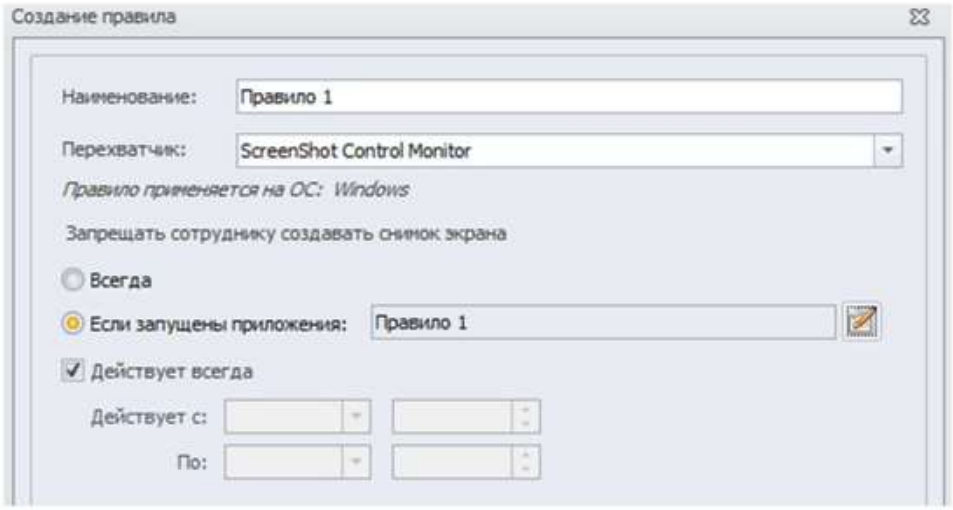


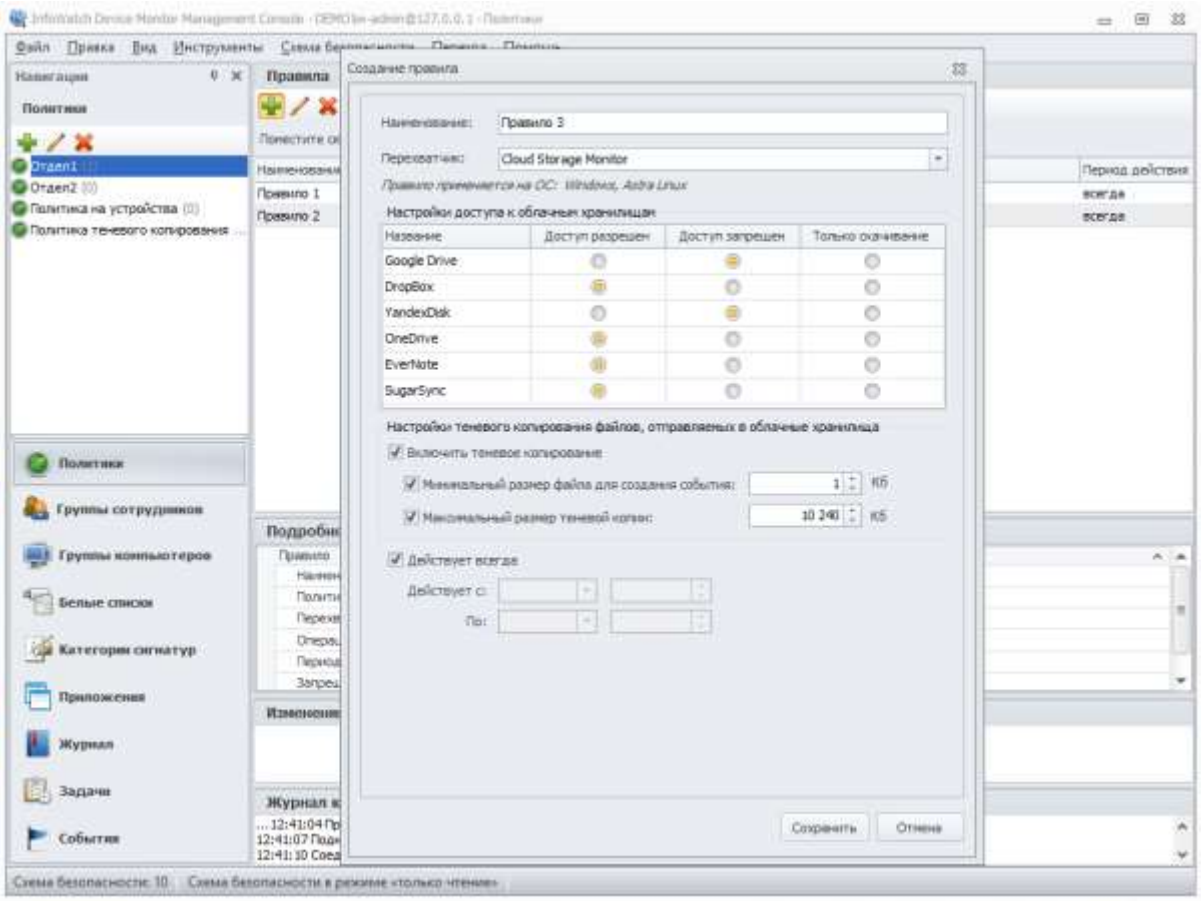
Рисунок 60 – «Правило 1»

Зафиксировать скриншотами необходимо!

Правило 3

Ограничить доступ к облачным хранилищам GoogleDrive и YandexDisk.

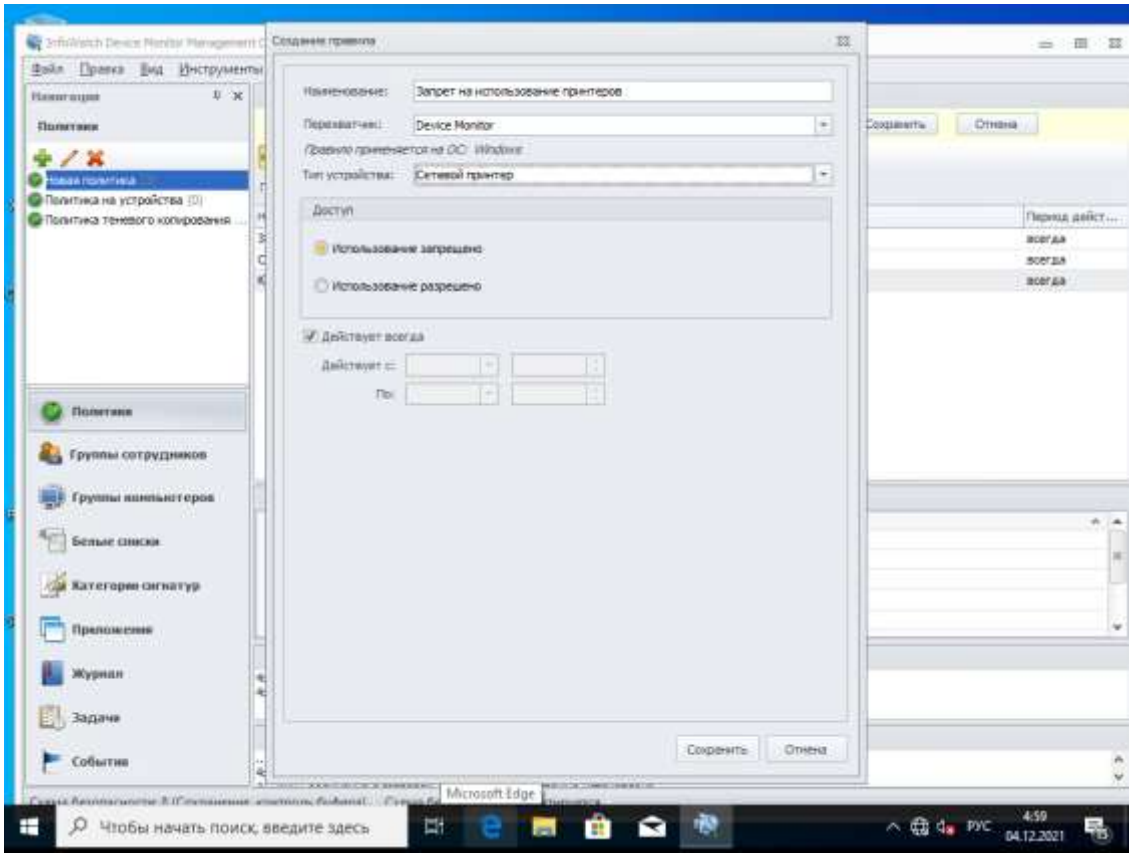
Проверить работоспособность и зафиксировать выполнение



Правило 4

Необходимо запретить печать на сетевых принтерах.

Зафиксировать создание политики скриншотом.

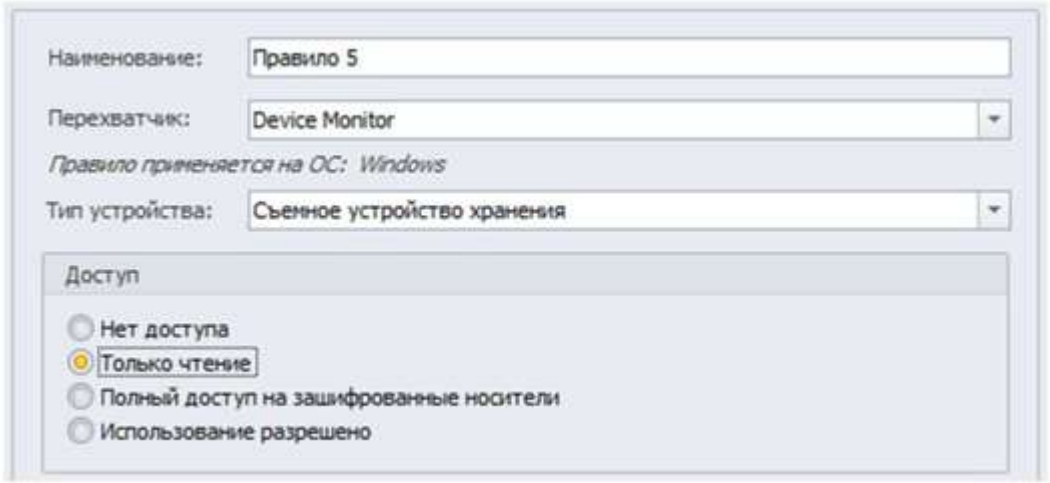


Зафиксировать создание политики скриншотом.

Правило 5

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

Проверить работоспособность и зафиксировать выполнение

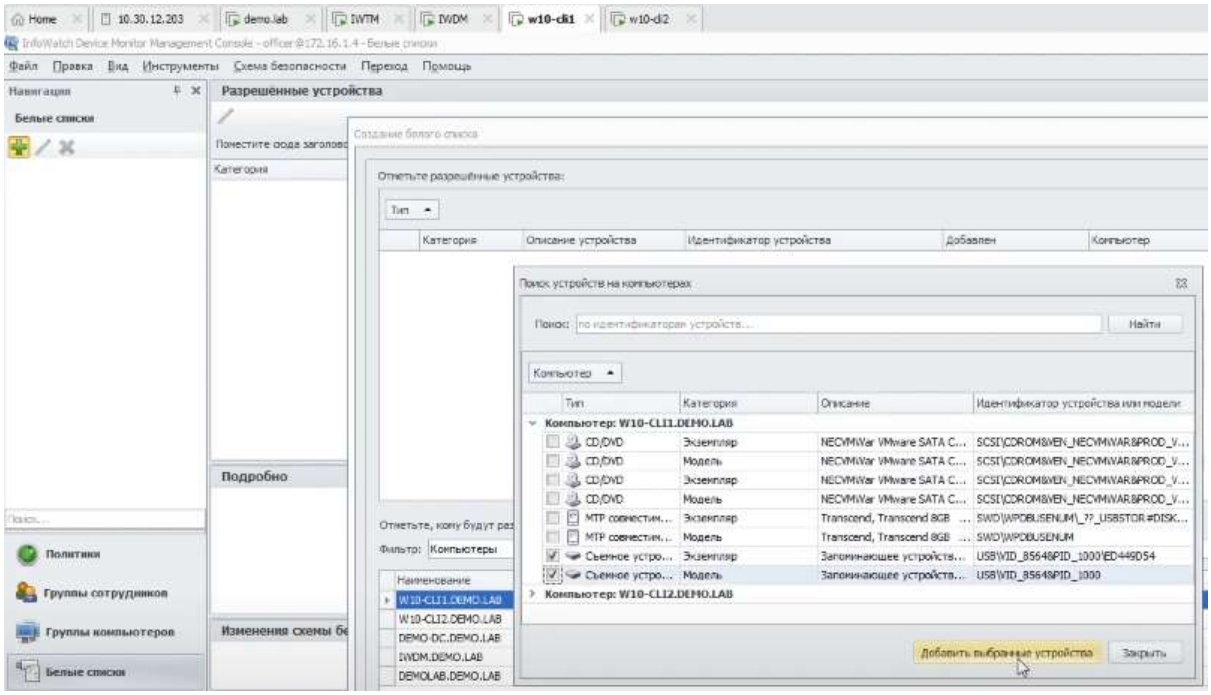


Проверить работоспособность и зафиксировать выполнение

Правило 6

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

Проверить работоспособность и зафиксировать выполнение

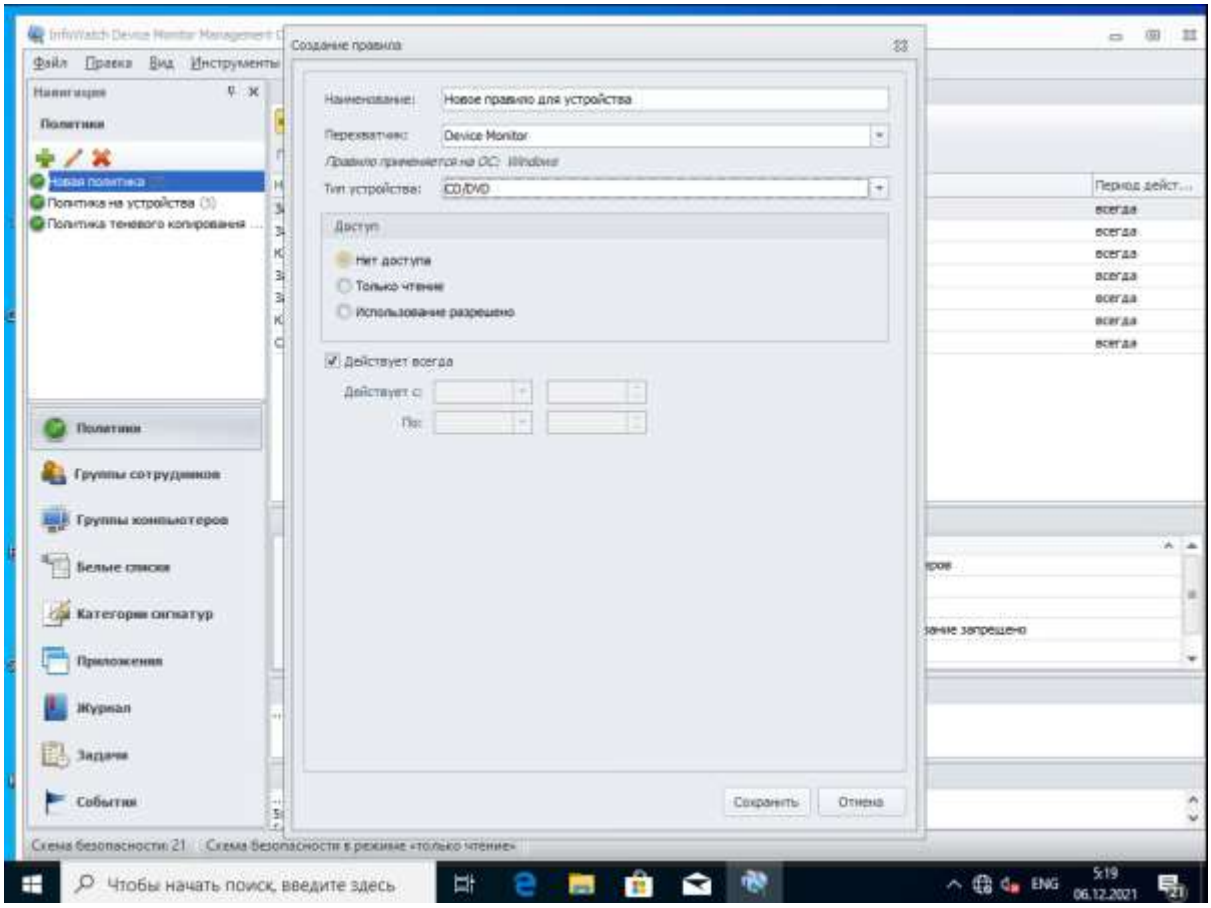


Проверить работоспособность и зафиксировать выполнение!

Правило 7

Полностью запретить использование CD/DVD-дисковода.

Проверить работоспособность и зафиксировать выполнение



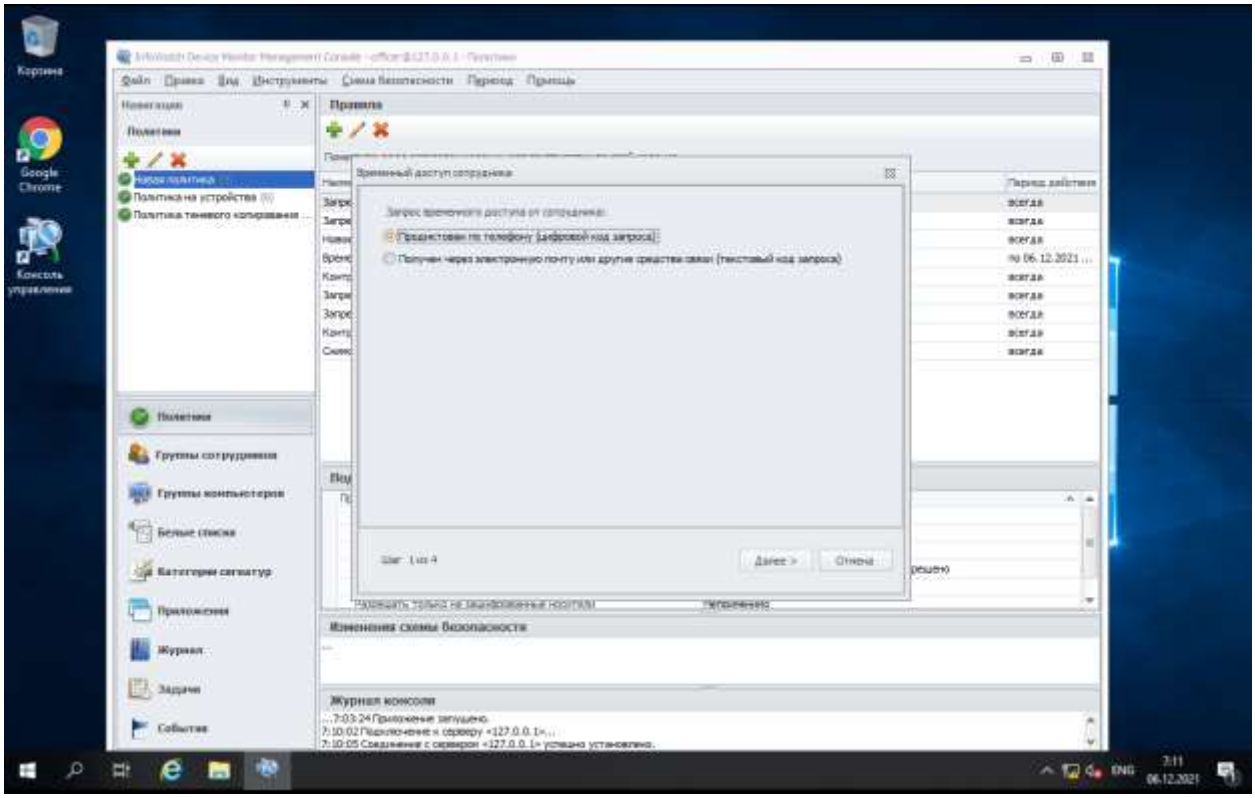
Проверить работоспособность и зафиксировать выполнение!

Правило 8

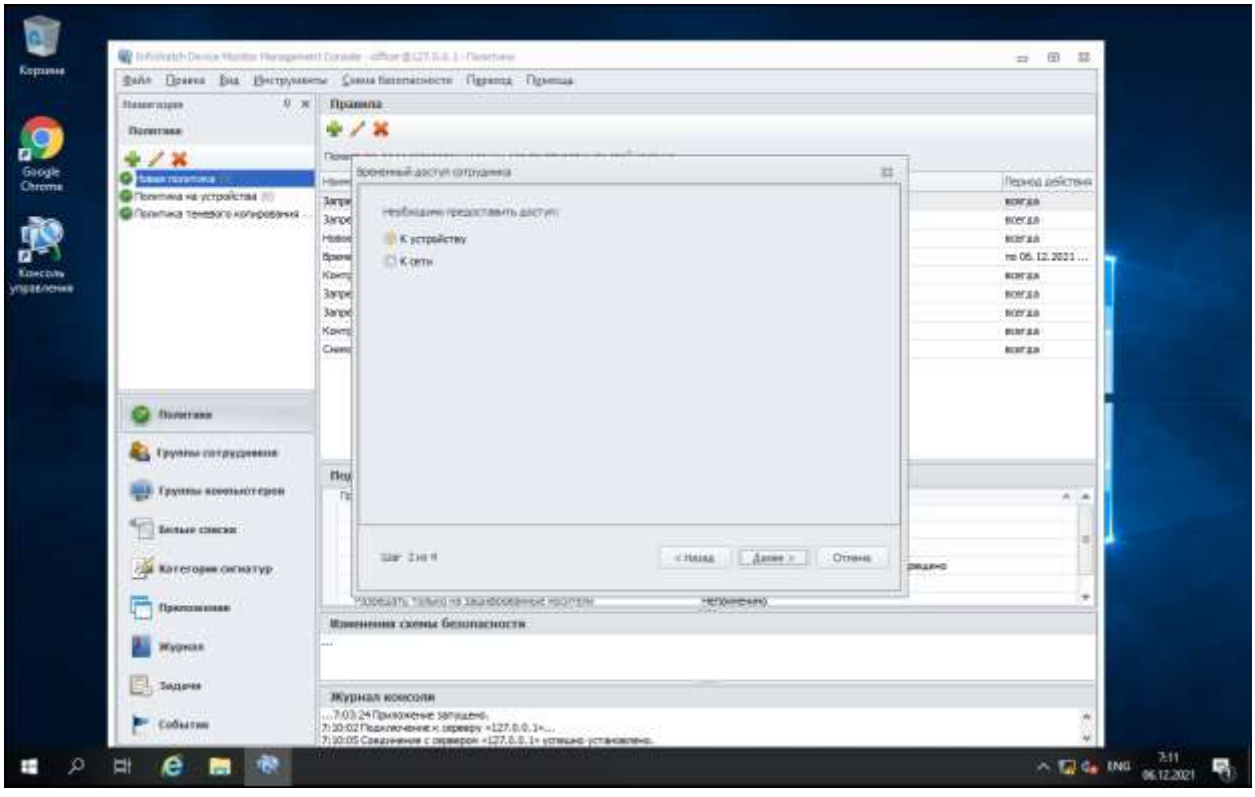
С учетом ранее выполненного запрета необходимо предоставить временный доступ для устройства на 7 минут для пользователя.

Зафиксировать этапы выдачи доступа и работоспособность скриншотами.

