

## ДЕМОЭКЗАМЕН

[Блог на WordPress.com.](#)

# Описание модуля А: Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз

Задание 1: Настройка контроллера домена

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

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

Логин: iwtm-root, пароль: xxXX5566, права пользователя домена

Логин: ldap-synch, пароль: xxXX5566, права пользователя домена

Логин: iwdm-adm, пароль: xxXX5566, права администратора домена и локального администратора

Логин: user-wind, пароль xxXX5566, права пользователя домена

Логин: user-grp, пароль xxXX5566, права пользователя домена

## заходим

The screenshot shows the Windows Active Directory Users and Computers management console. On the left, the navigation pane displays the structure of the domain 'demo.lab'. A context menu is open over the 'demo.lab' container, with the 'Create' option selected, which has brought up a 'New Object - Department' dialog box. In this dialog, the name 'delabs' is entered in the 'Name:' field. Below the name field is a checkbox labeled 'Protect container from accidental deletion', which is currently unchecked. At the bottom of the dialog are three buttons: 'OK' (highlighted in blue), 'Cancel', and 'Help'.

Имя	Тип	Описание
Builtin	builtinDomain	
Computers	Контейнер	Default container for u
ForeignSecurityPrincipals	Контейнер	Default container for se
Managed Service Accounts	Контейнер	Default container for m

Правой кнопкой на demo.lab → создать → подразделение. В нашем случае изменяется название подразделение – Delabs (и лучше убрать галочку «Защитить контейнер от случайного удаления»)

Новый объект - Пользователь X

Создать в: demo.lab/delabs

Имя: iwtm-root Инициалы:

Фамилия:

Полное имя: iwtm-root

Имя входа пользователя: iwtm-root @demo.lab

Имя входа пользователя (пред-Windows 2000): DEMO\ iwtm-root

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

Новый объект - Пользователь X

Создать в: demo.lab/delabs

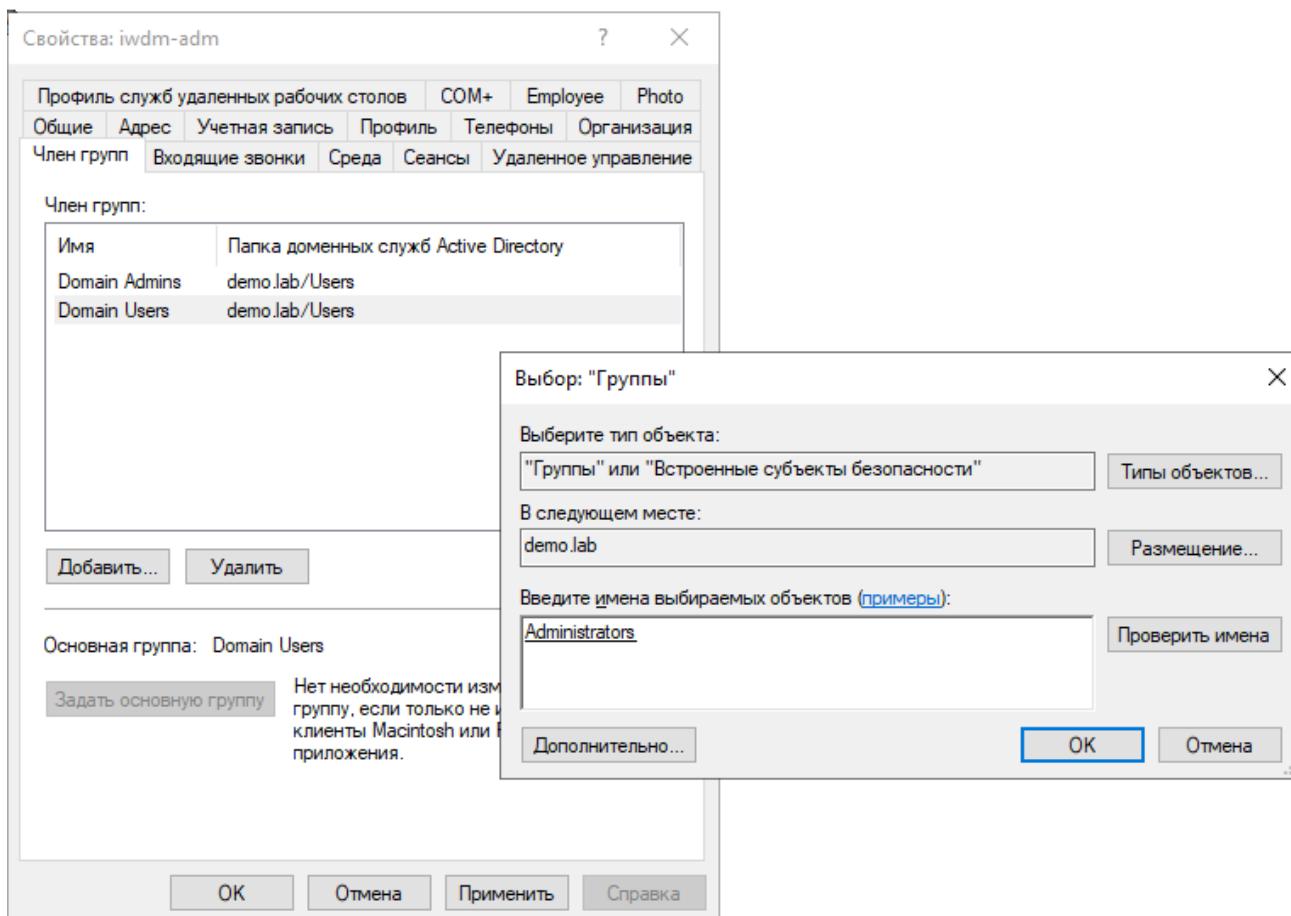
Пароль:

Подтверждение:

Требовать смены пароля при следующем входе в систему  
 Запретить смену пароля пользователем  
 Срок действия пароля не ограничен  
 Отключить учетную запись

Имя	Тип	Описание
iwtmp-root	Пользователь	
ldap-synch	Пользователь	
iwdm-adm	Пользователь	
user-wind	Пользователь	
user-gp	Пользователь	

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



Права администратора для iwdm-adm (зайти в его свойства > член групп). добавляем по заданию (Domain Admins, Administrators)

Задание 2: Настройка DLP сервера

DLP-сервер контроля сетевого трафика уже предустановлен, но не настроен. Необходимо узнать IP-адрес сервера через локальную консоль виртуальной машины и проверить настройки DNS на сервере для корректной работы, в случае несовпадений настроить DNS правильно.

Необходимо проверить наличие активной лицензии и в случае ее отсутствия обратиться к экспертам.

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

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

Заходим на вебку трафик монитора

INFOWATCH TRAFFIC MONITOR

Вход в Систему

Логин

officer

Пароль

Войти

Управление

- LDAP-синхронизация
- Лицензии
- Управление доступом
- Состояние Системы
- Аудит
- Контроль целостности
- Службы
- Плагины
- Почтовый сервер
- Почтовые уведомления

Выбранного периода данные отсутствуют

### LDAP-серверы

	+	✎	✖	▼
DC				

---

#### Настройки соединения

**Внимание!** После сохранения измененных настроек все данные от предыдущих синхронизаций будут потеряны.

LDAP-сервер: 192.168.11.100

Использовать протокол Kerberos:

Глобальный LDAP-порт: 3268

LDAP-порт: 389

Использовать глобальный каталог:

LDAP-запрос: dc=demo,dc=lab

Анонимный доступ:

Логин: ldap-synch@demo.lab

Пароль: .....  
.....

**Сохранить** **Проверить соединение** **Отменить**

[Управление](#)[Еще](#)[LDAP-синхронизация](#)[Лицензии](#)[Управление доступом](#)[Состояние Системы](#)[Аудит](#)[Контроль целостности](#)[Службы](#)[Плагины](#)[Почтовый сервер](#)[Почтовые уведомления](#)

## Управление доступом

### Пользователи

[Создать пользователя](#)[Добавить пользователя из LDAP](#)

Название

Администратор

Офицер без

## Добавить из ldap

Выберите пользователя из LDAP

LDAP-сервер для поиска DC

Поиск iwtm-

Пользователь	Доменный аккаунт	Адрес сервера	Департамент
<input checked="" type="checkbox"/> iwtm-root	iwtm-root@demo.lab	192.168.11.100	

**Сохранить** **Отменить**

## Пользователи

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

## Редактирование пользователя

Логин

Статус

Email

Полное имя

Роли

Области видимости

Описание

Создано: 28.02.2023, 14:51 — Изменено: 28.02.2023, 14:51

**Сохранить** **Отменить**

## Задание 3: Установка и настройка сервера агентского мониторинга

Необходимо ввести сервер в домен, после перезагрузки войти в систему от ранее созданного пользователя iwdm-adm (важно).

После входа в систему необходимо переместить введенный в домен компьютер в ранее созданное подразделение “Delabs” на домене.

Установить базу данных PostgreSQL или функциональный аналог с паролем суперпользователя xxXX5566.