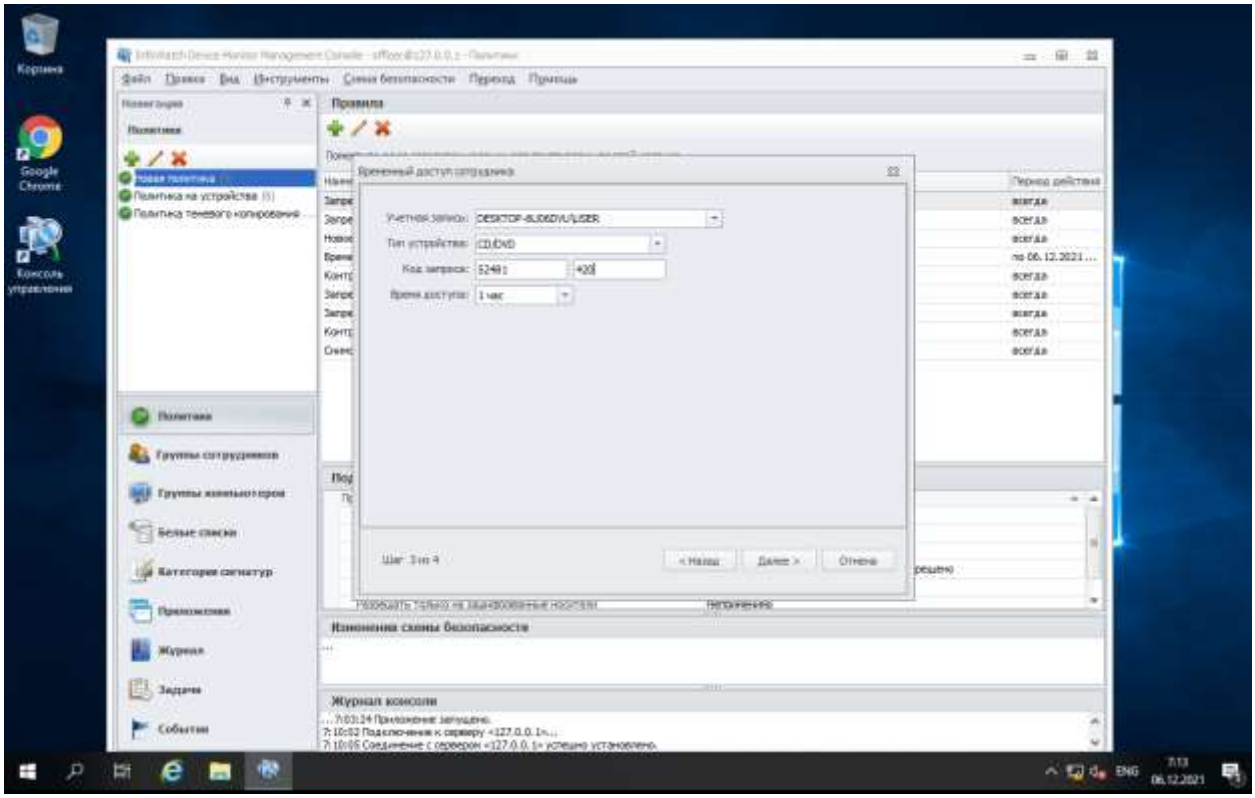
Выдаем временный доступ сотруднику



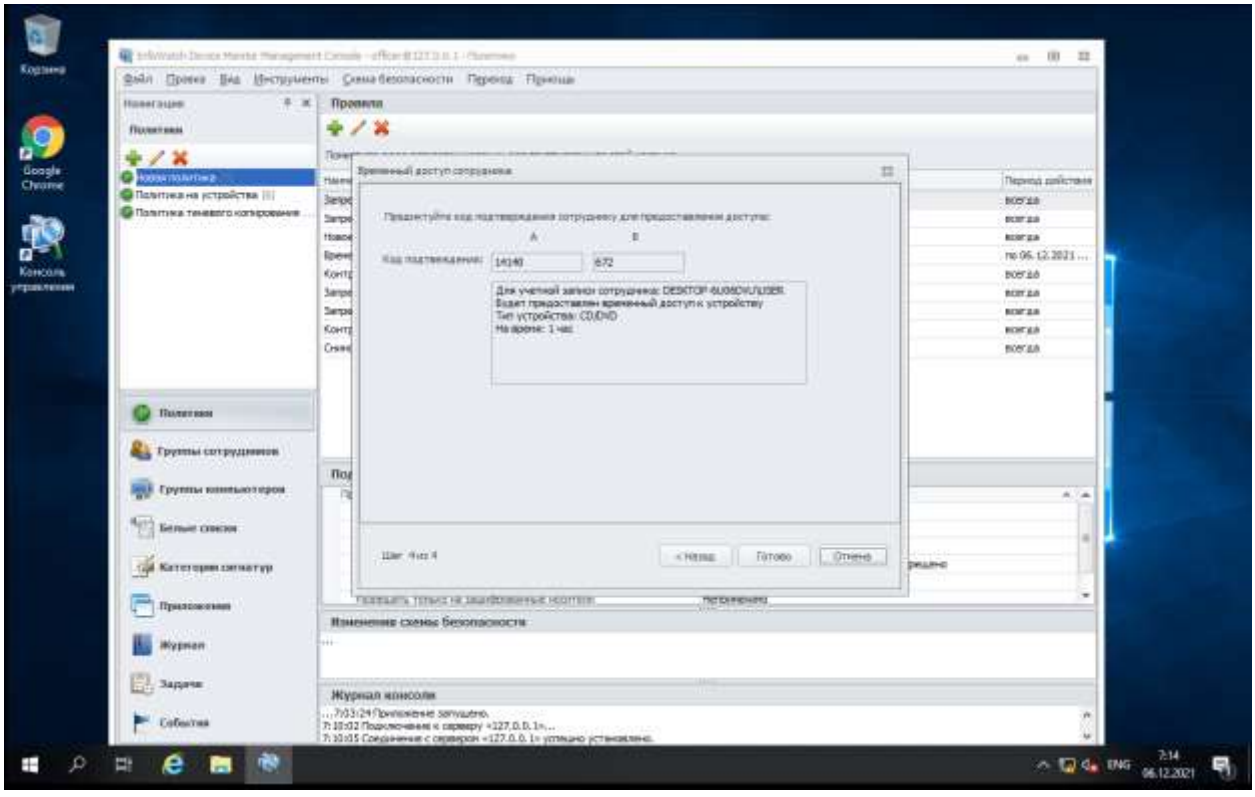
Предоставляем доступ к устройству



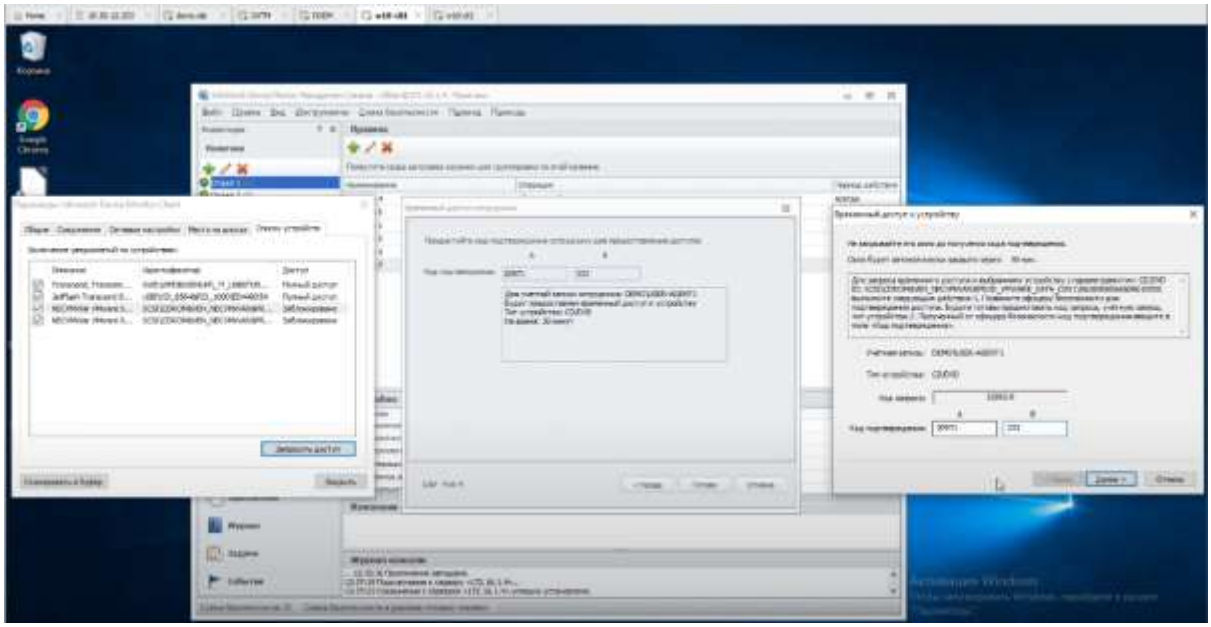
Выбираем компьютер, время доступа

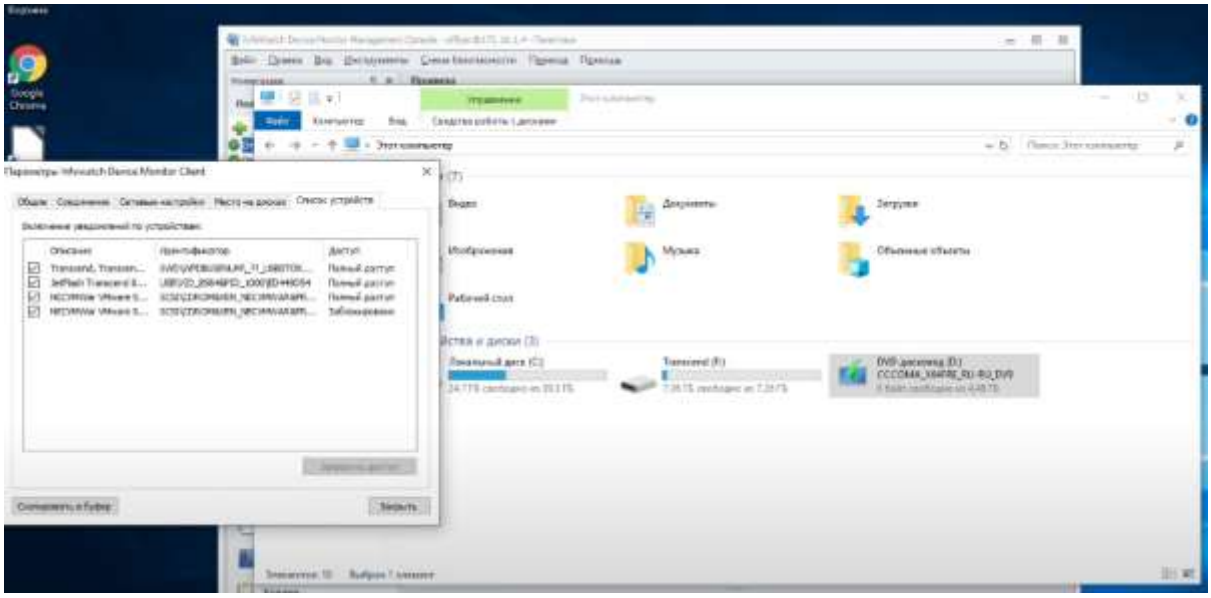


Временный доступ



Скриншотим





Зафиксировать этапы выдачи доступа и работоспособность скриншотами.

Следующие правила создаются в политике «Отдел2».

Следующие правила создаются в политике «Отдел2».

Правило 9

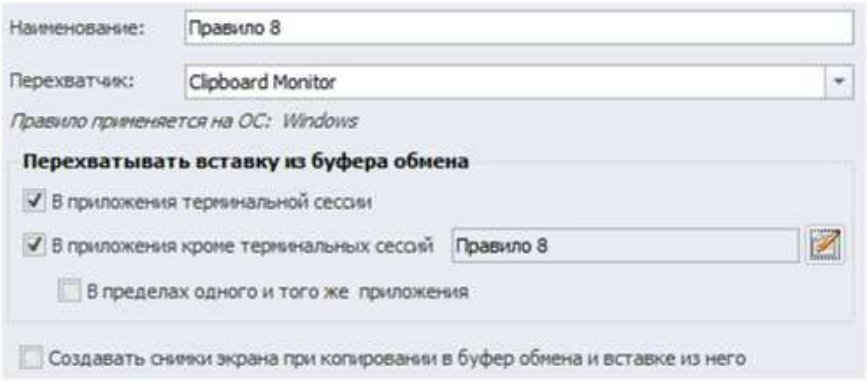
Необходимо поставить на контроль буфер обмена в блокноте и notepad++.

Проверить занесение нескольких событий в WEB-консоль.

Проверить работоспособность и зафиксировать выполнение скриншотом.

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

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

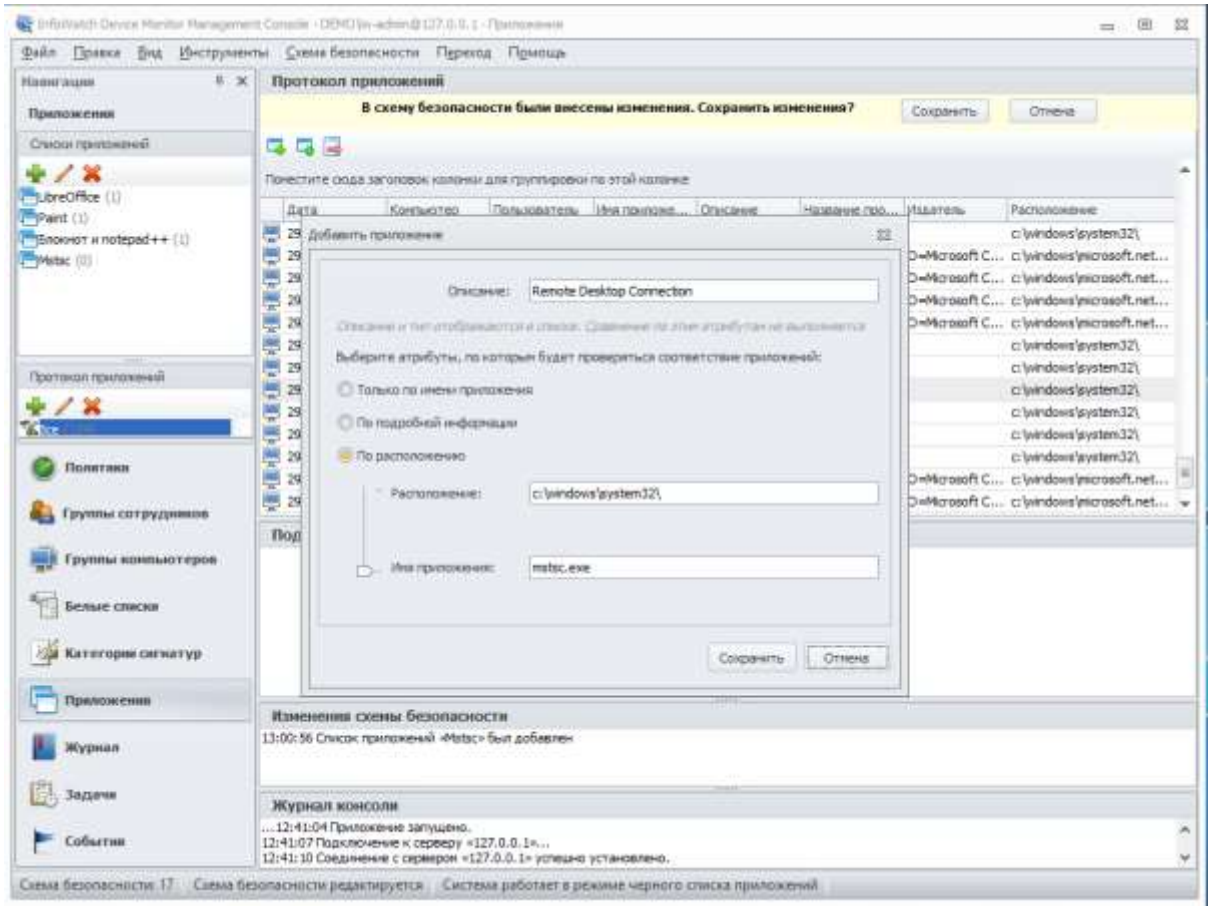


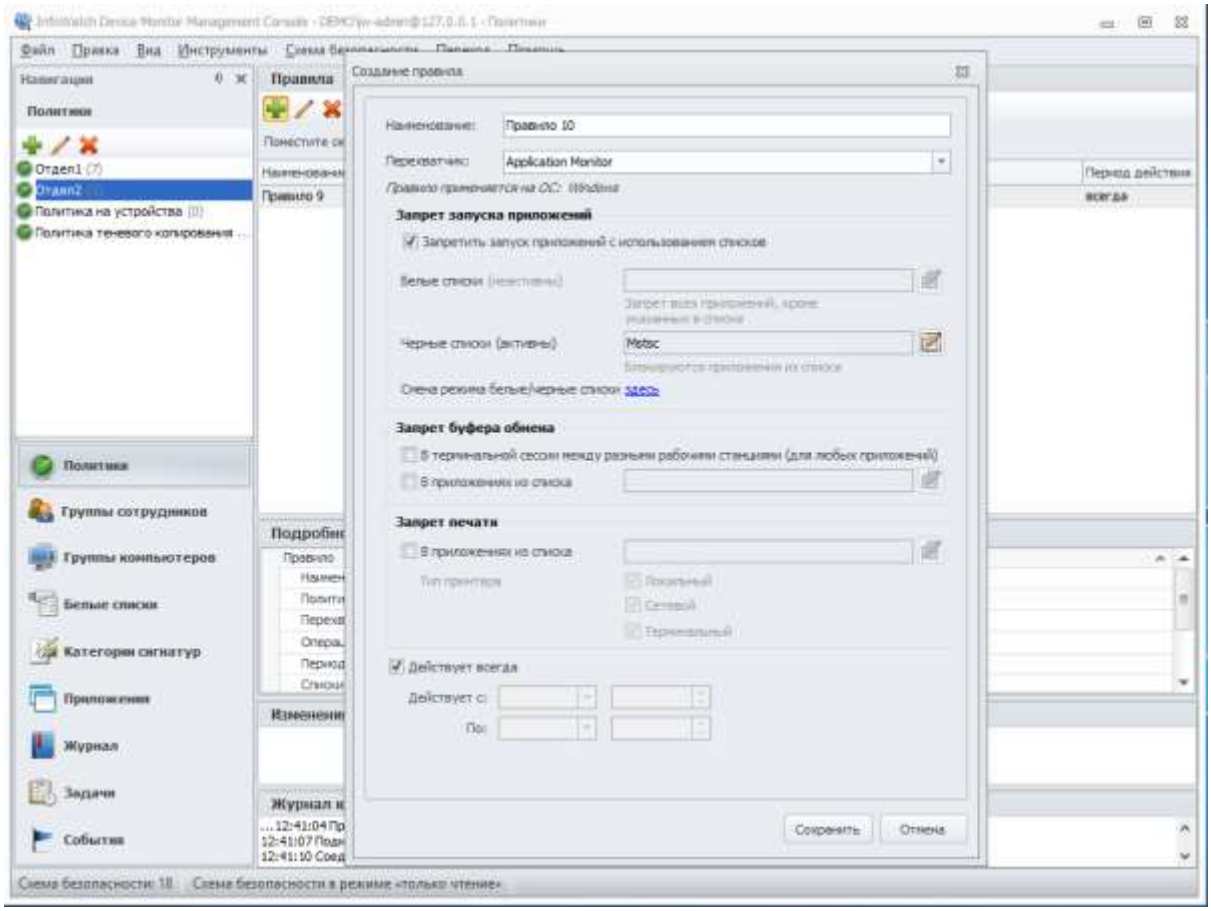
Проверить работоспособность и зафиксировать выполнение скриншотом. Чтобы проверить работоспособность нужно зайти в Device Monitor, затем журнал и там создать фильтр на 1000 записей, только после этого зафиксировать скриншотом

Правило 10

Необходимо запретить использовать терминальные сессии для пользователя.

Проверить работоспособность и зафиксировать выполнение


Файл Правка Вид Инструменты Схема безопасности Переход Помощь
Навигация
Приложения
Списки приложений
LibreOffice (1)
Paint (1)
Блокнот и notepad++ (1)
Mstsc (0)
Протокол приложений
Политики
Группы сотрудников
Группы компьютеров
Белые списки
Категории сигнатур
Приложения
Журнал
Задачи
События
Протокол приложений
В схему безопасности были внесены изменения. Сохранить изменения?
Сохранить
Отмена
Перенесите сюда заголовок колонки для группировки по этой колонке
Дата
Компьютер
Пользователь
Имя приложе...
Описание
Название про...
Издатель
Расположение
Добавить приложение
Описание:
Remote Desktop Connection
Выберите атрибуты, по которым будет проверяться соответствие приложений:
Только по имени приложения
По подробной информации
По расположению
Расположение:
c:\windows\system32\
Имя приложения:
mstsc.exe
Сохранить
Отмена
Изменения схемы безопасности
13:00:56 Список приложений «Mstsc» был добавлен
Журнал консоли
...12:41:04 Приложение запущено.
12:41:07 Подключение к серверу «127.0.0.1»...
12:41:10 Соединение с сервером «127.0.0.1» успешно установлено.
Схема безопасности: 17
Схема безопасности редактируется
Система работает в режиме черного списка приложений

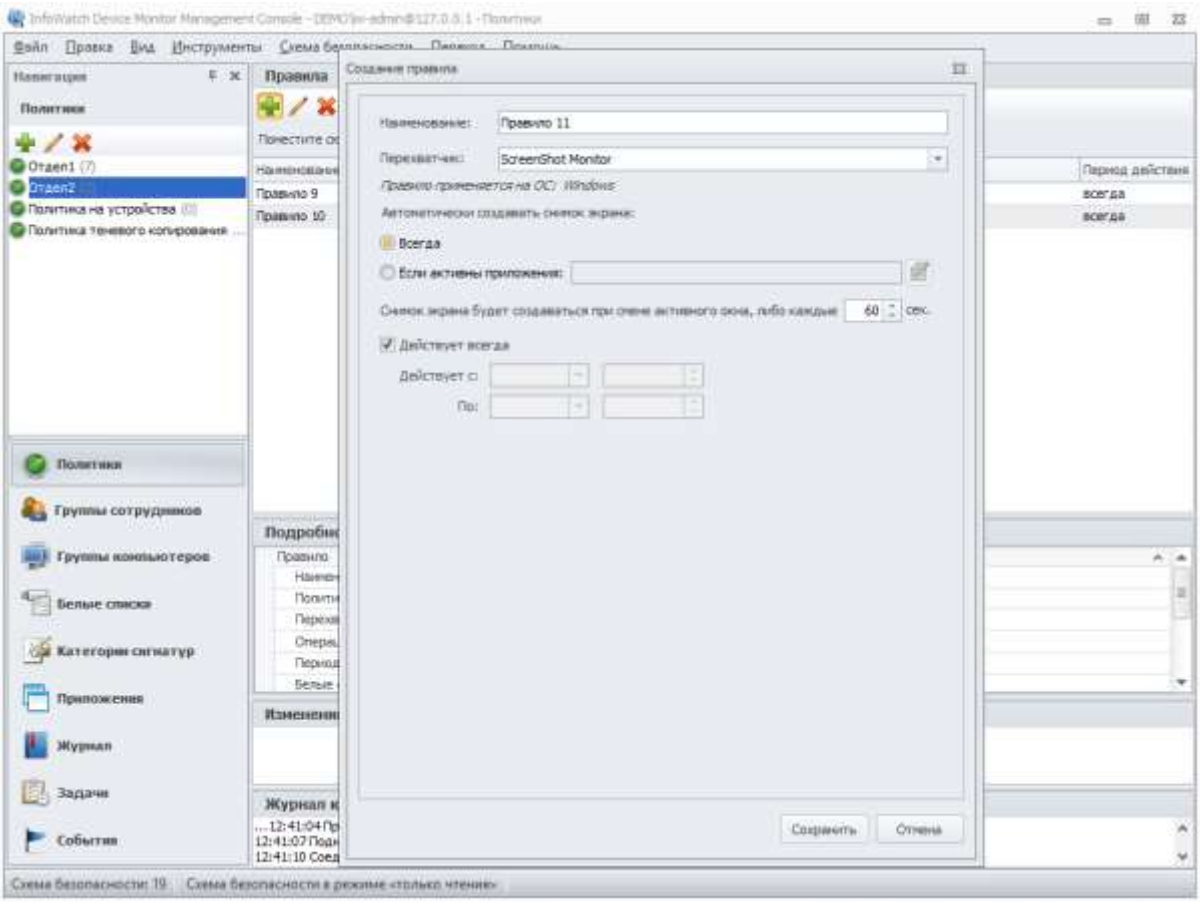


Проверить работоспособность и зафиксировать выполнение!

Правило 11

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

Проверить работоспособность и зафиксировать выполнение



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

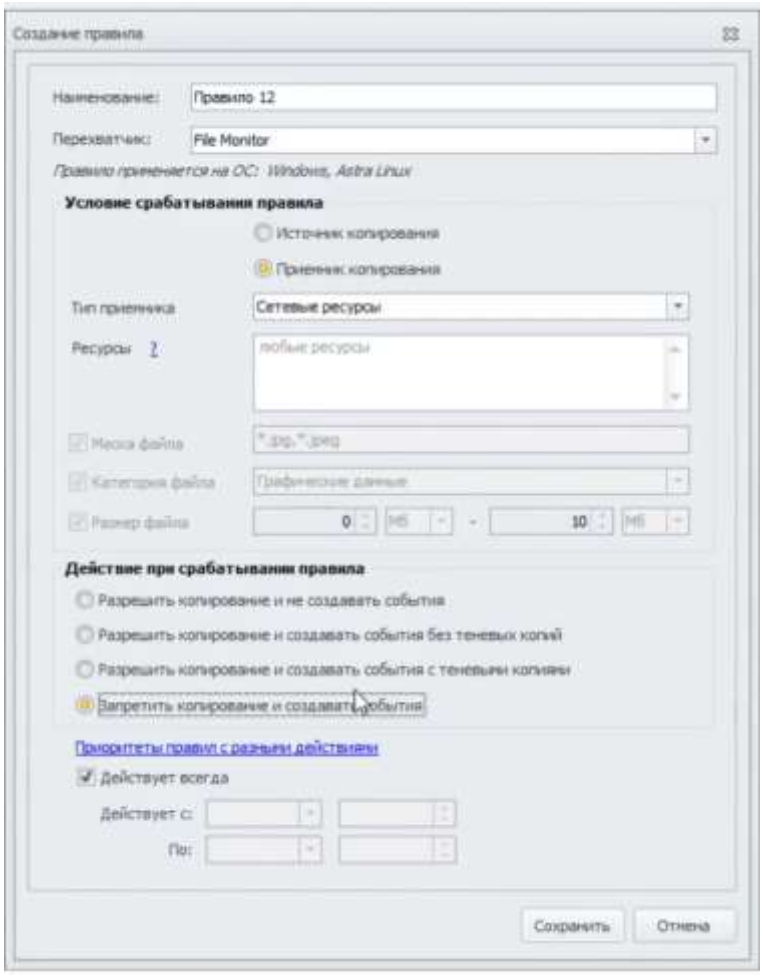
Проверить работоспособность и зафиксировать выполнение

Правило 12

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

Проверить работоспособность и зафиксировать выполнение

Галочку размер файла можно снять



Проверить работоспособность и зафиксировать выполнение!

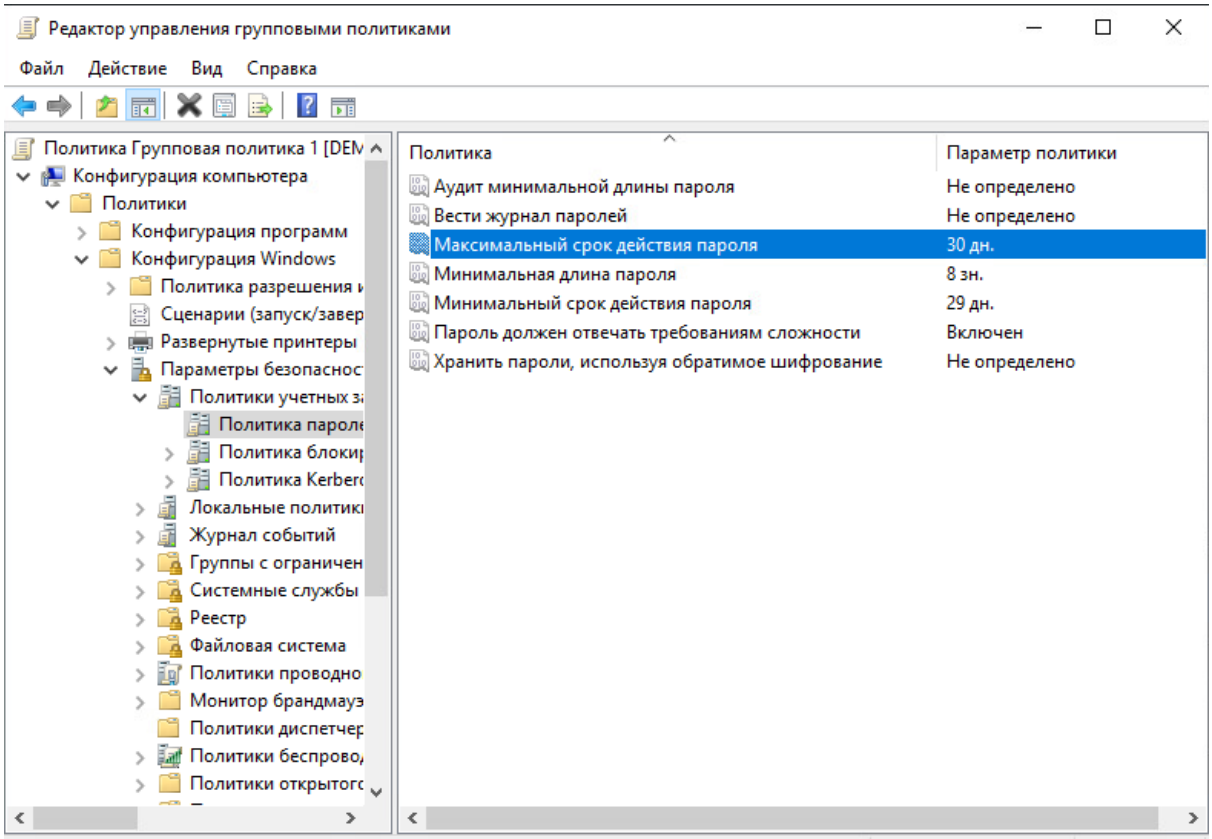
Групповые политики домена

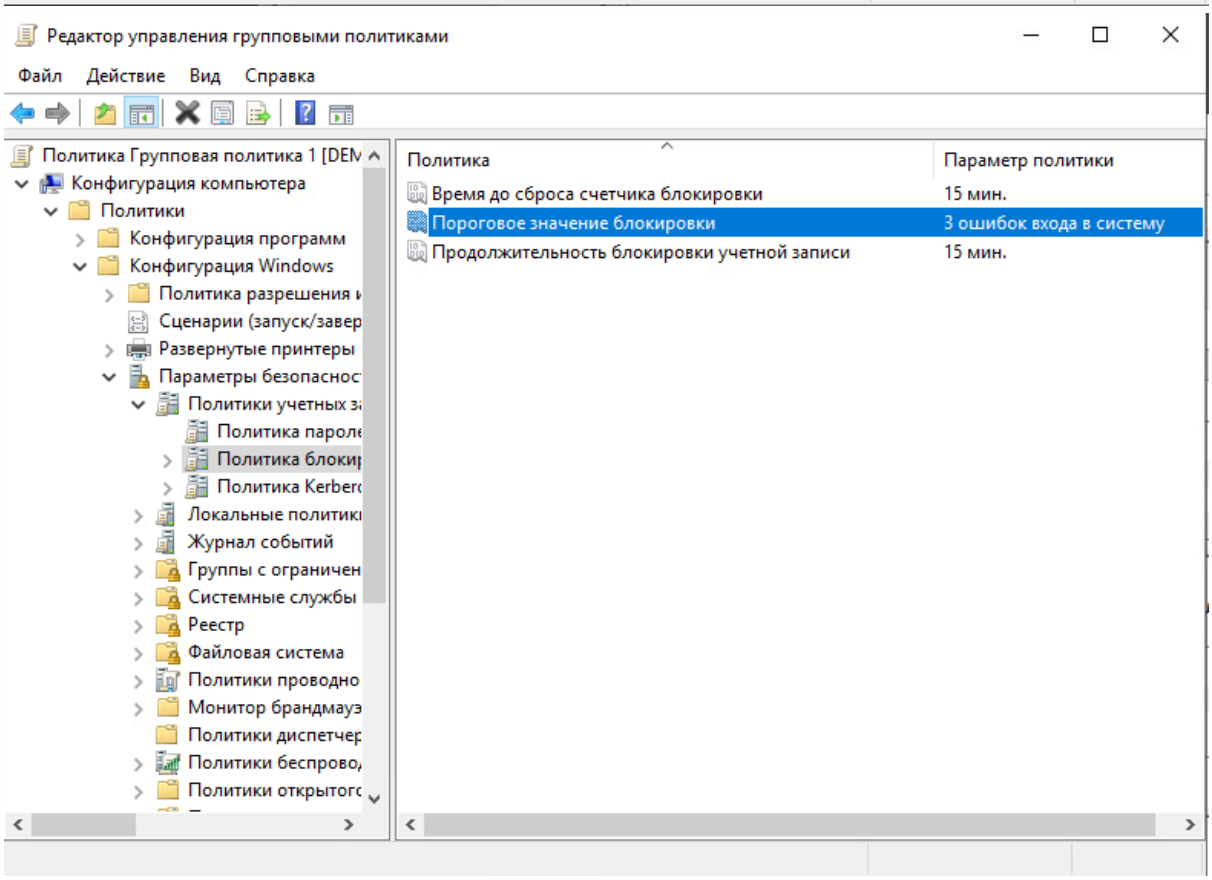
Групповые политики применяются только на компьютер 2, должны быть созданы в домене. Зафиксировать настройку политик скриншотами, при возможности проверки зафиксировать скриншотами проверку политик (например запрет запуска).

Групповая политика 1

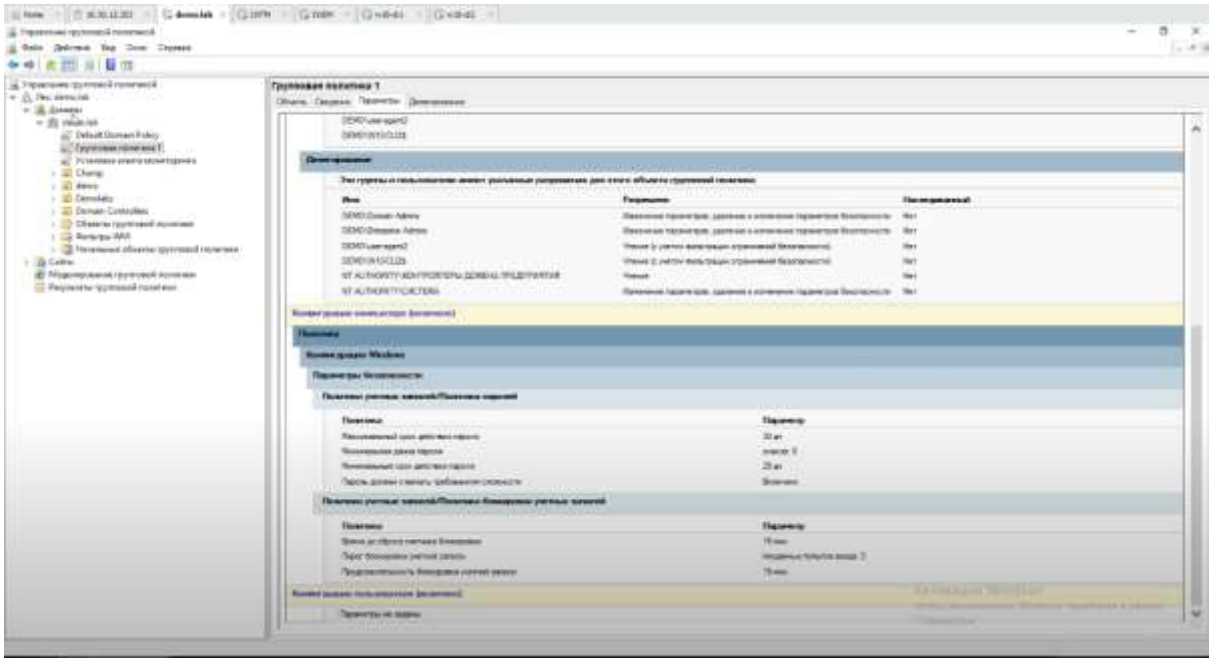
Настроить политику паролей и блокировки: Максимальный срок действия пароля - 30 дней, Минимальная длина пароля - 8, пароль должен отвечать требованиям сложности, Блокировка учетной записи при повторном вводе неверного пароля (3 раза), продолжительность блокировки 15 минут.

Зафиксировать настройки политики скриншотами.


Редактор управления групповыми политиками
Файл Действие Вид Справка
Политика Групповая политика 1 [DEM
Конфигурация компьютера
Политики
Конфигурация программ
Конфигурация Windows
Политика разрешения и
Сценарии (запуск/завер
Развернутые принтеры
Параметры безопаснос
Политики учетных за
Политика паролe
Политика блокир
Политика Kerberc
Локальные политики
Журнал событий
Группы с ограничен
Системные службы
Реестр
Файловая система
Политики проводно
Монитор брандмауэ
Политики диспетчер
Политики беспрово
Политики открытогс
Политика
Параметр политики
Аудит минимальной длины пароля
Не определено
Вести журнал паролей
Не определено
Максимальный срок действия пароля
30 дн.
Минимальная длина пароля
8 зн.
Минимальный срок действия пароля
29 дн.
Пароль должен отвечать требованиям сложности
Включен
Хранить пароли, используя обратимое шифрование
Не определено


Редактор управления групповыми политиками
Файл Действие Вид Справка
Политика Групповая политика 1 [DEM
Конфигурация компьютера
Политики
Конфигурация программ
Конфигурация Windows
Политика разрешения и
Сценарии (запуск/завер
Развернутые принтеры
Параметры безопаснос
Политики учетных за
Политика паролe
Политика блокир
Политика Kerberc
Локальные политики
Журнал событий
Группы с ограничен
Системные службы
Реестр
Файловая система
Политики проводно
Монитор брандмауэ
Политики диспетчер
Политики беспрово
Политики открытогс
Политика
Параметр политики
Время до сброса счетчика блокировки
15 мин.
Пороговое значение блокировки
3 ошибок входа в систему
Продолжительность блокировки учетной записи
15 мин.

Скриншот



Зафиксировать настройки политики скриншотами.

Групповая политика 2

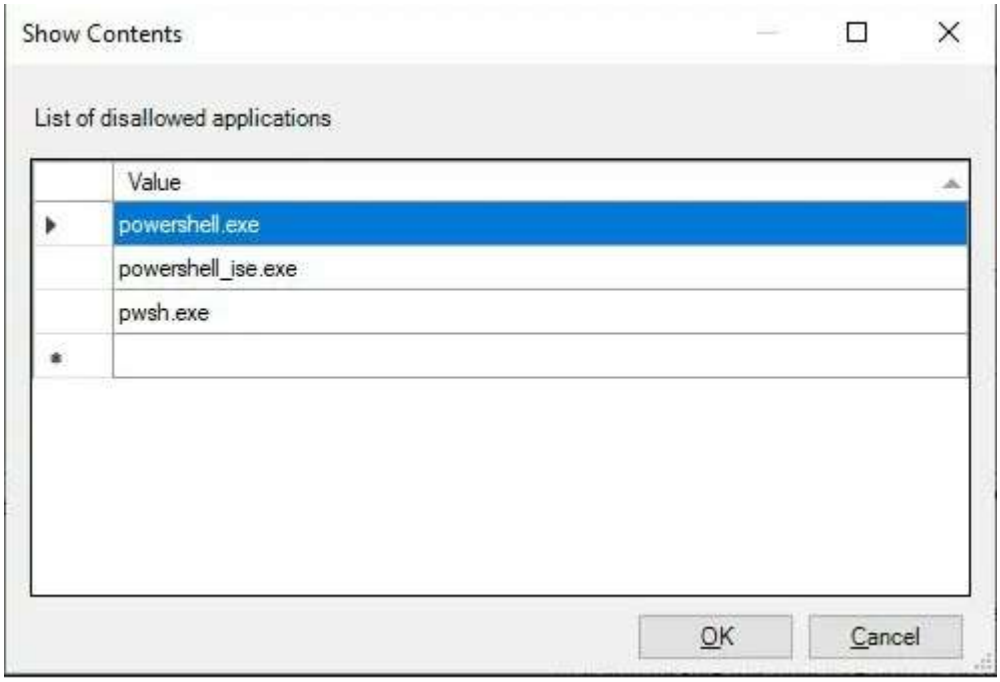
Запретить запуск приложений по списку: PowerShell, ножницы, сведения о системе.

Зафиксировать настройки политики и выполнение скриншотами.

Конфигурация пользователя → Политики → Административные шаблоны → Система

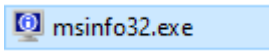
Включаем политики → “Не запускать указанные приложения Windows”

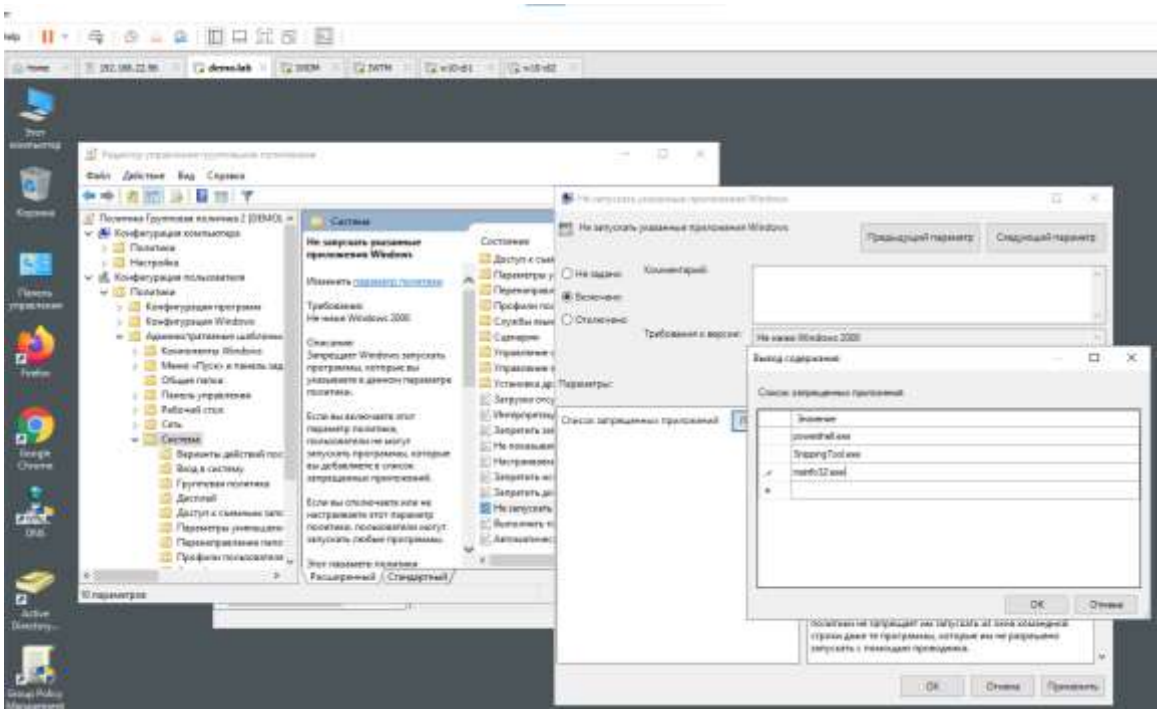
Нажимаем кнопку → Показать и вводим список команд, запускающих PowerShell



Также вводим ножницы

И сведения о системе





Зафиксировать настройки политики и выполнение скриншотами.

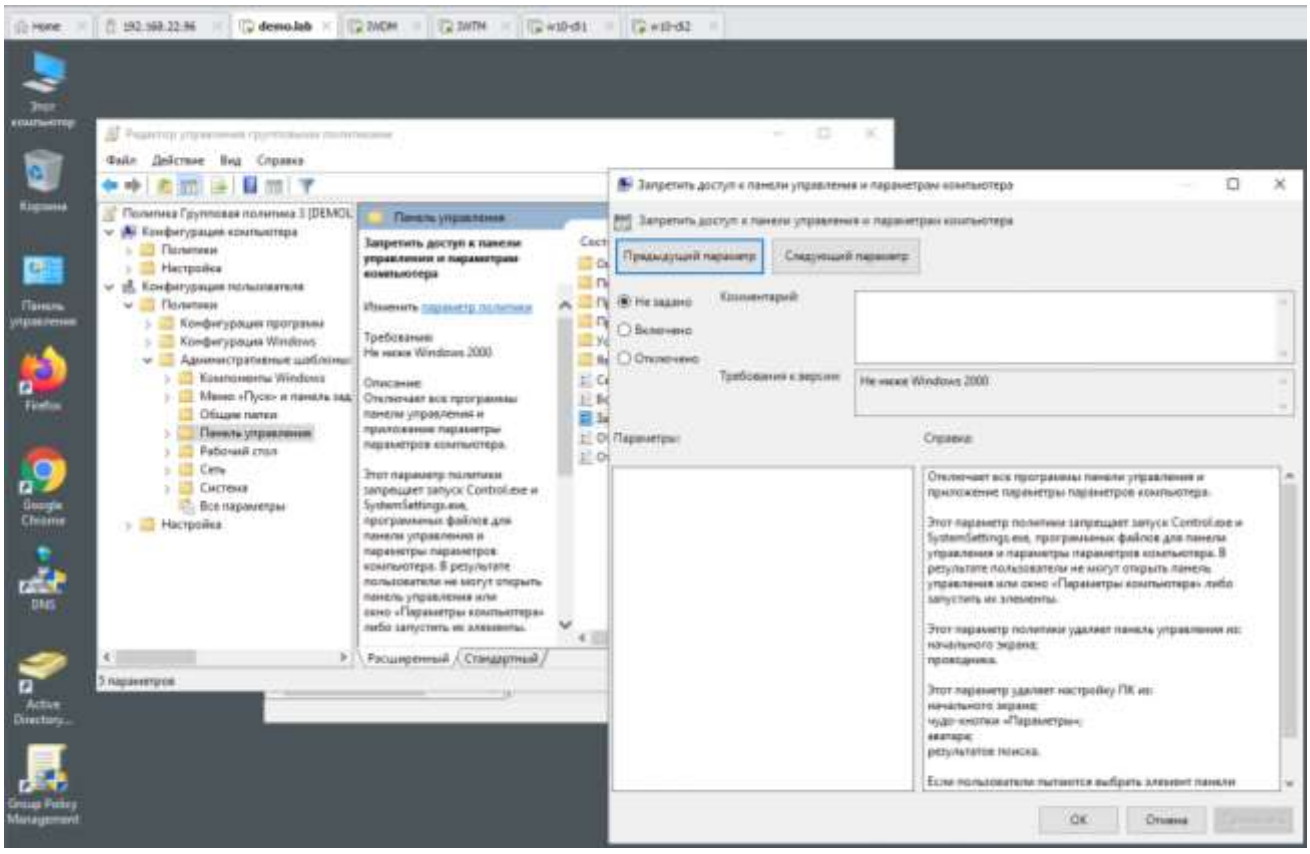
Групповая политика 3

Запретить использование панели управления стандартными политиками.

Зафиксировать настройки политики и выполнение скриншотами.

Создаем новую политику безопасности переходим к её редактированию

Конфигурация пользователя → Политики → Административные шаблоны → Панель управления
Здесь нужно включить политику → “Запретить доступ к панели управления”

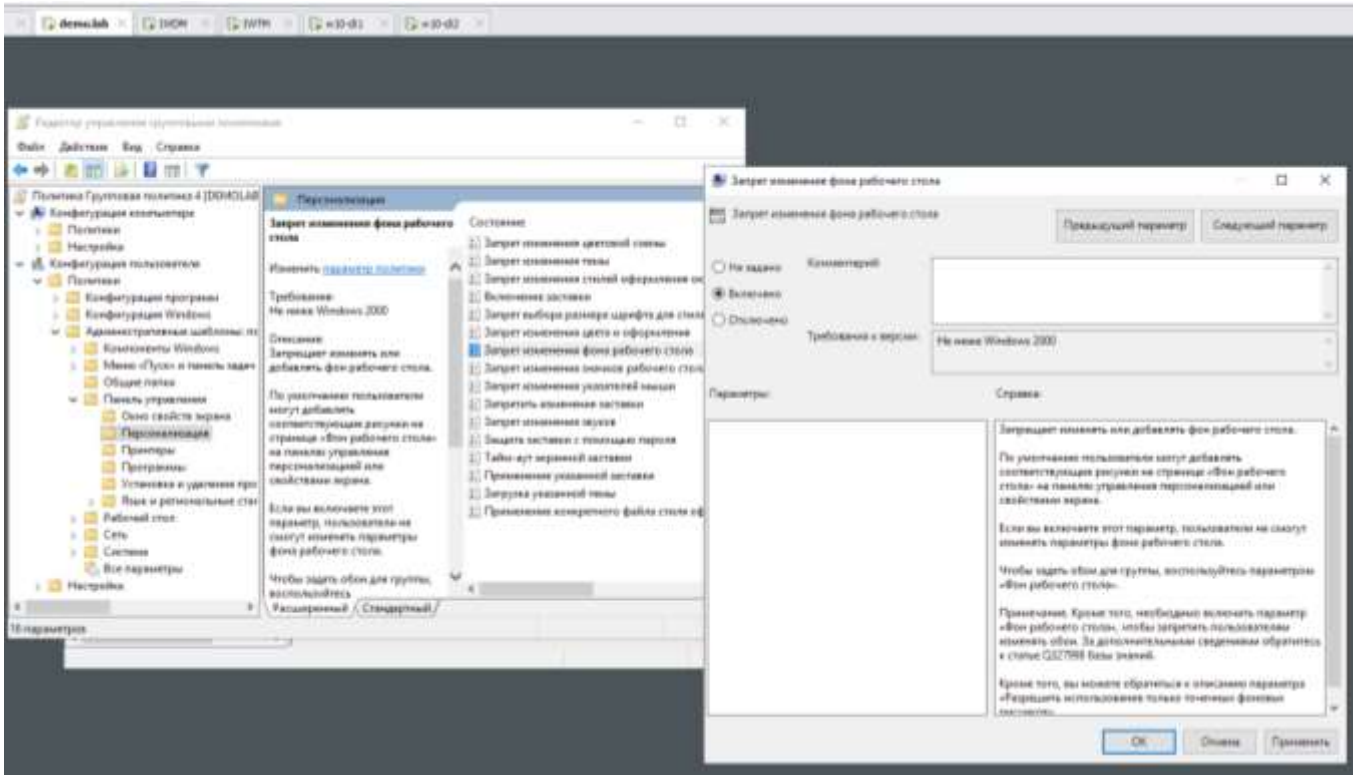


Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 4
Запретить пользователю самостоятельно менять обои рабочего стола.
Зафиксировать настройки политики и выполнение скриншотами.

Конфигурация пользователя → Административные шаблоны – Панель управления – Персонализация.

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



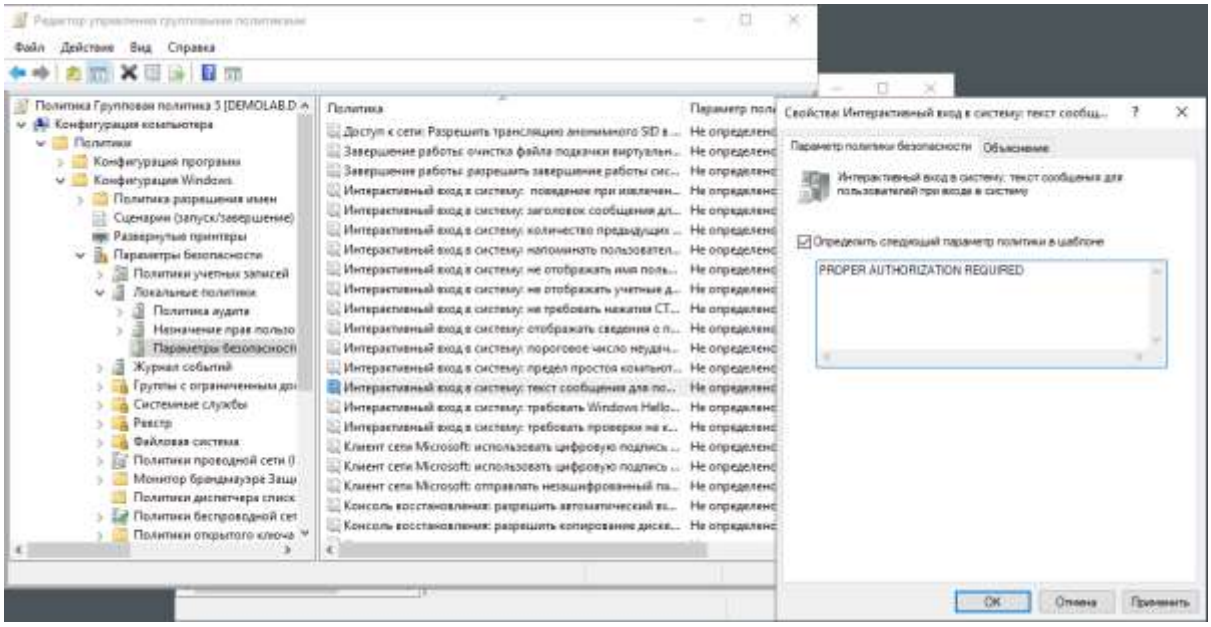
Зафиксировать настройки политики и выполнение скриншотами.

Групповая политика 5

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

Зафиксировать настройки политики и выполнение скриншотами.

Создаем новую политику безопасности переходим к её редактированию
Переходим по пути в → Параметры безопасности



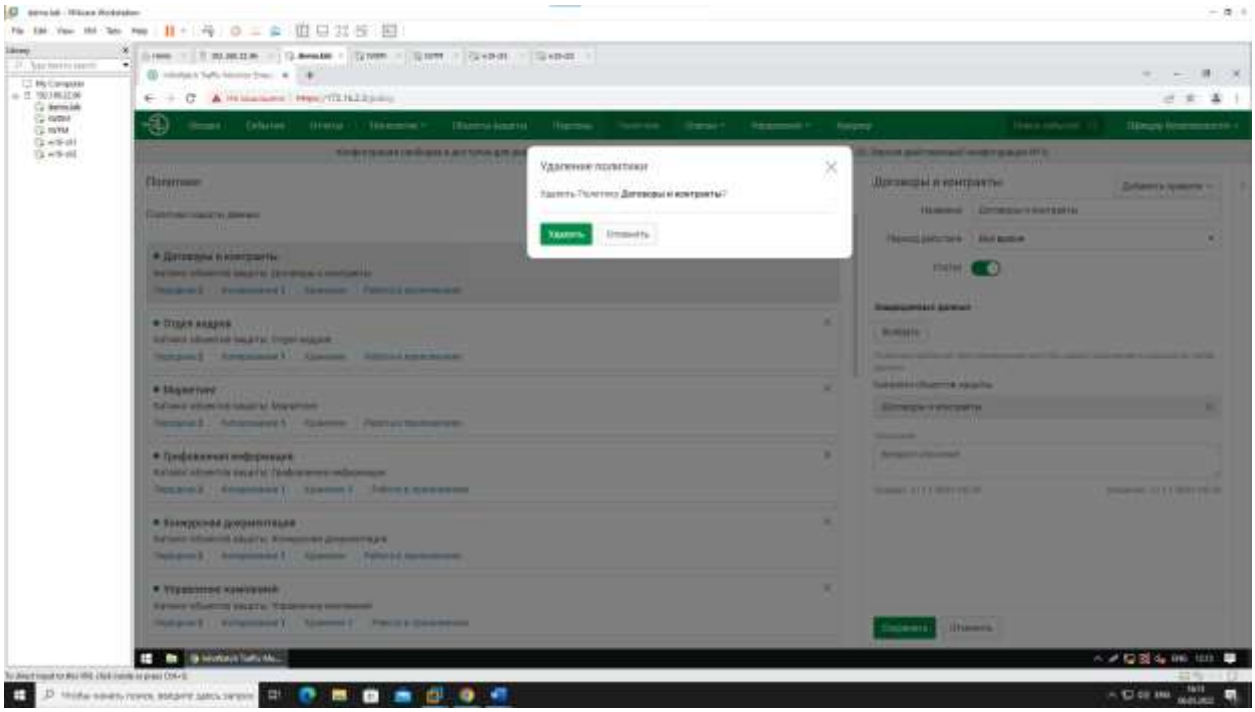
Включаем следующий элемент настройки и вводим нужный текст → “ сообщение с именем сервера авторизации” – Сервер авторизации: demo.lab

Зафиксировать настройки политики и выполнение скриншотами.

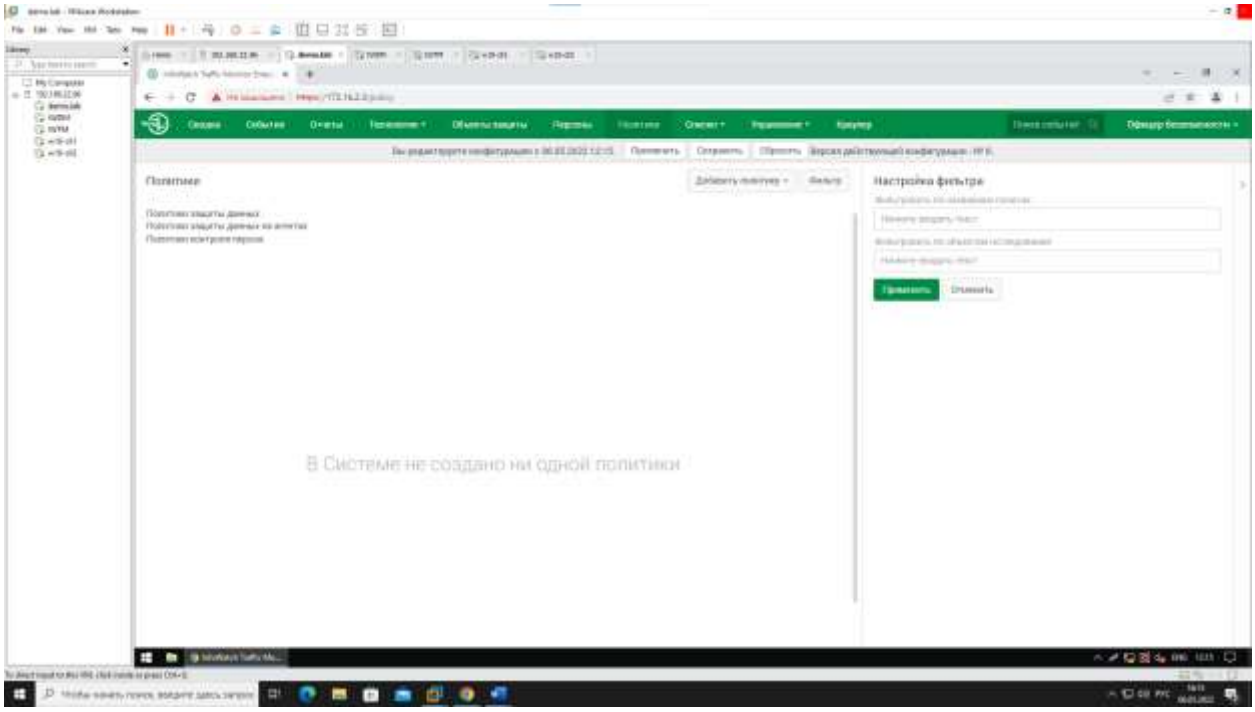
После всего этого применяем групповые политики через cmd → gpupdate /force и смотрим результат: запускаем панель управления на агенте2 и фиксируем работу политики

Модуль 3

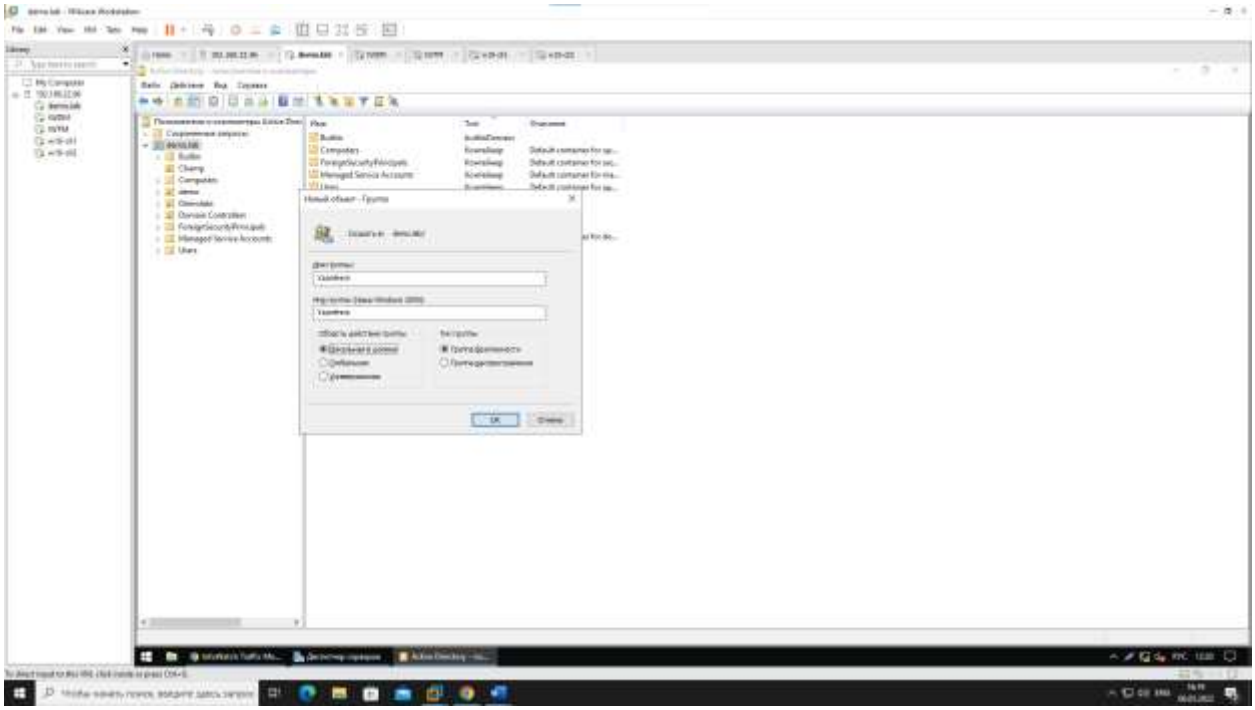
Удаляем все стандартные политики



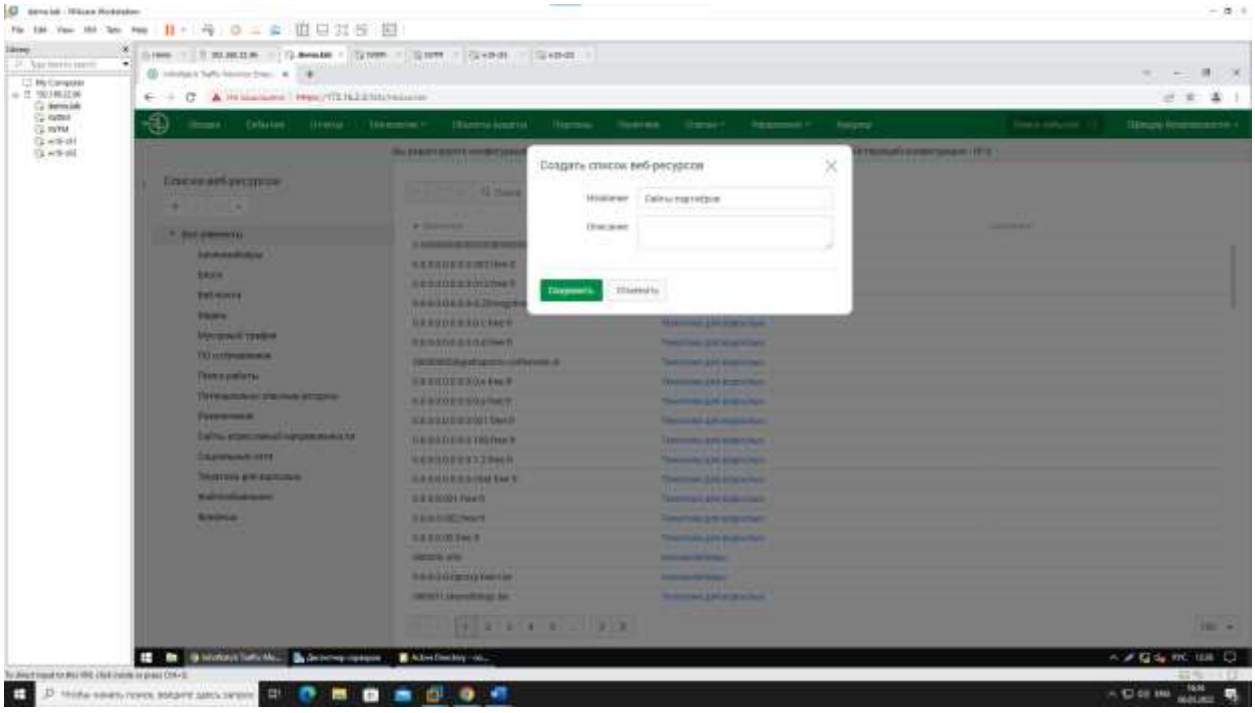
После удаления выглядит вот так



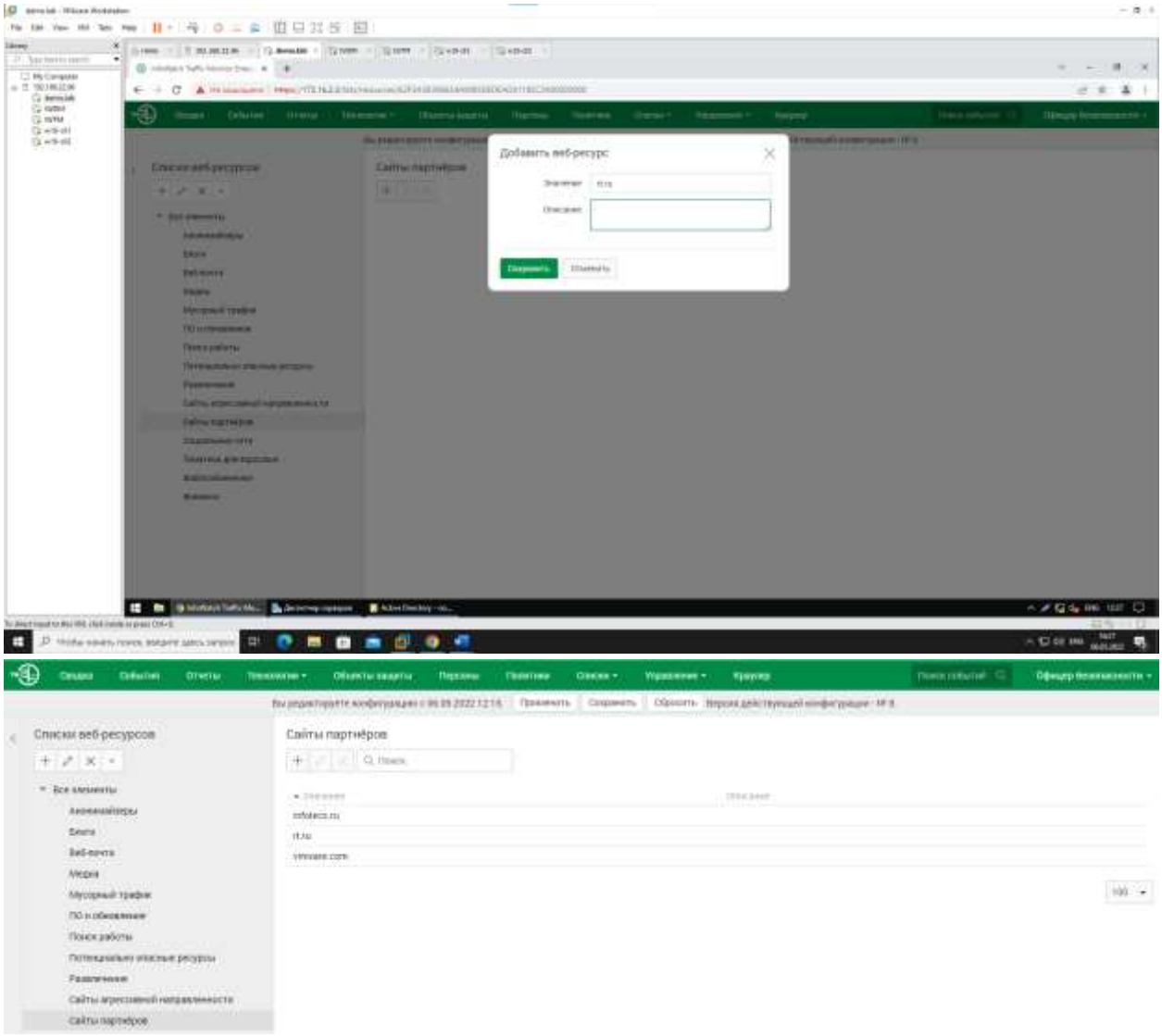
Создаем локальную группу с название – удалёнка



Создаем список веб ресурсов (Списки – Веб-ресурсы)

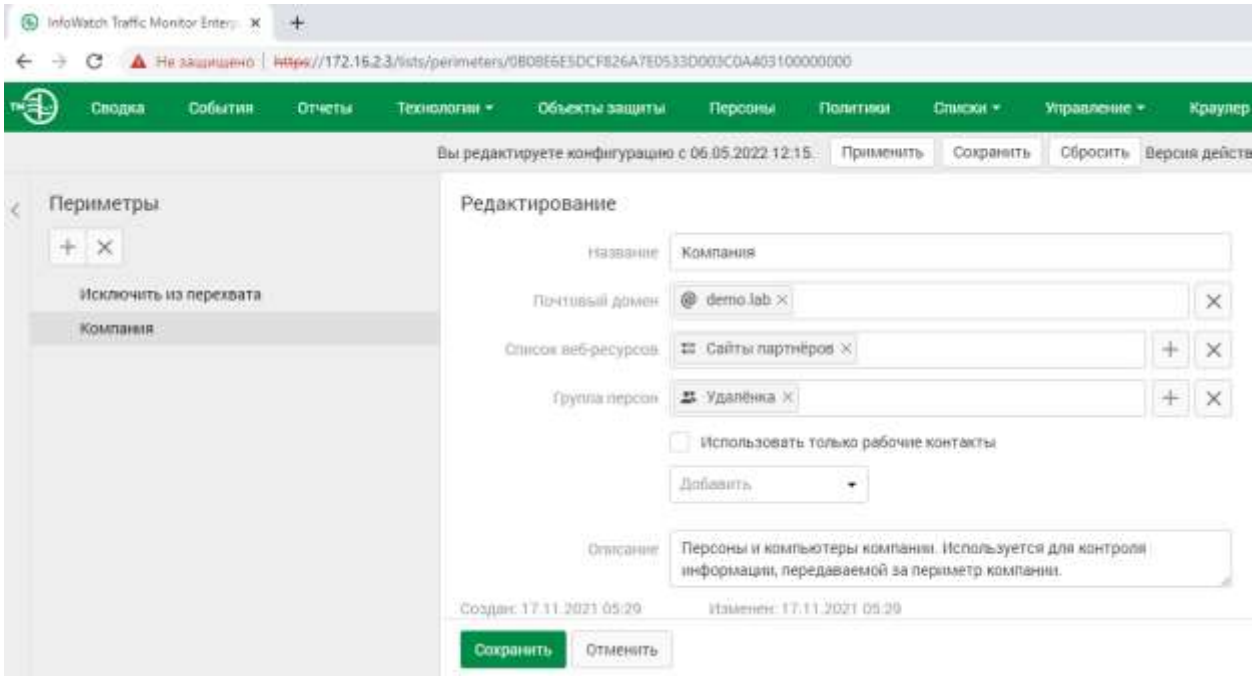


Добавляем веб-ресурсы

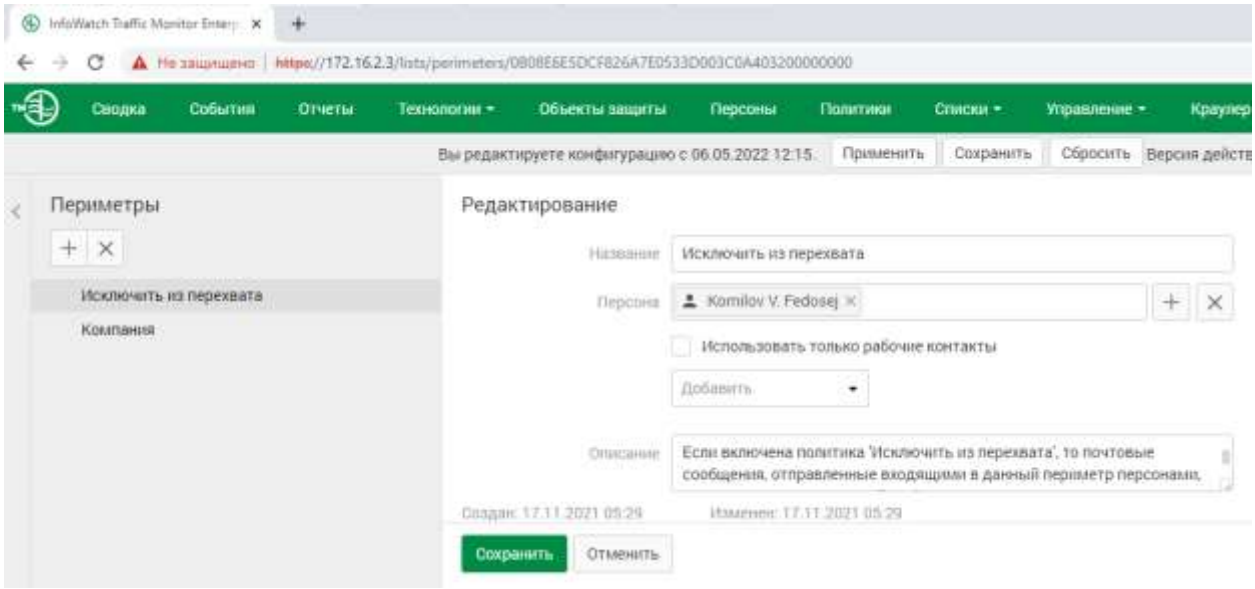


Задание 4

Периметр компании



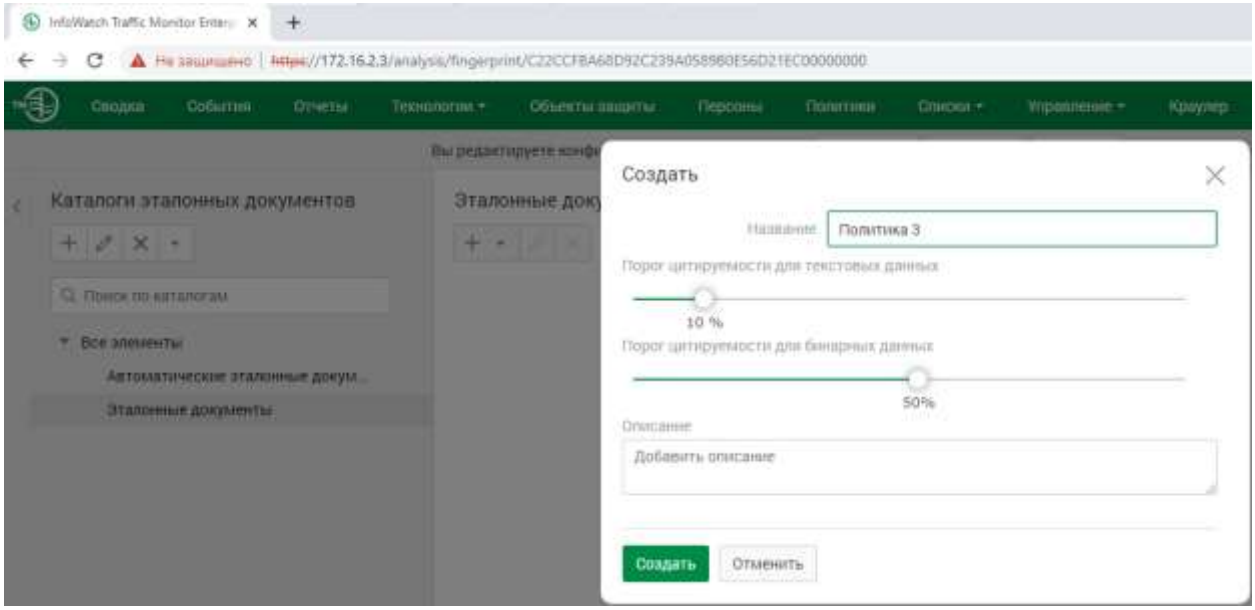
Исключение из перехвата



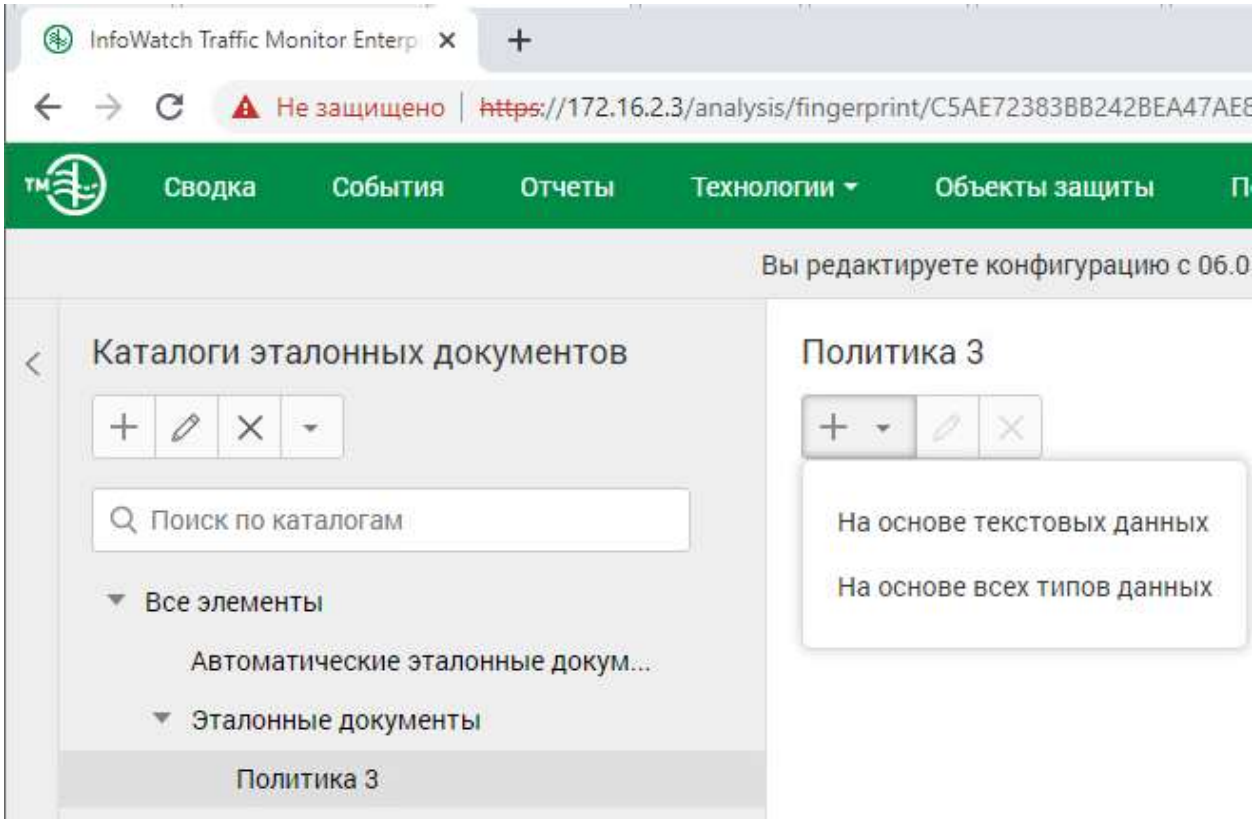
В ПОСЛЕДНЮЮ ОЧЕРЕДЬ

Политика 3

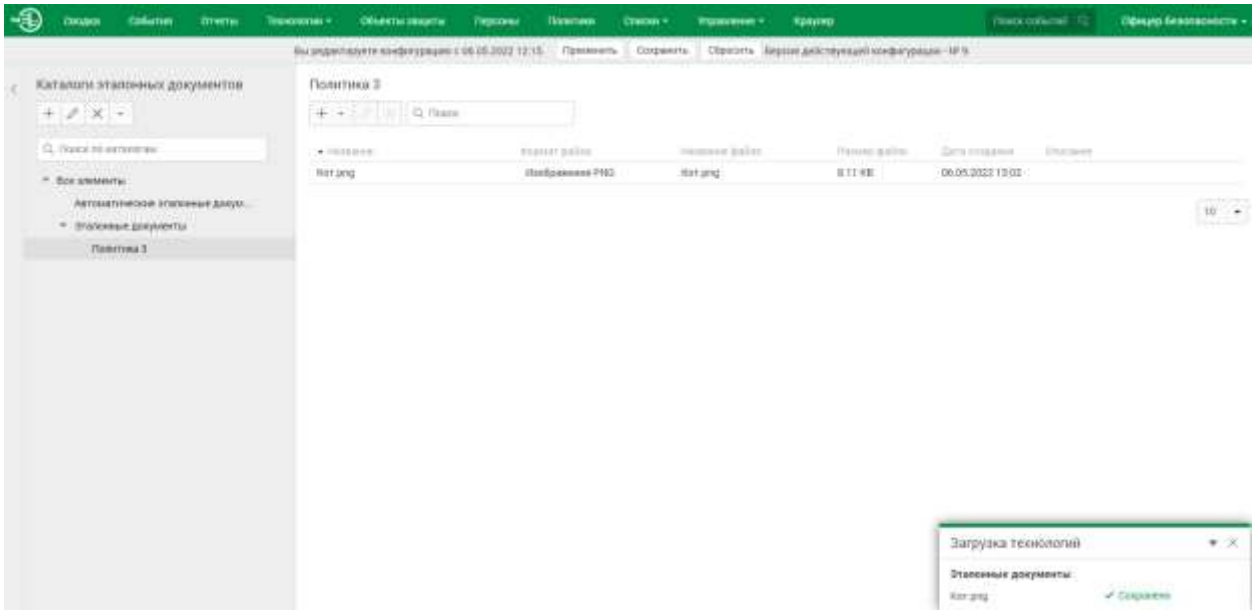
Технологии – Эталонные документы, создаем политику в эталонных документах



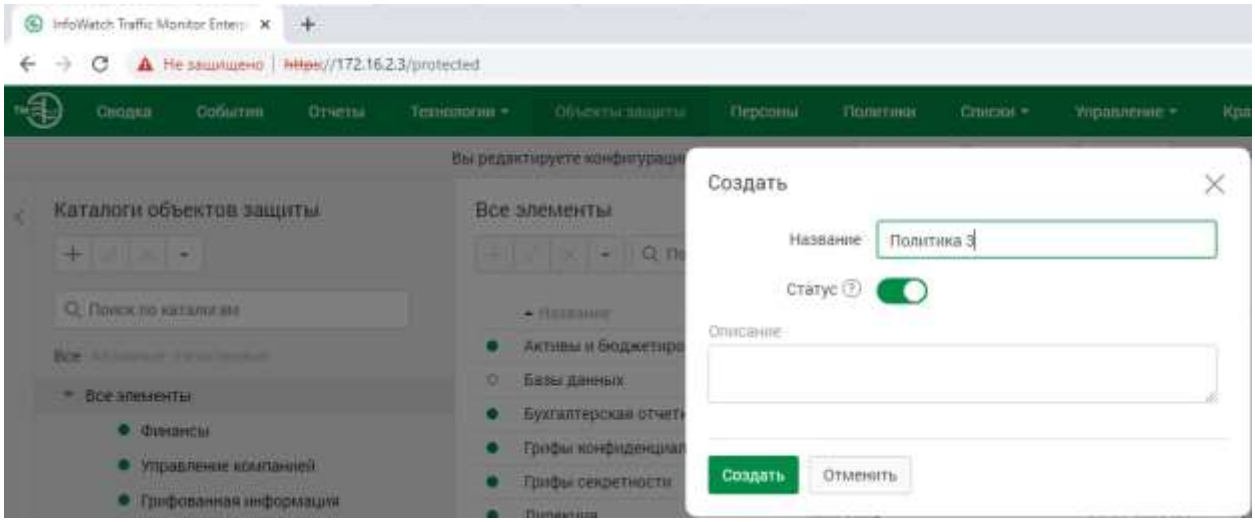
На основе всех типов данных



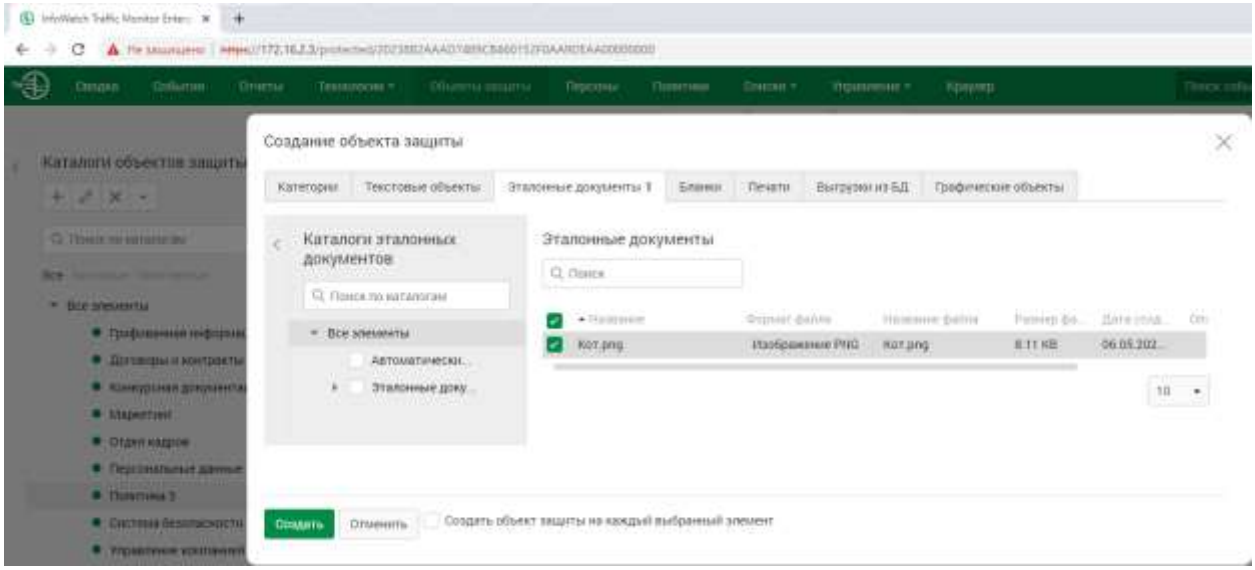
Добавляем картинку котика



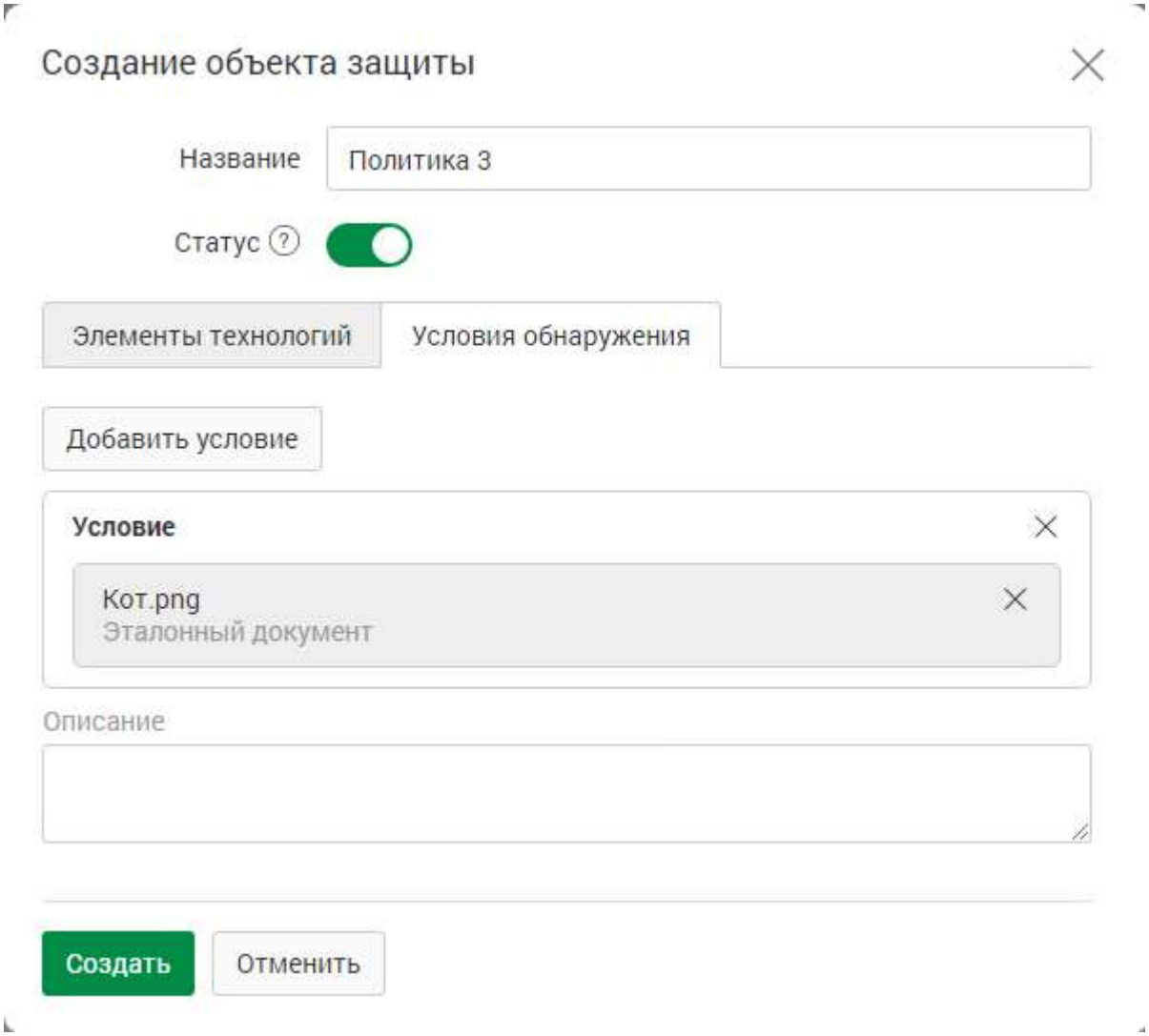
Добавляем объекты защиты



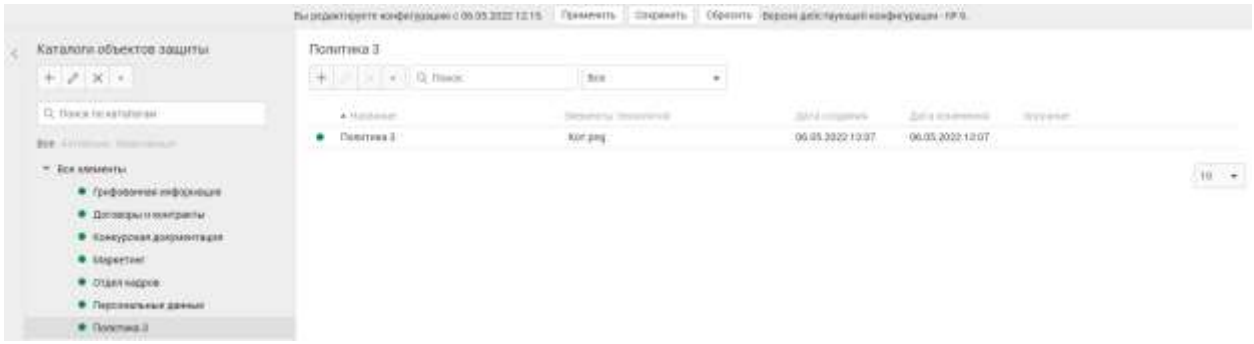
После создание обьекта защиты под названием – Политика 3, переходим в неё и создаем так объект (“+”)



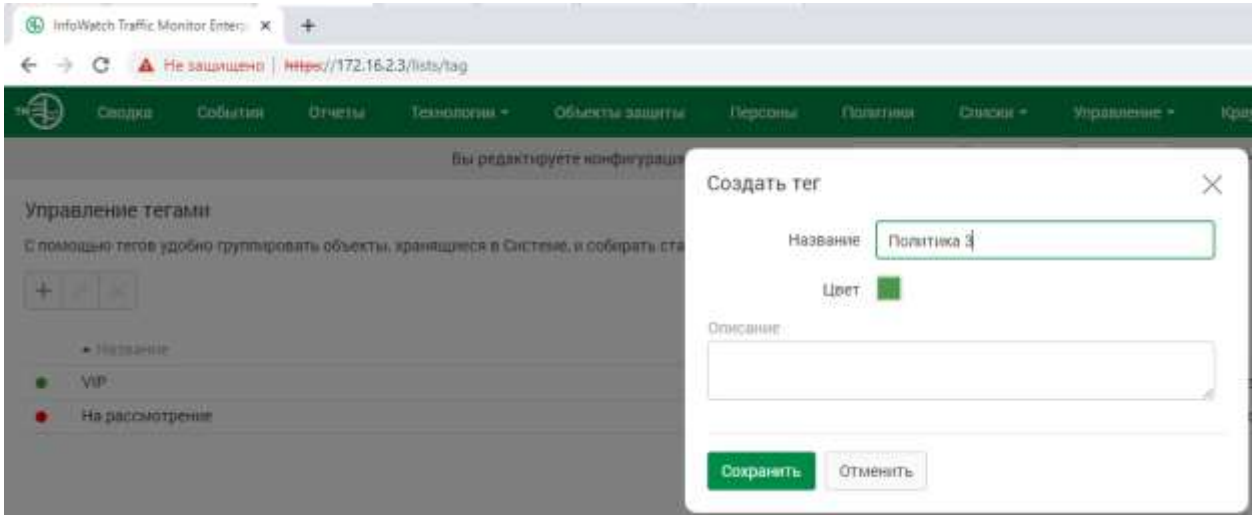
Условием – выбираем кортику Кота



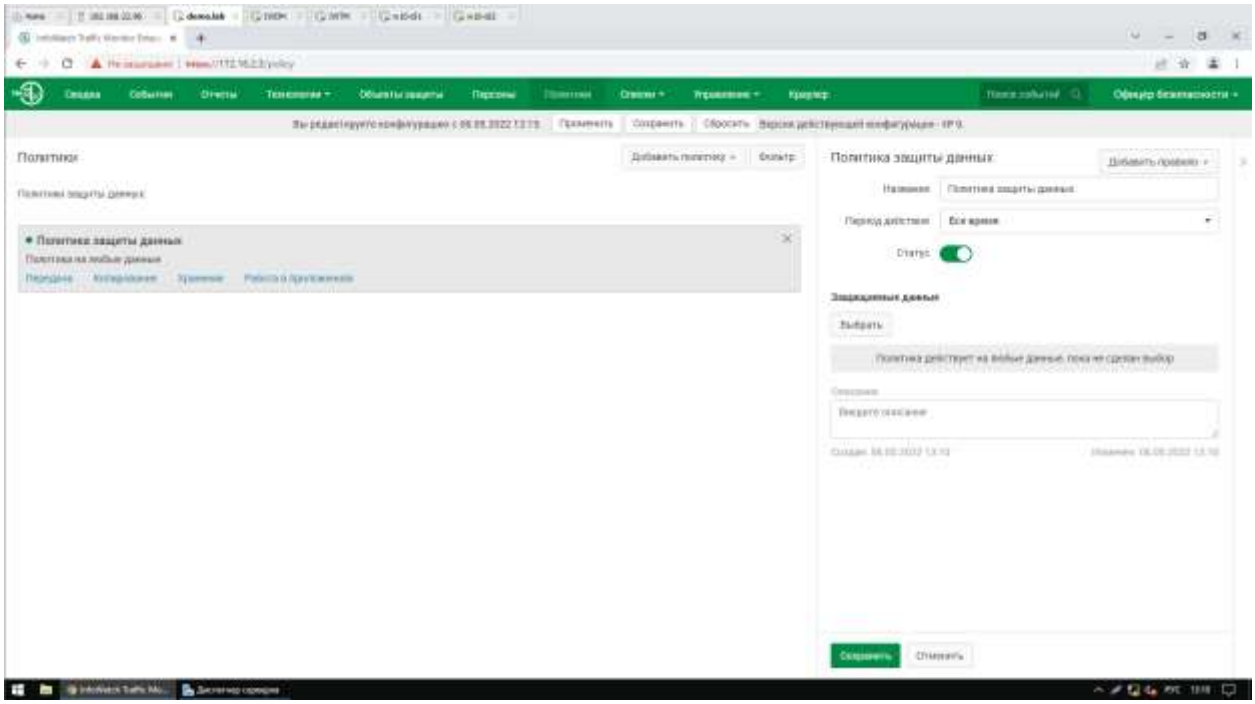
Вот так



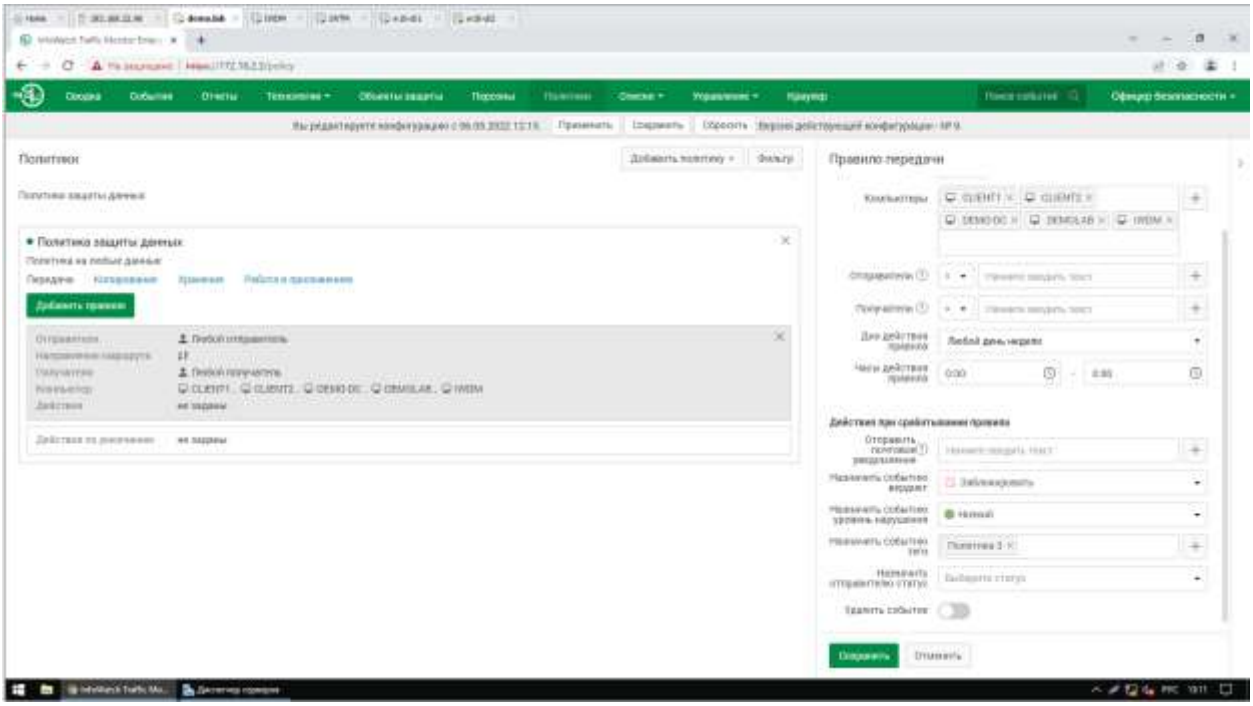
Списки – Теги, создаем новый тег



Переходим в политики, создаем политику защиты данных

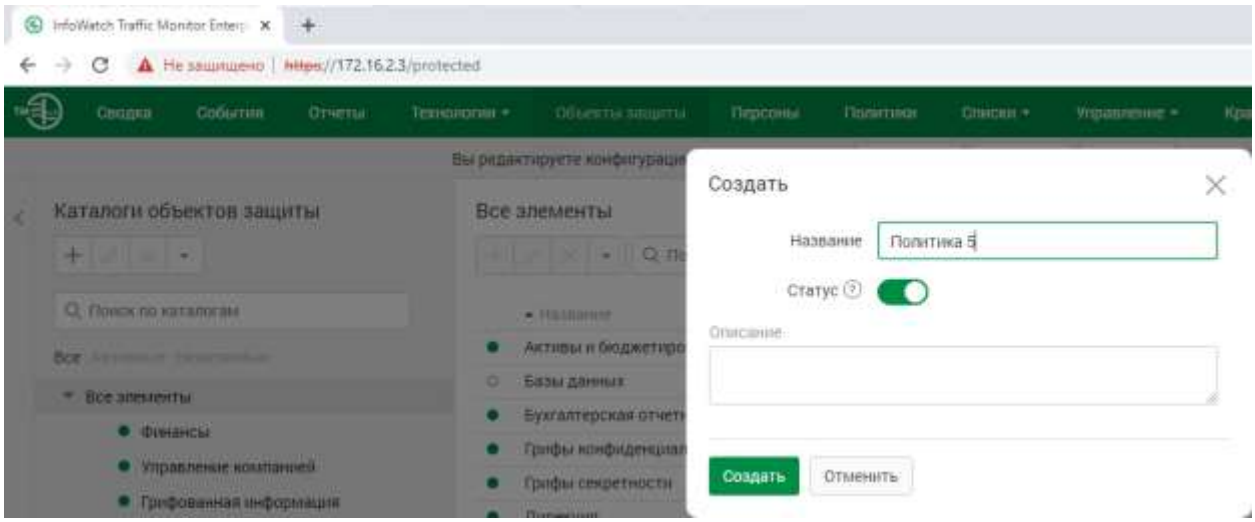


Добавляем правило передачи

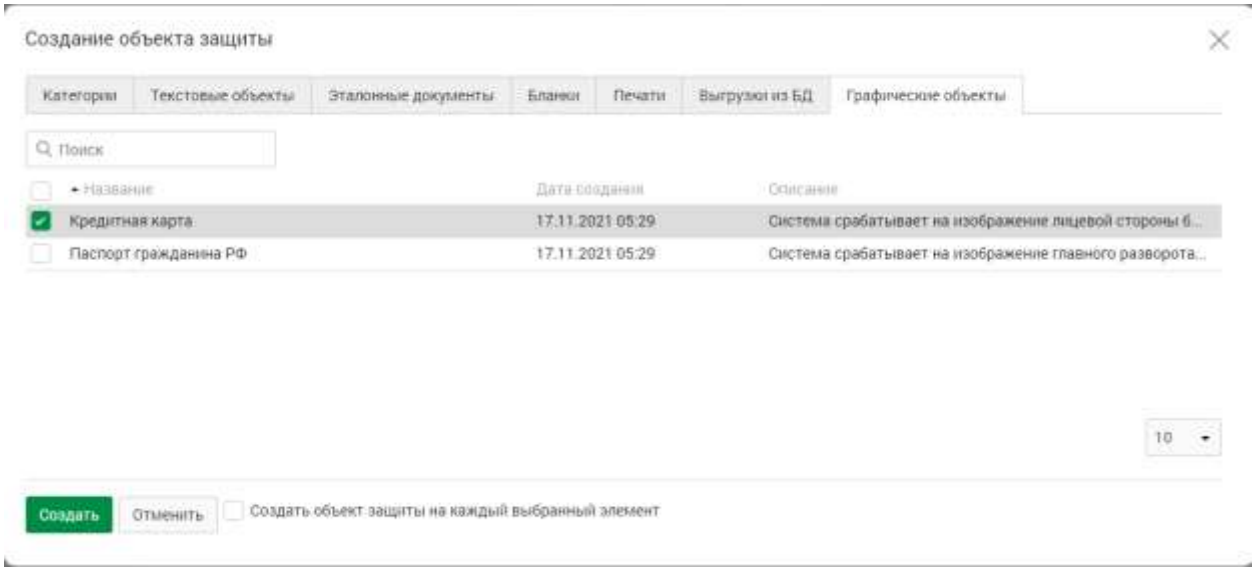


Политика 5

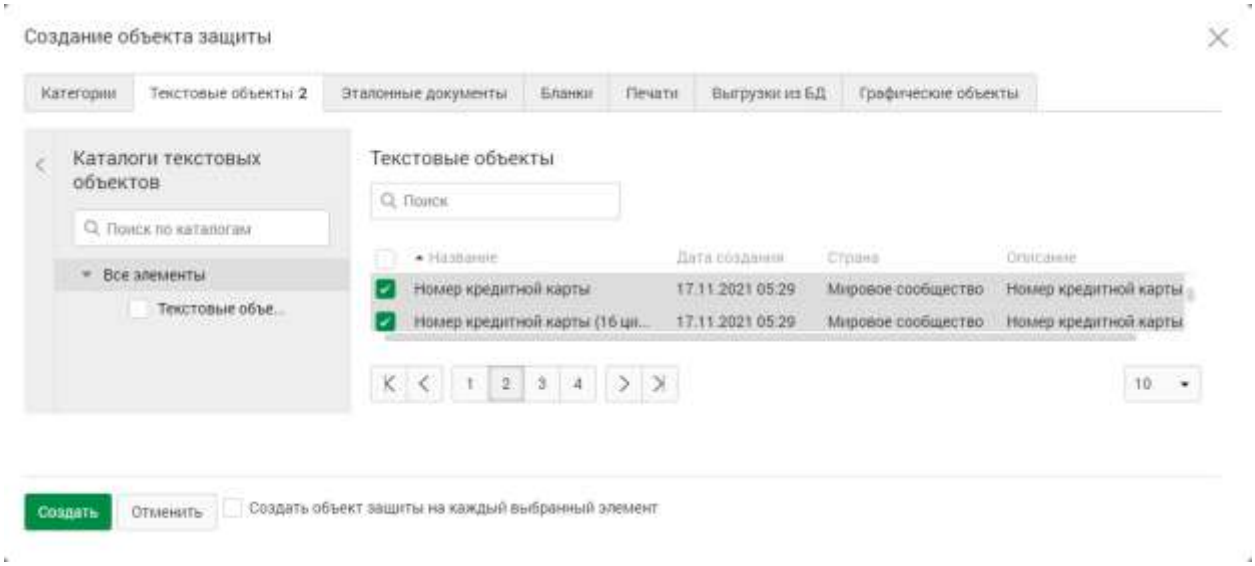
Переходим в объекты защиты и создаем новый объект защиты



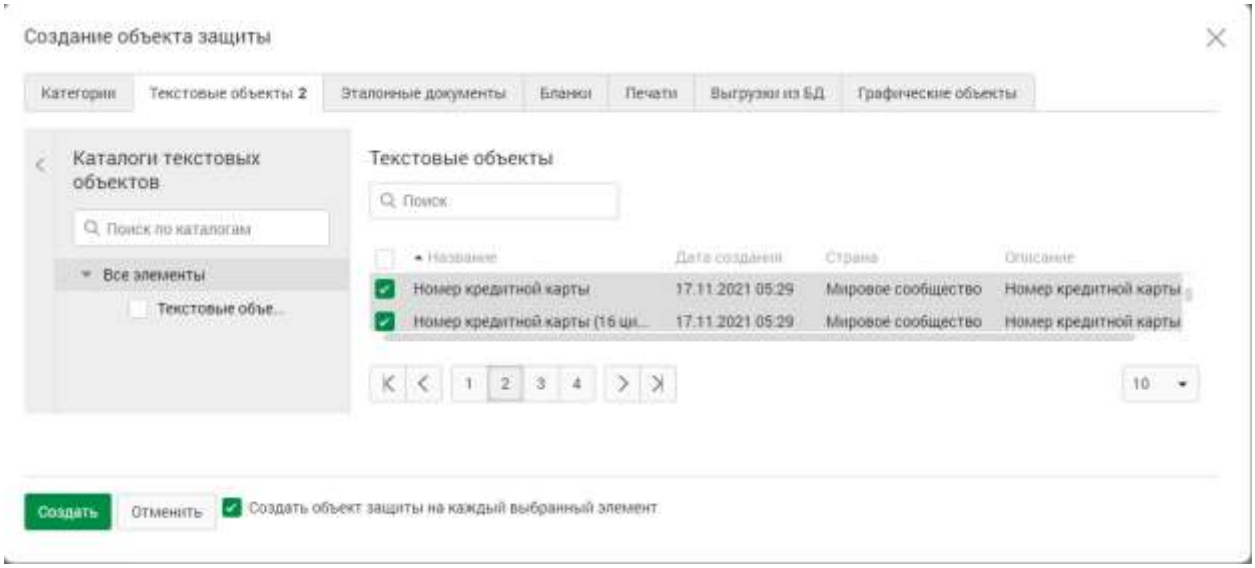
Добавляем



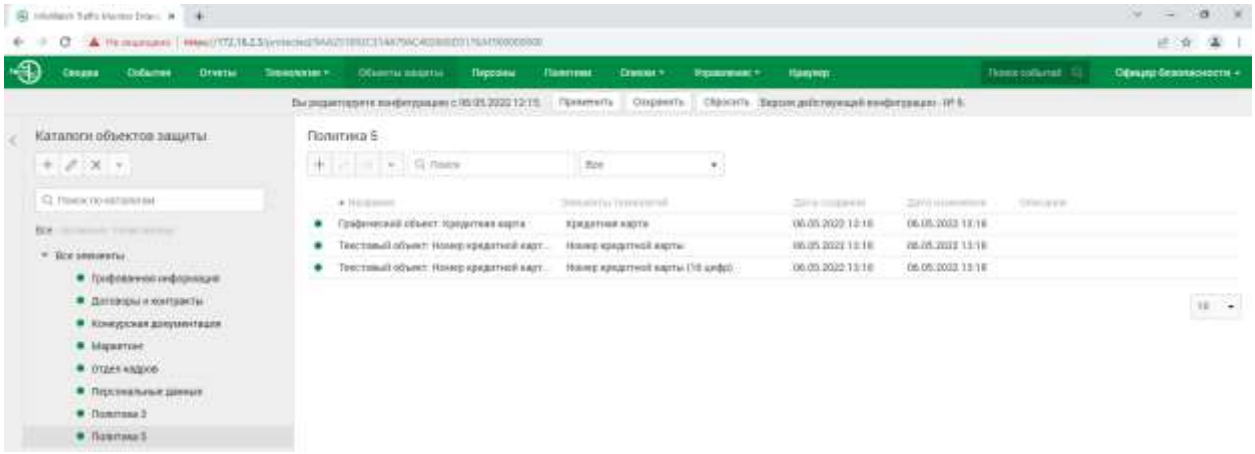
Добавляем



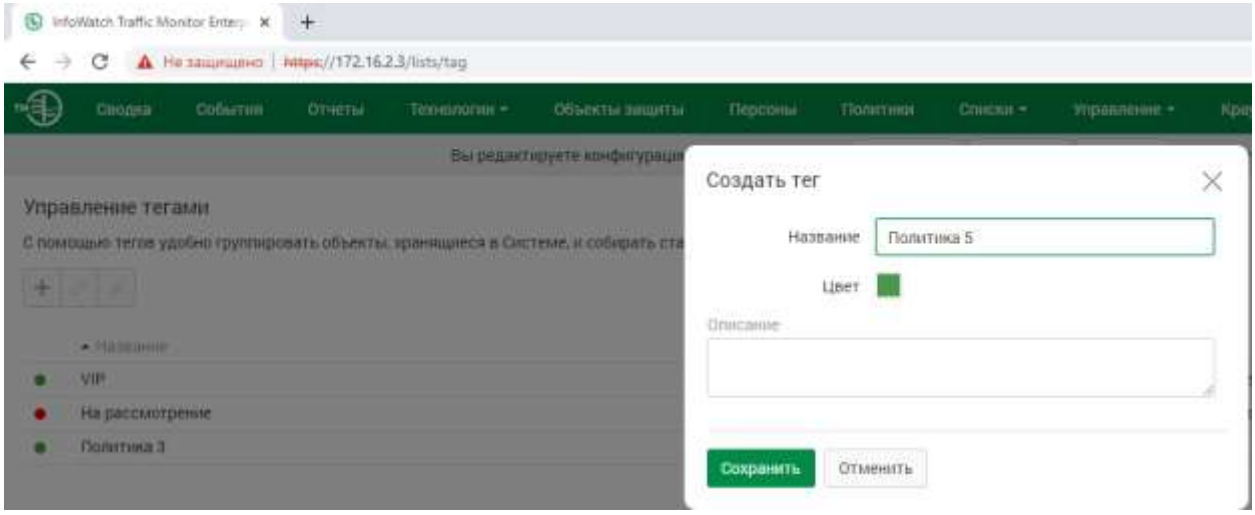
Важно! Ставим снизу галочку



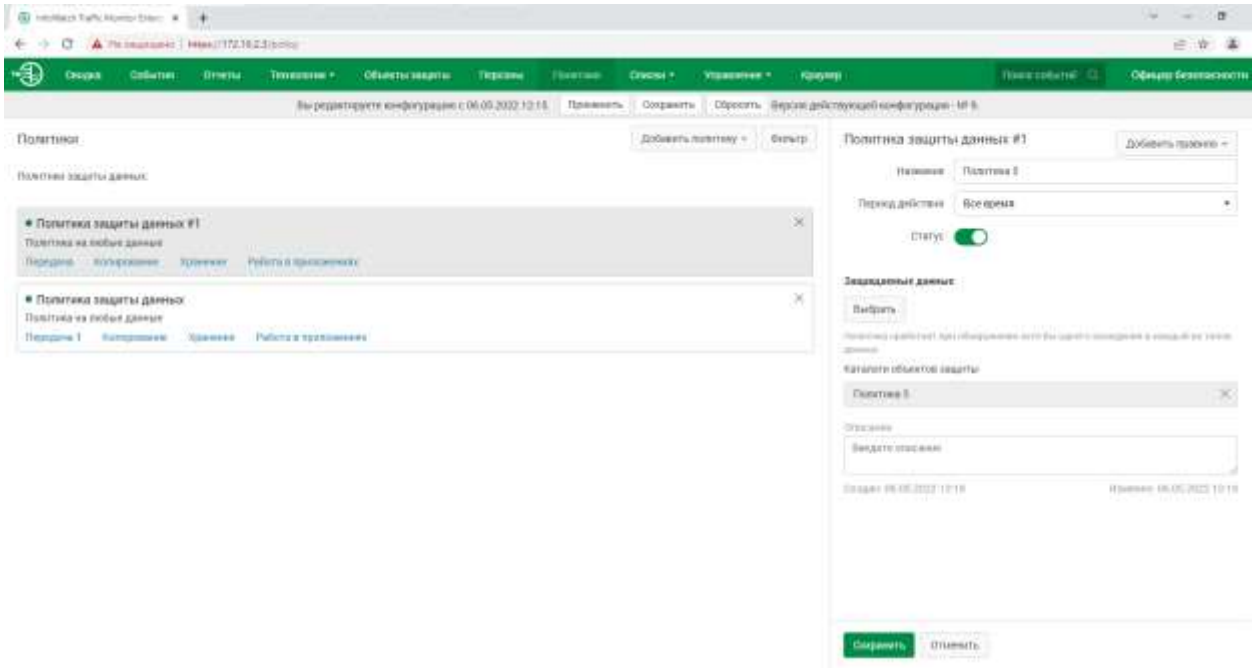
Вот так выглядит



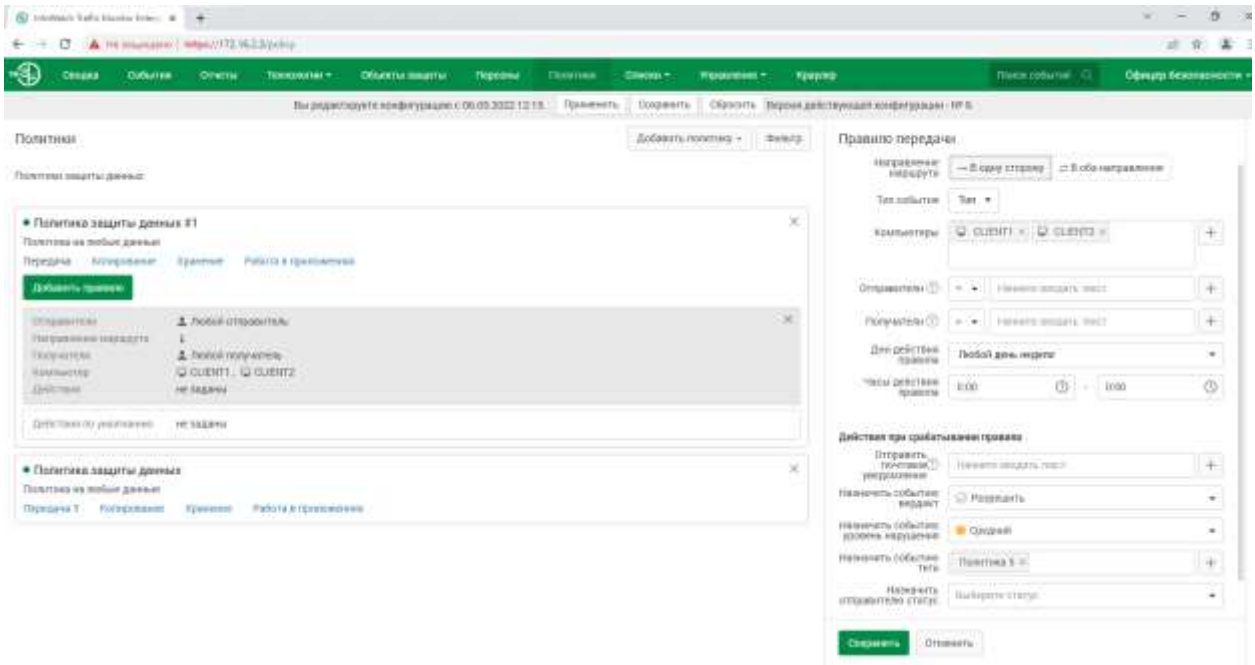
Переходим, списки – теги, создаем новый тег



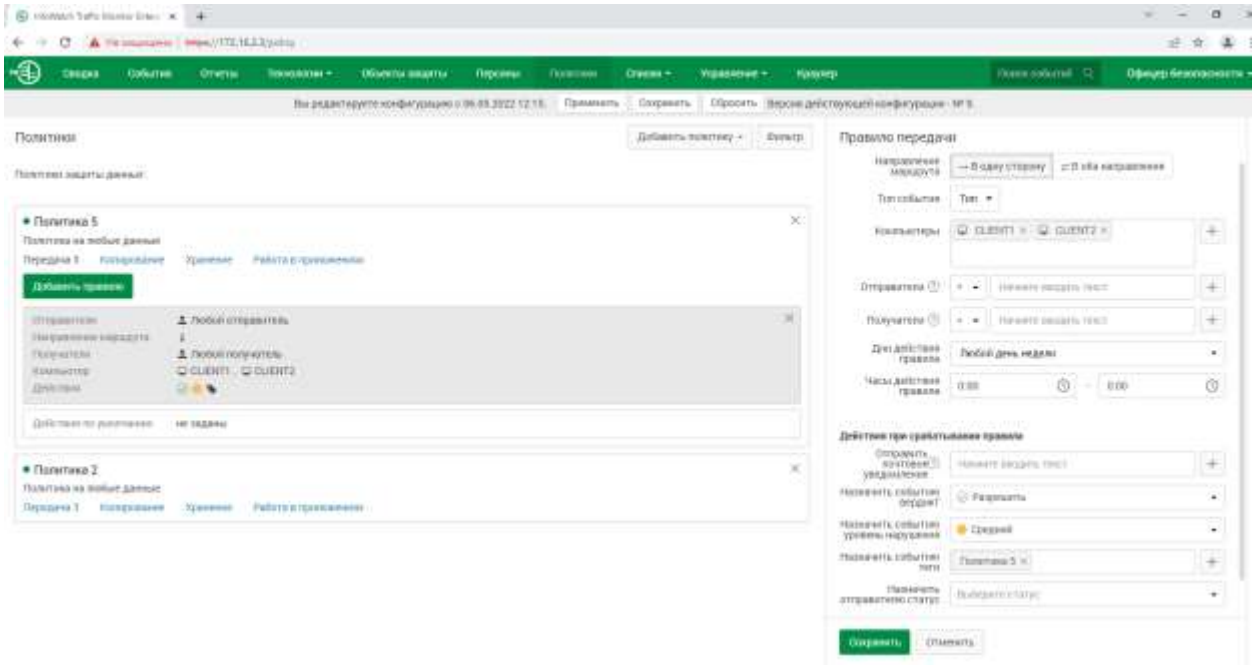
Создаем новую политику защиты данных, защищаемые данные – указывает политика нашу



Правило передачи



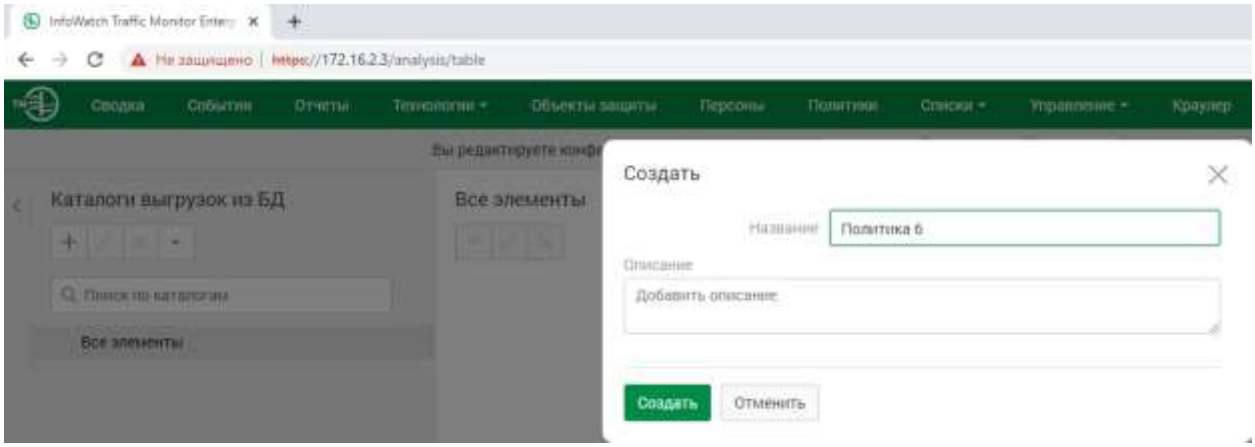
Вот так должно получится



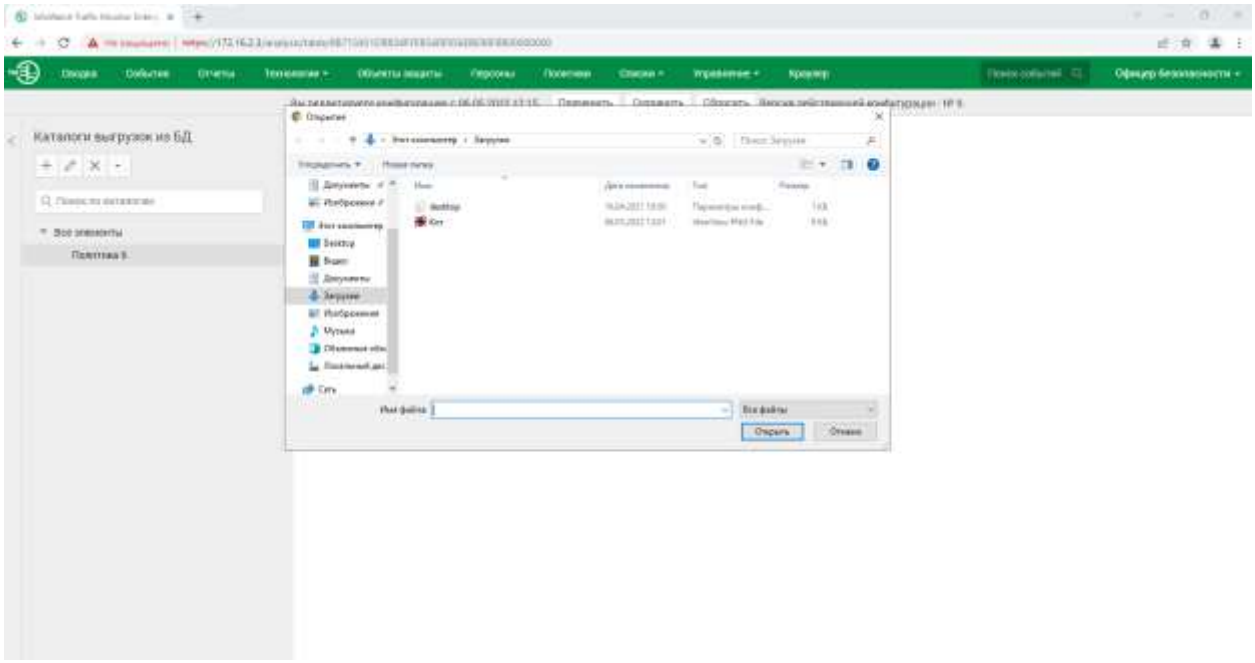
Политика 6

Переходим, технологии – выгрузки из бд

Создаем каталог



Выгрузка из БД



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

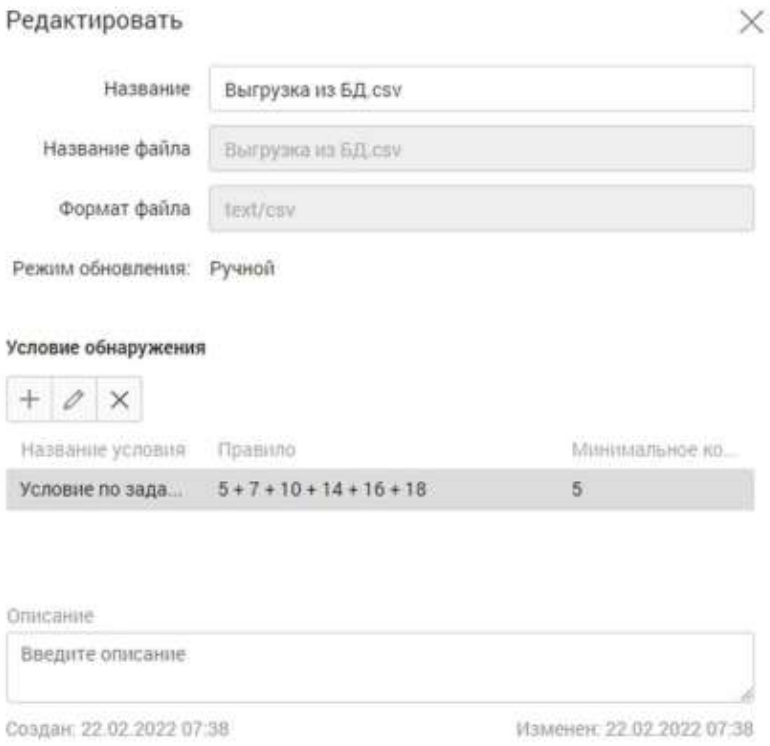


Рисунок 85 – «Условие выгрузки из БД»

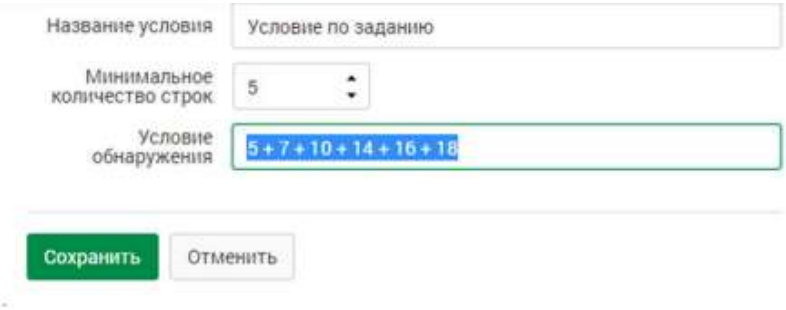


Рисунок 85 – «Условие выгрузки из БД»

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

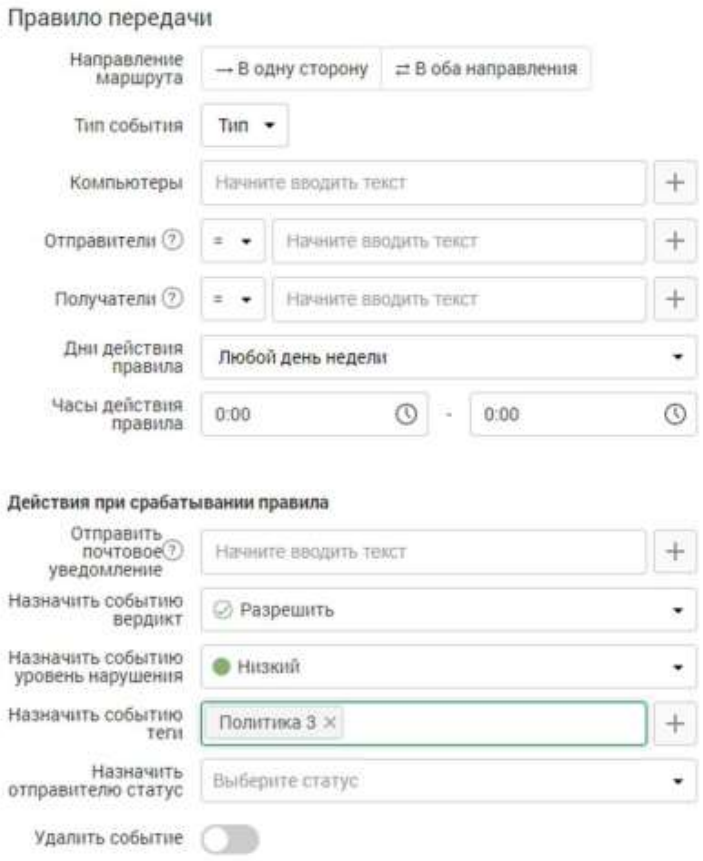
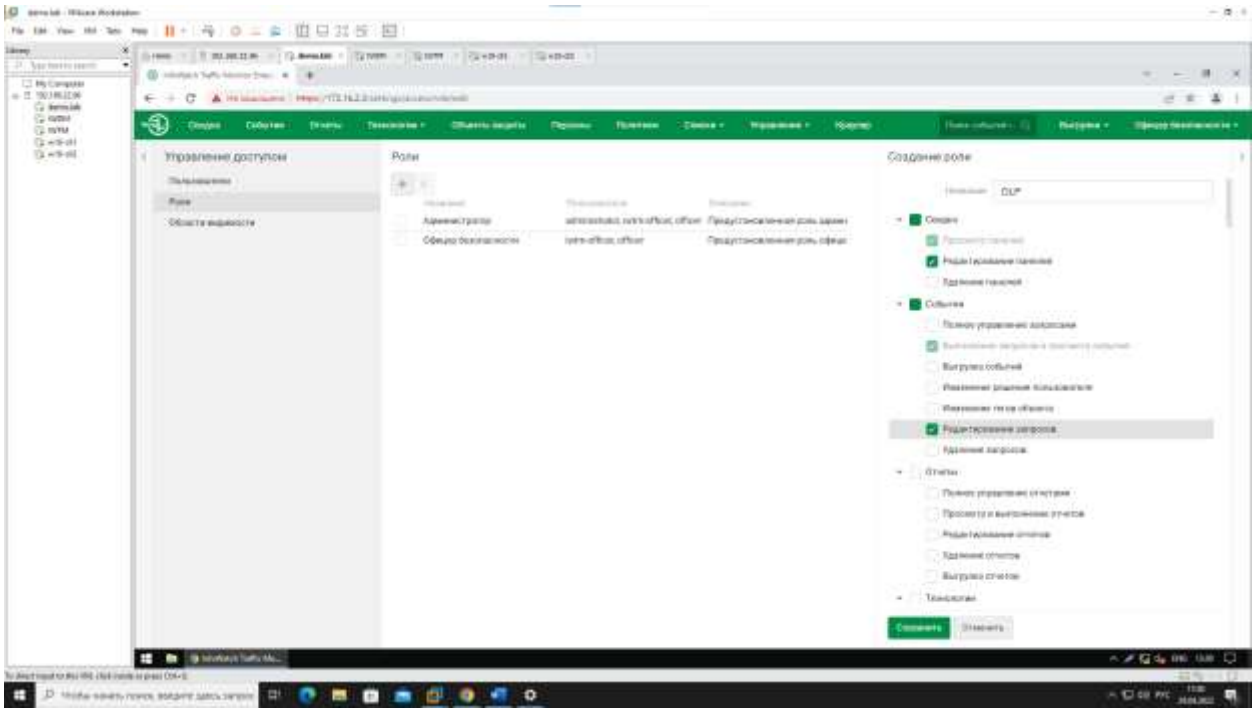
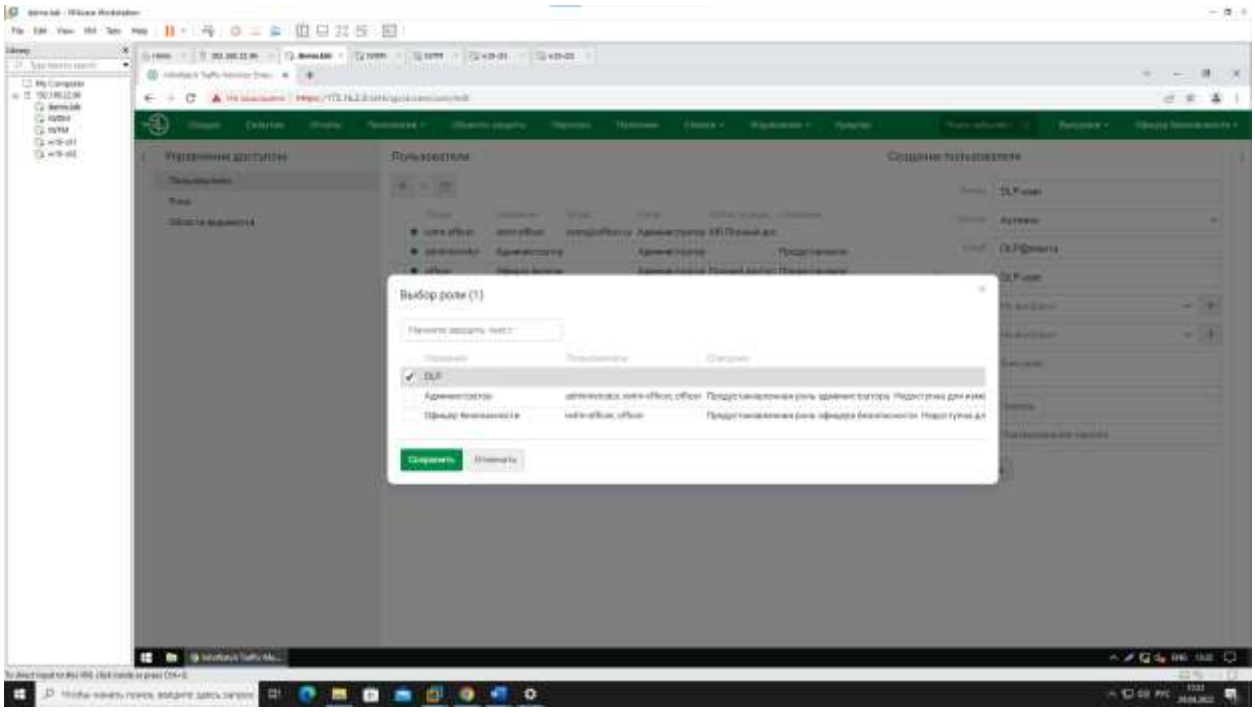


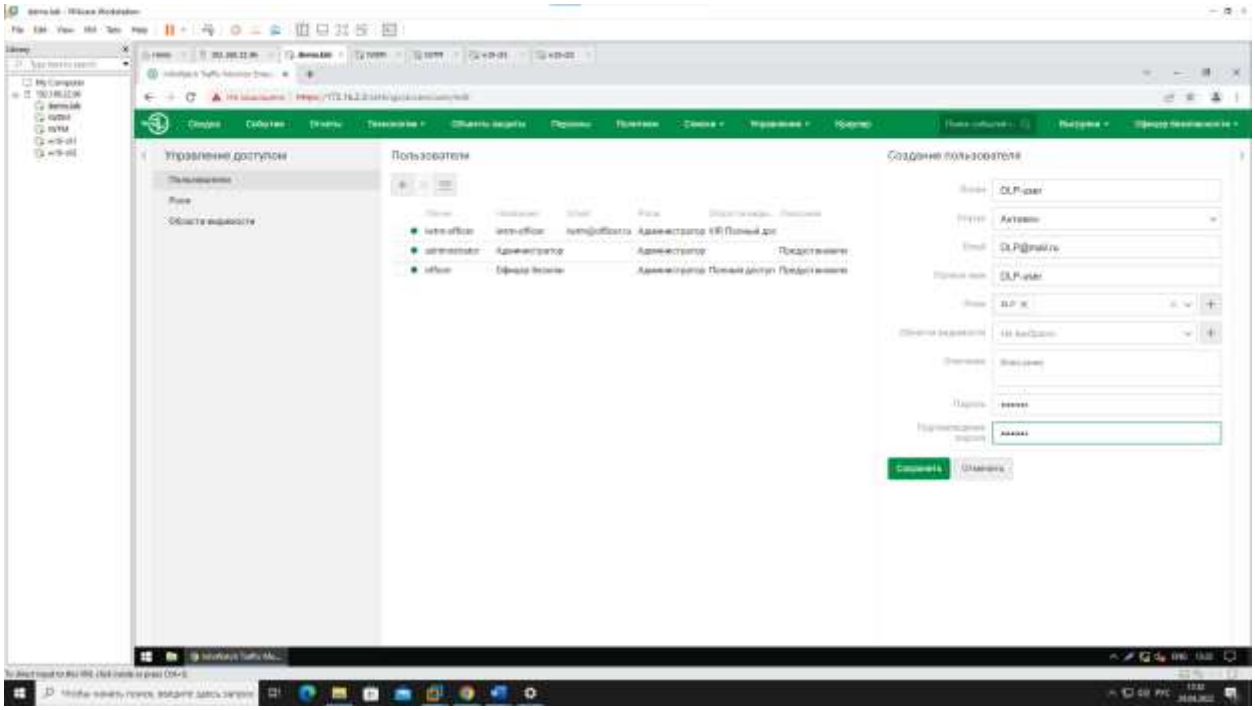
Рисунок 86 – «Правило передачи политики 3»

Модуль 4

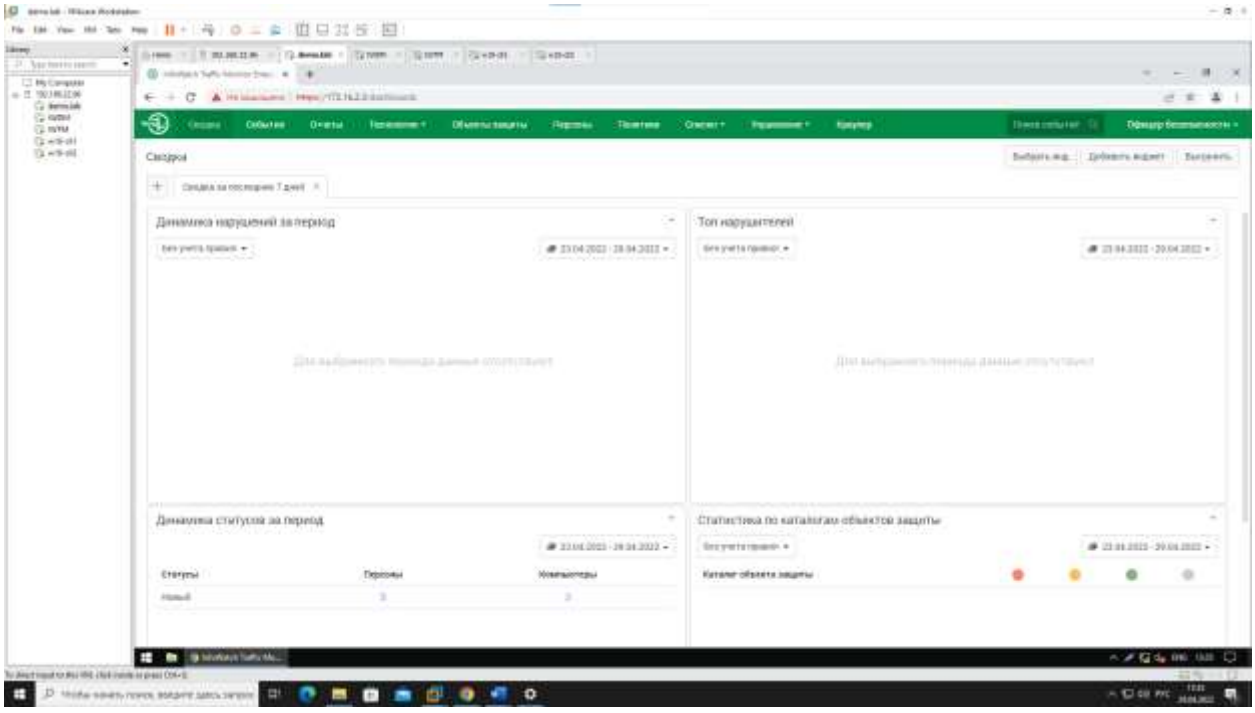
Создание пользователя и роль для него

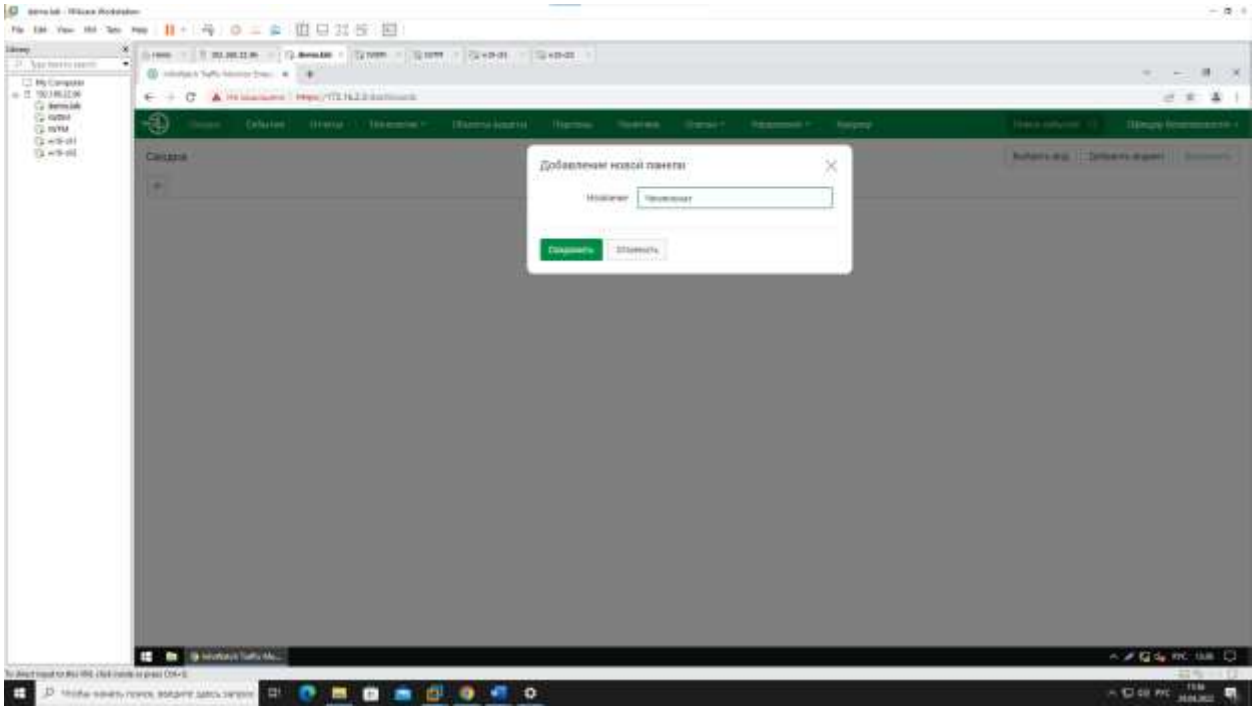


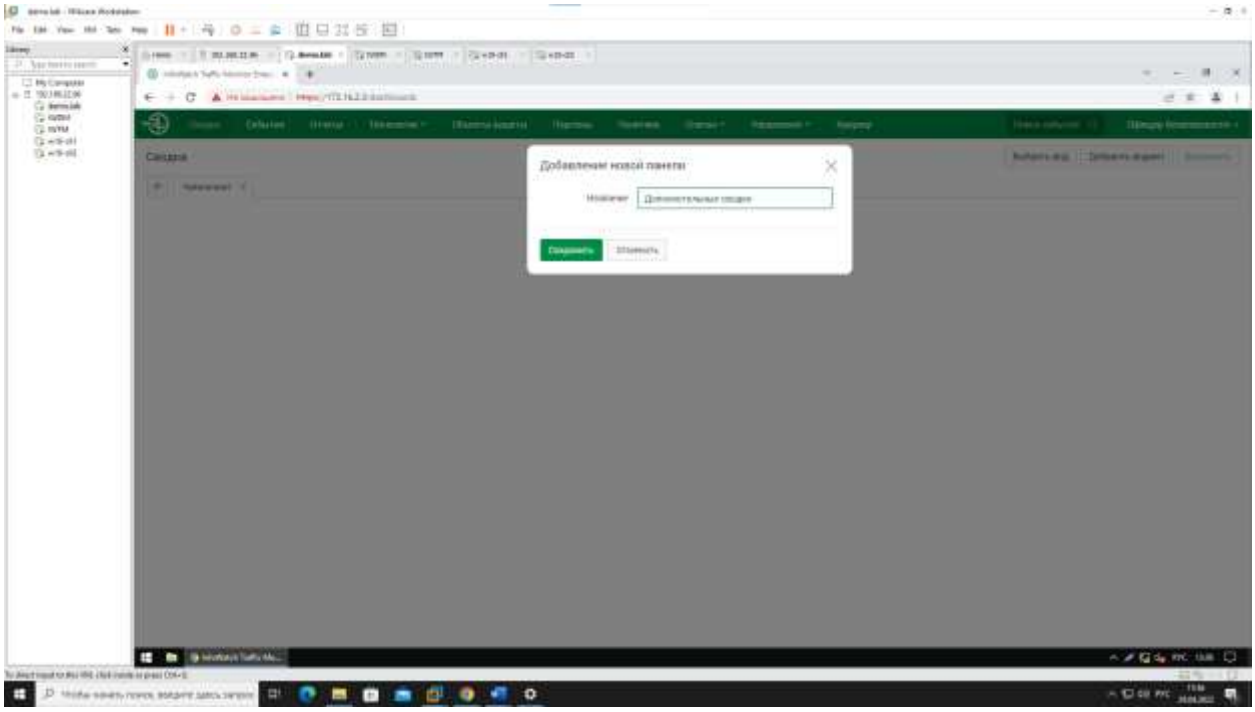




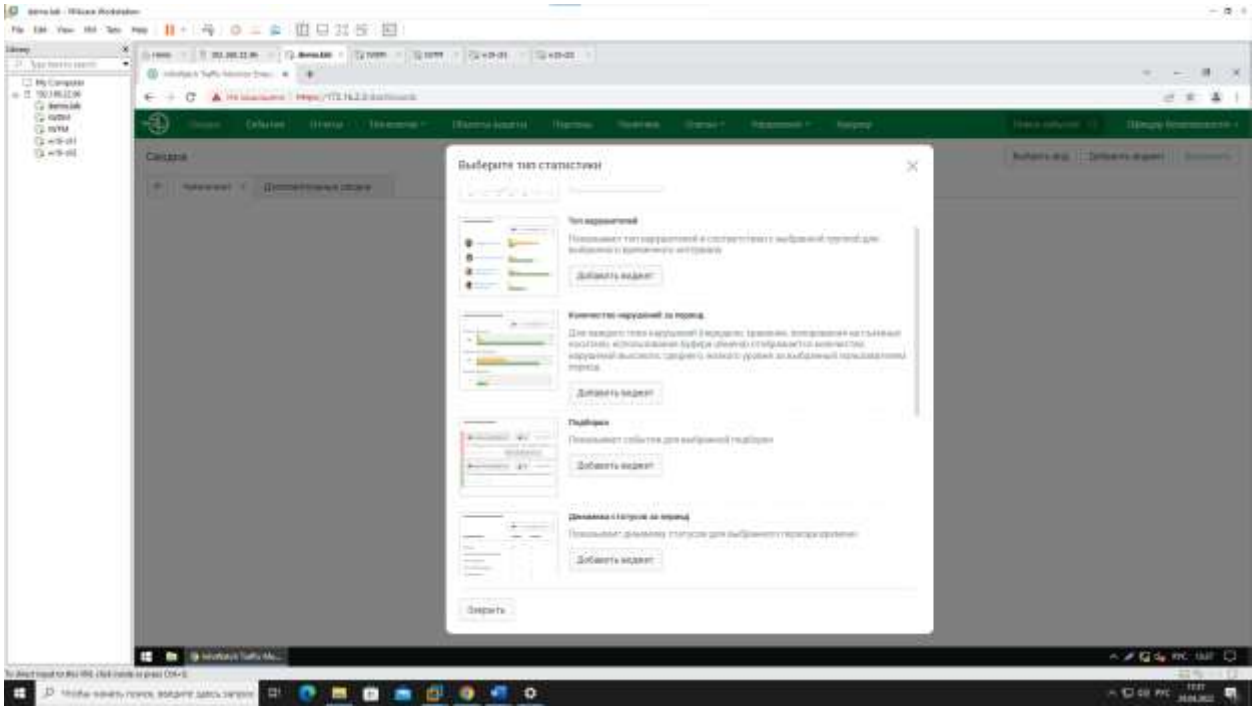
Удаляем все сводки

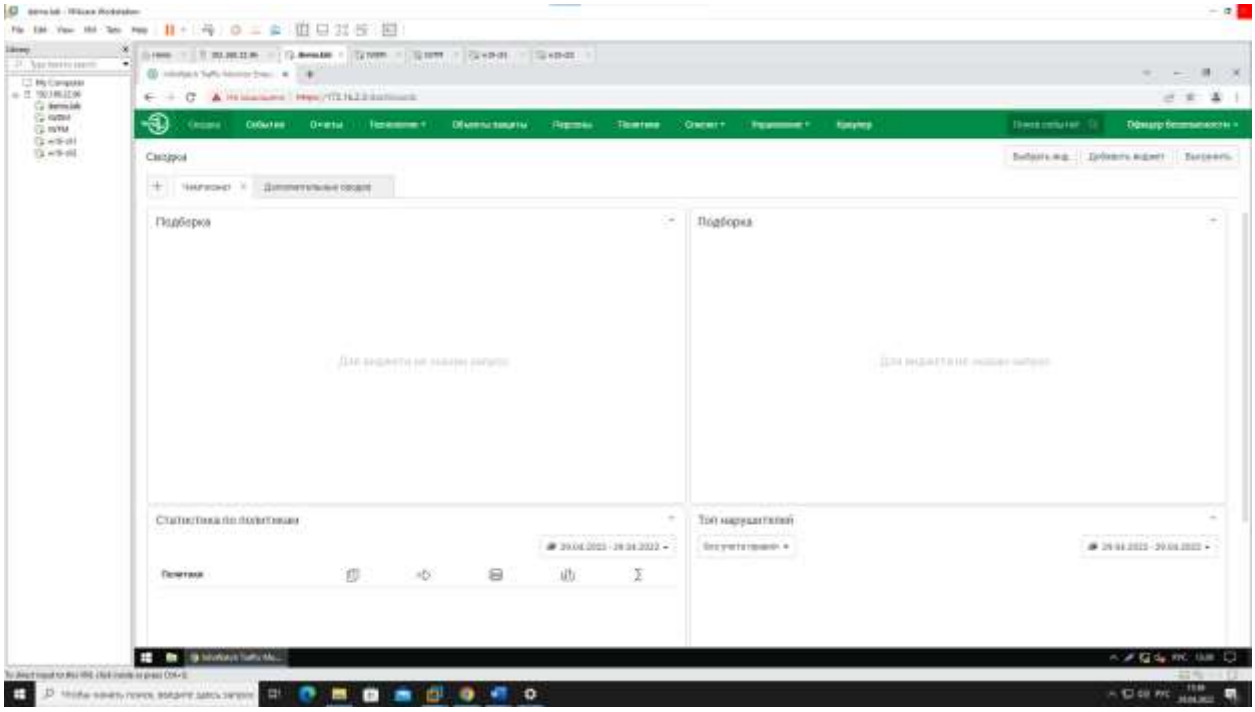


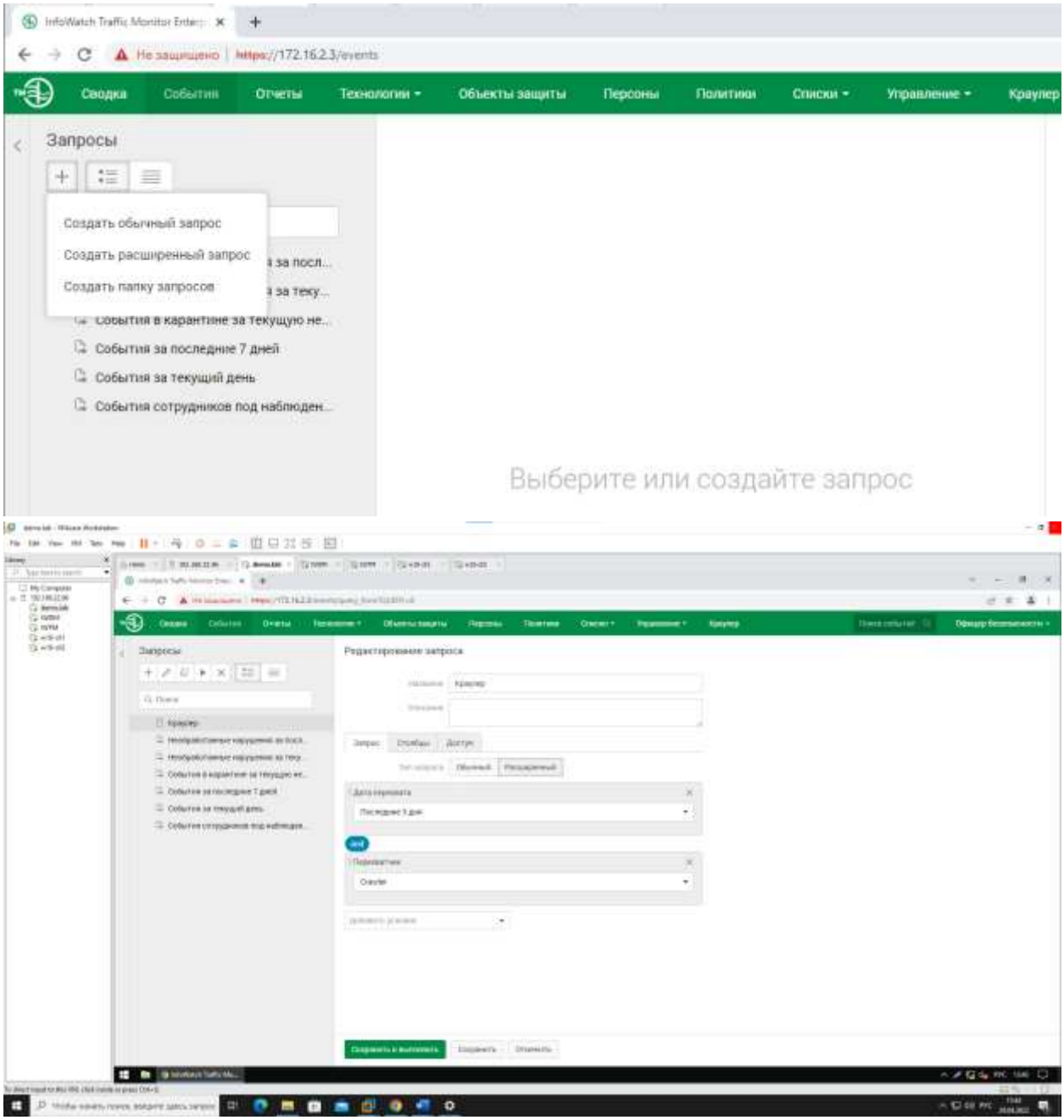




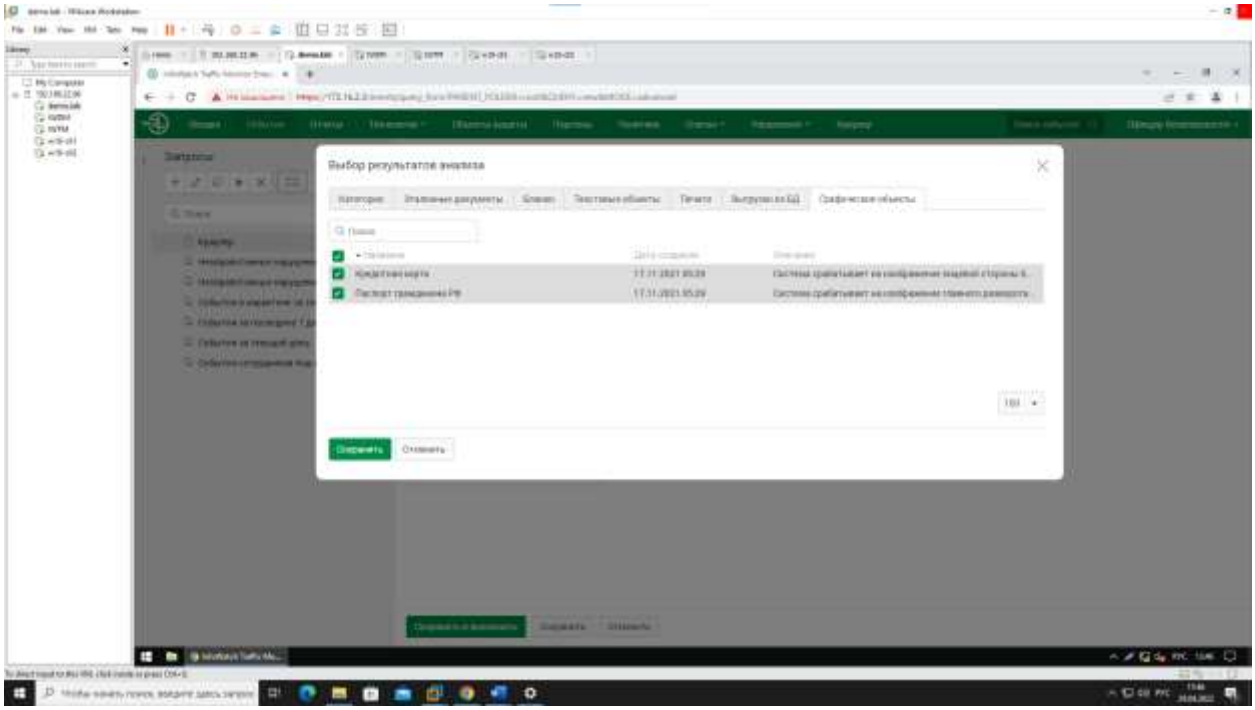
Добавляем подборку

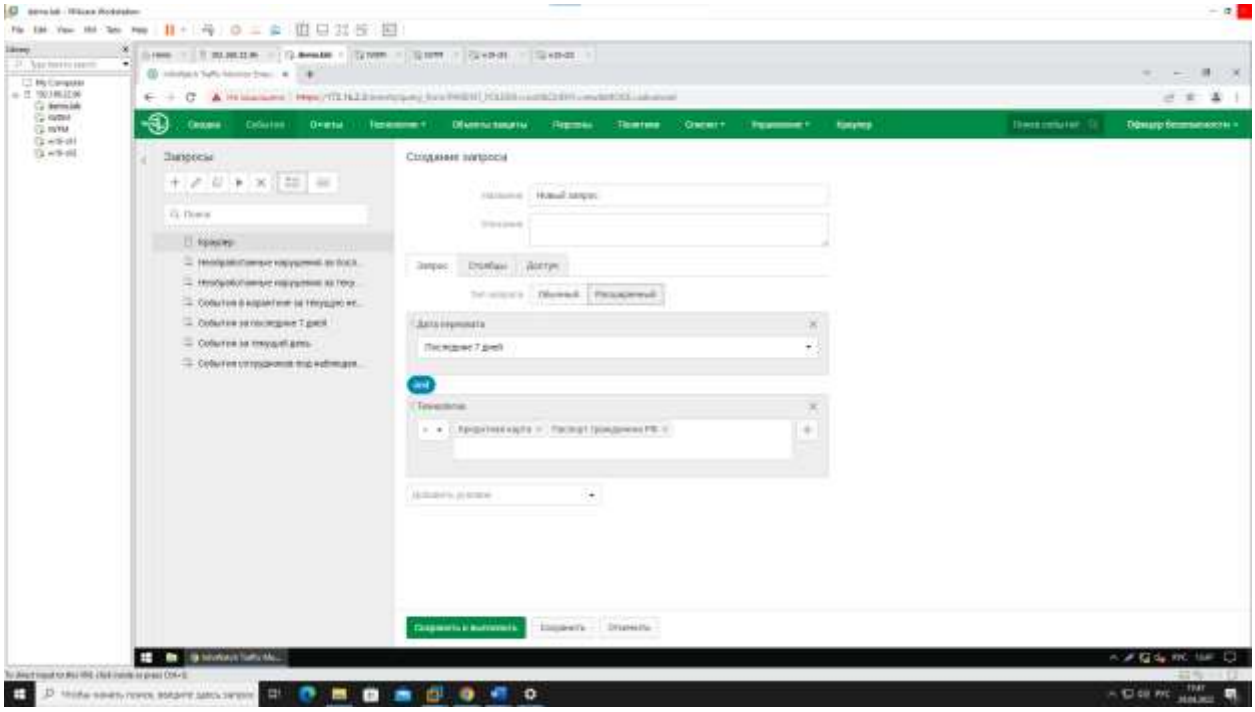

Выберите тип статистики
Сводка
Открыть


Сводка
Подборка
Подборка
Статистика по политикам
Тип нарушителей



Добавляем условие – технологии


Выбор результатов анализа
Сохранить
Отменить


Запросы
Создание запроса
Сохранить и выполнить
Сохранить
Отменить

Сводка

+ | Чемпионат × | Дополнительные сводки

Общие настройки виджета

Название: Краулер

Интервал обновления: Не обновлять

Подборка: Краулер ×

Событий на странице:

Сохранить | Отменить

Общие настройки виджета

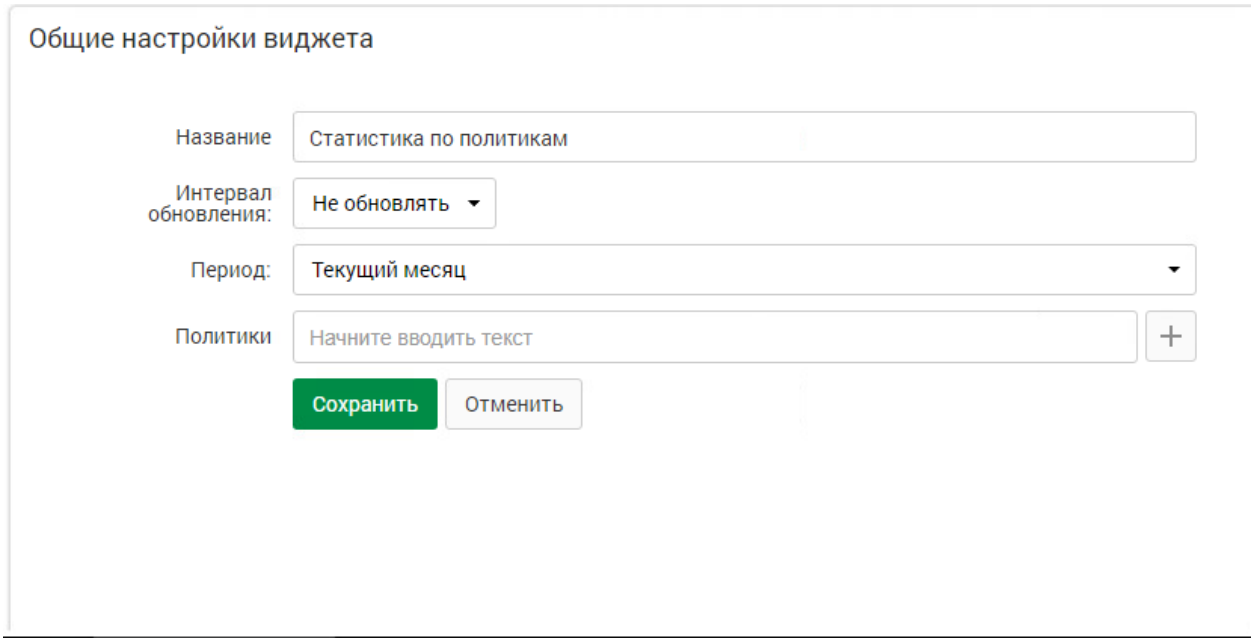
Название: Технологии

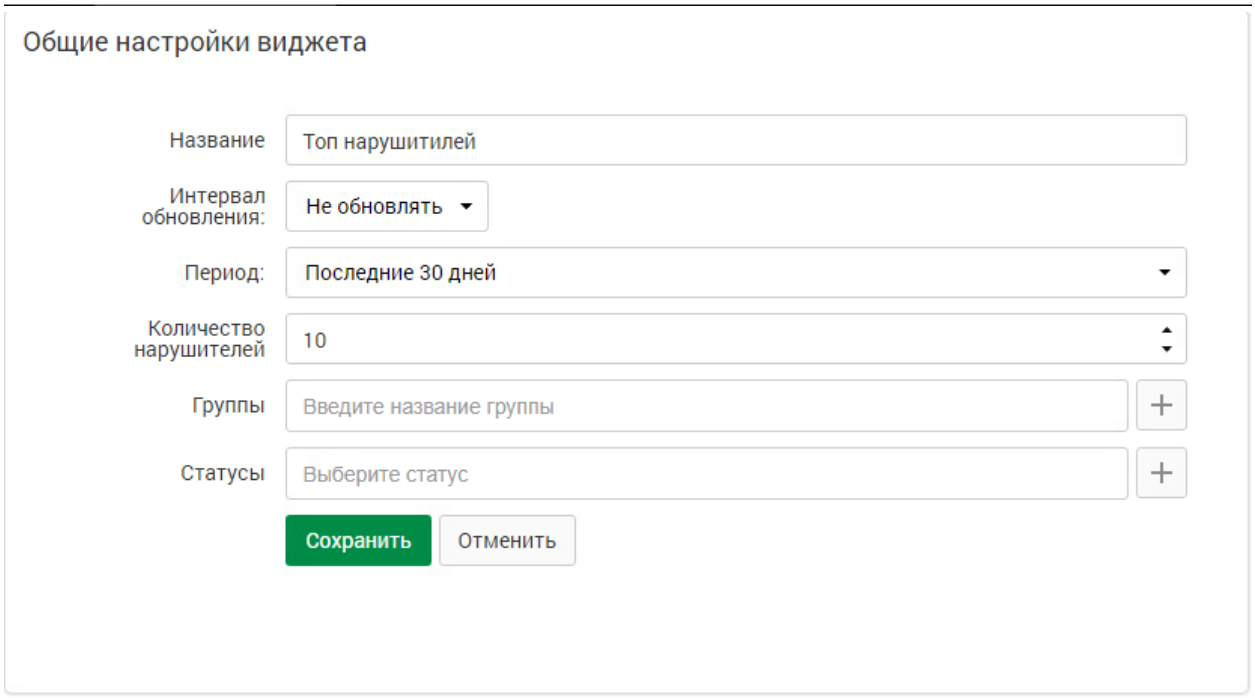
Интервал обновления: Не обновлять

Подборка: Новый запрос ×

Событий на странице:

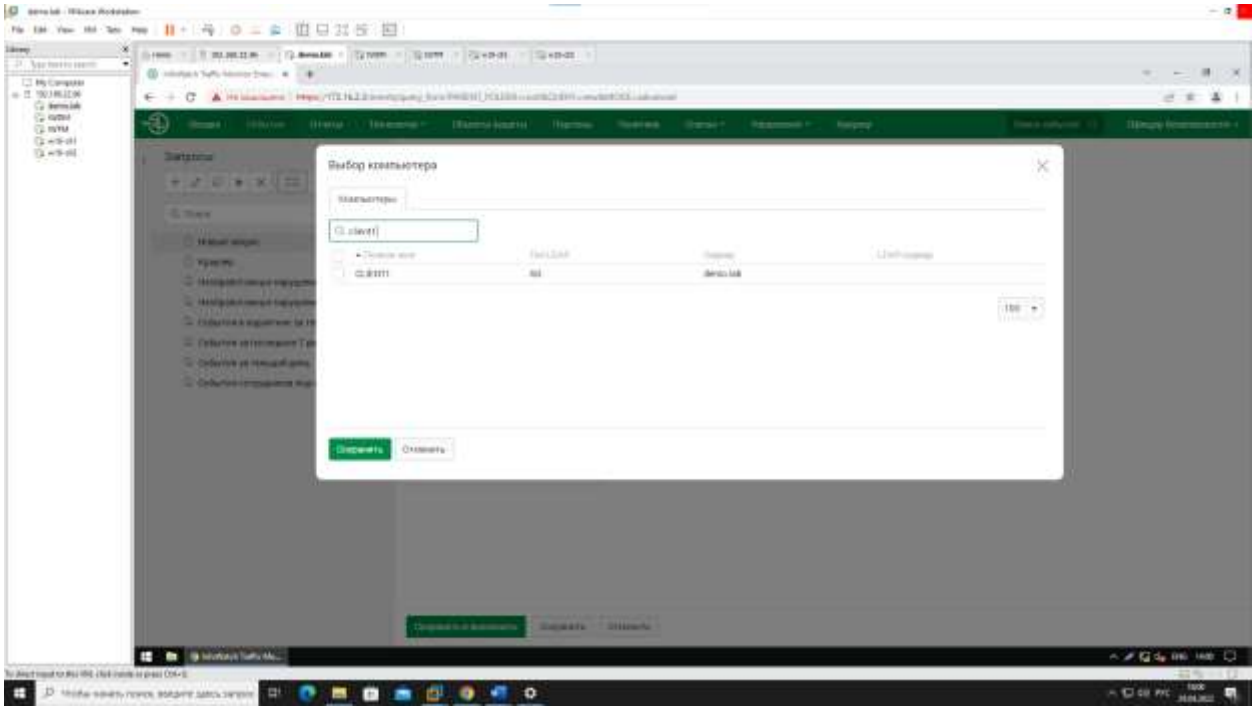
Сохранить | Отменить



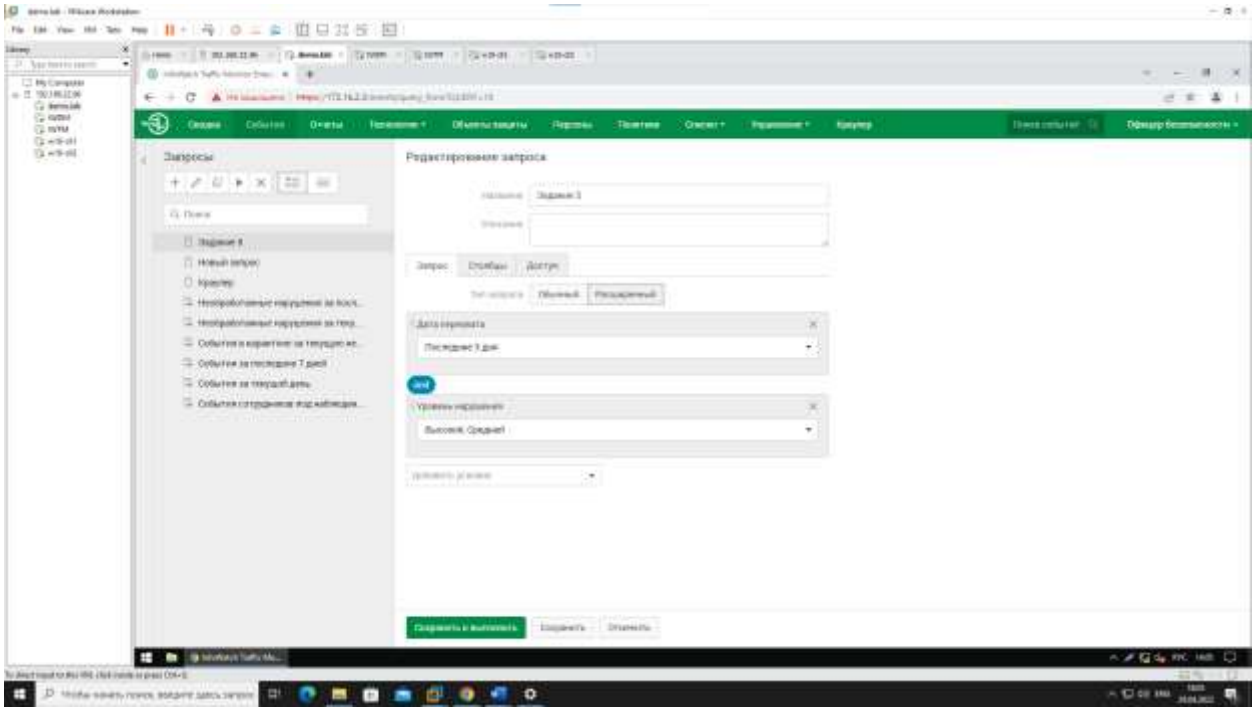


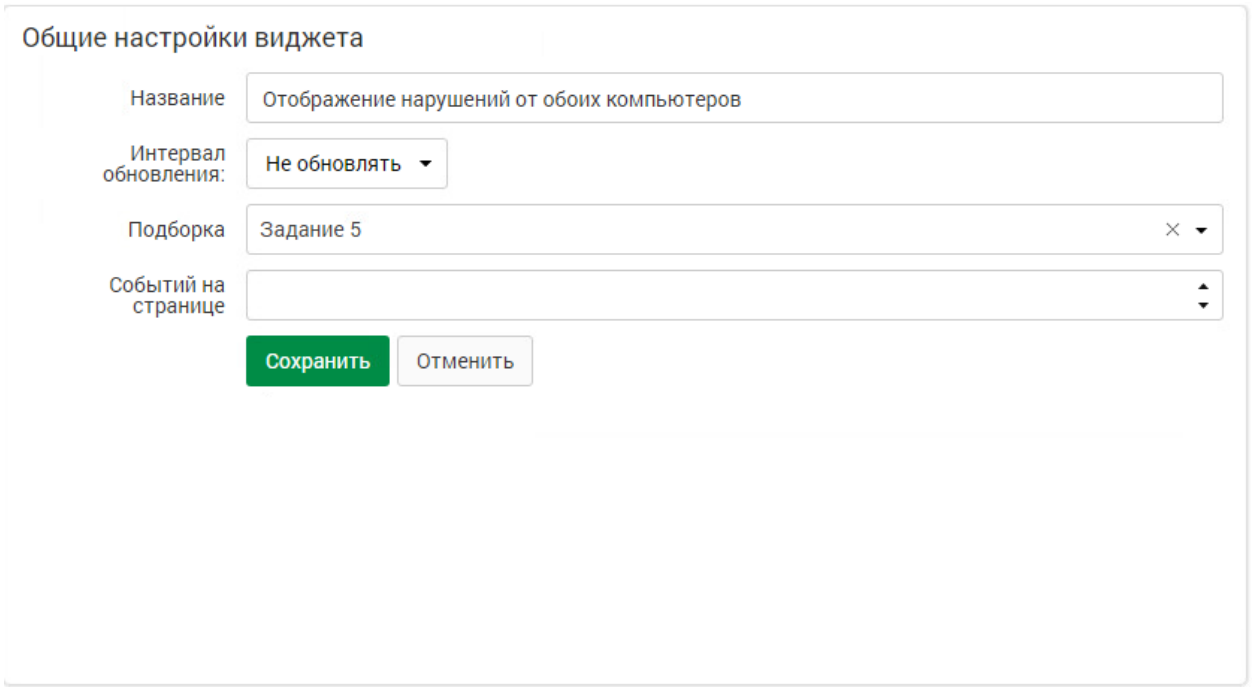
Задание 5

Добавляем компьютеры нарушителей – client1 и client2



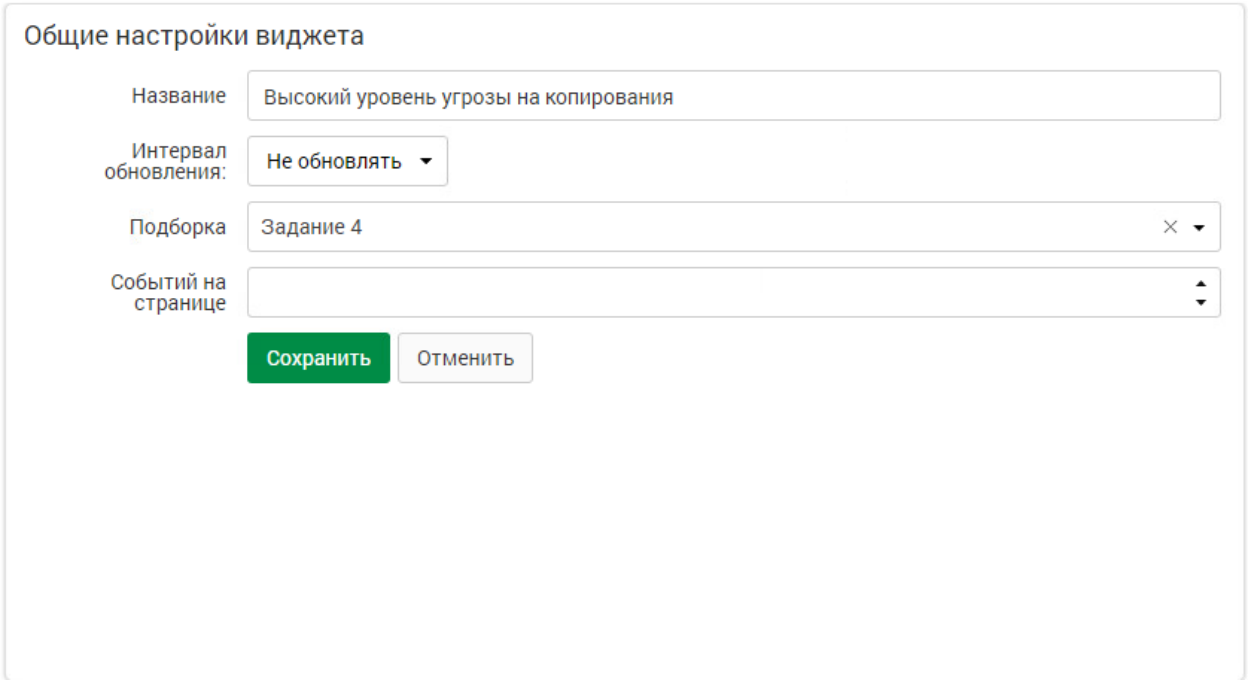
Добавляем уровень нарушения – высокий и средний

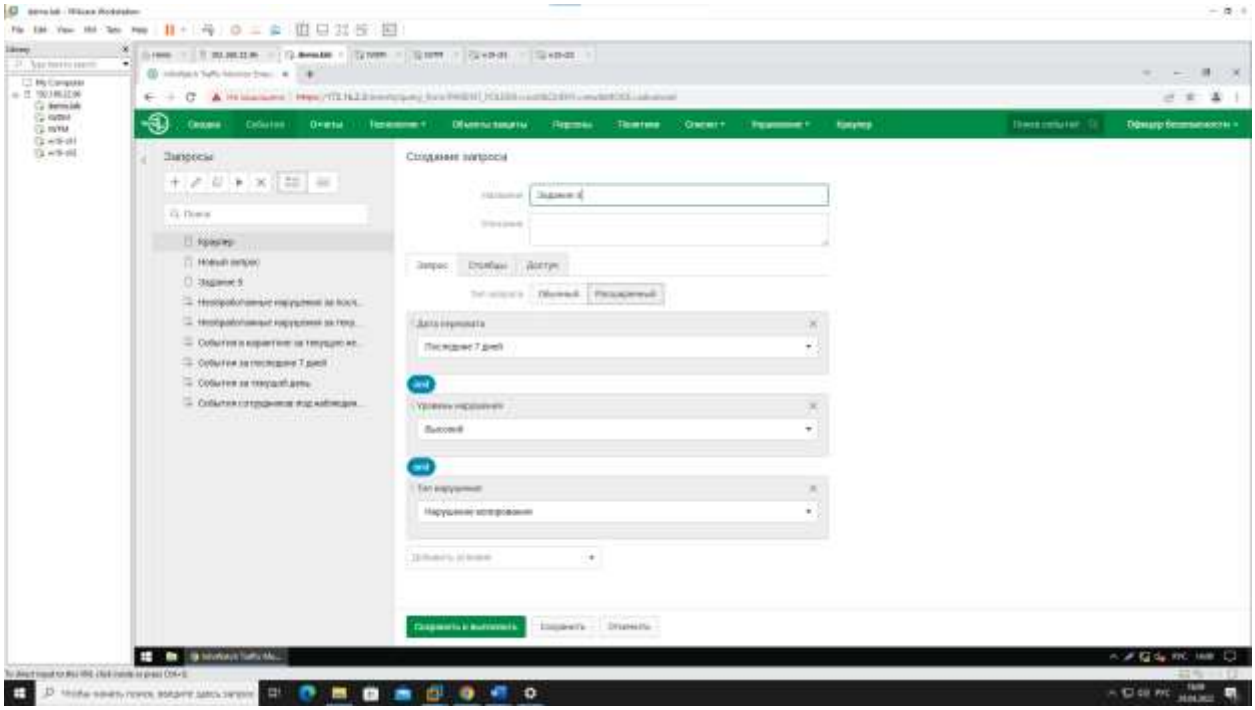


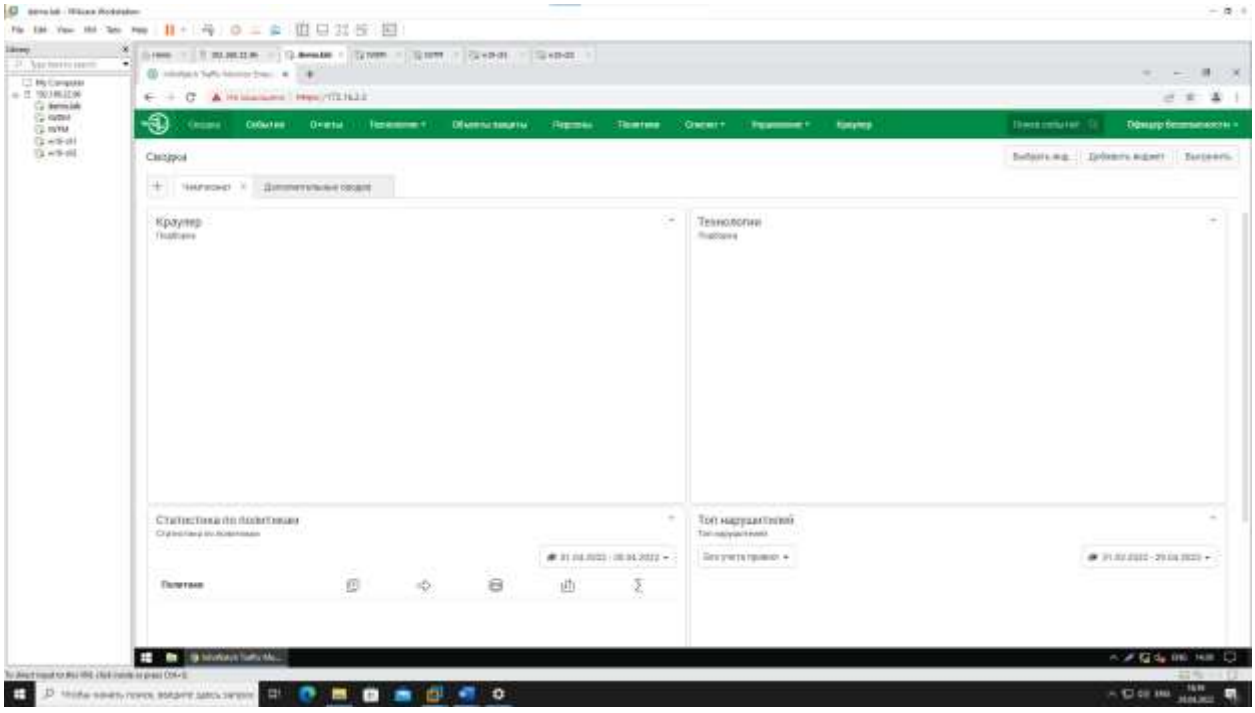


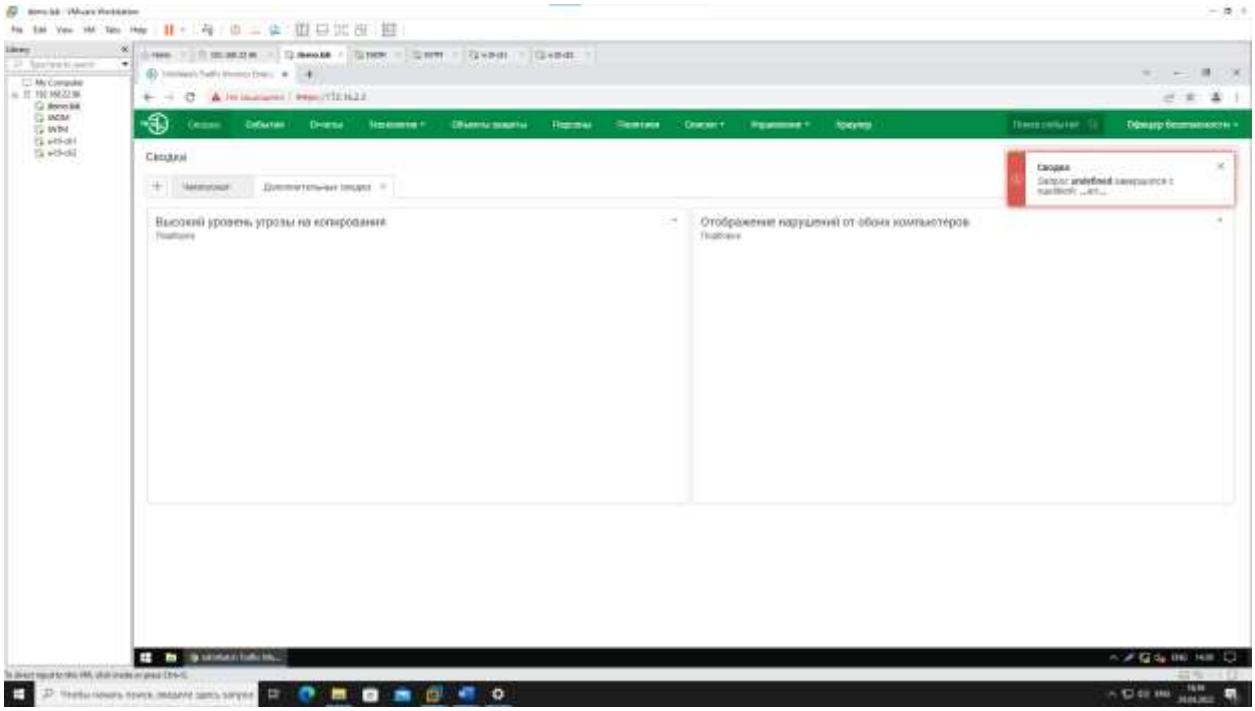
Задание 4

Дополнительные сводки








Сводки
Высокий уровень угрозы на копирование
Отображение нарушений от обоих компьютеров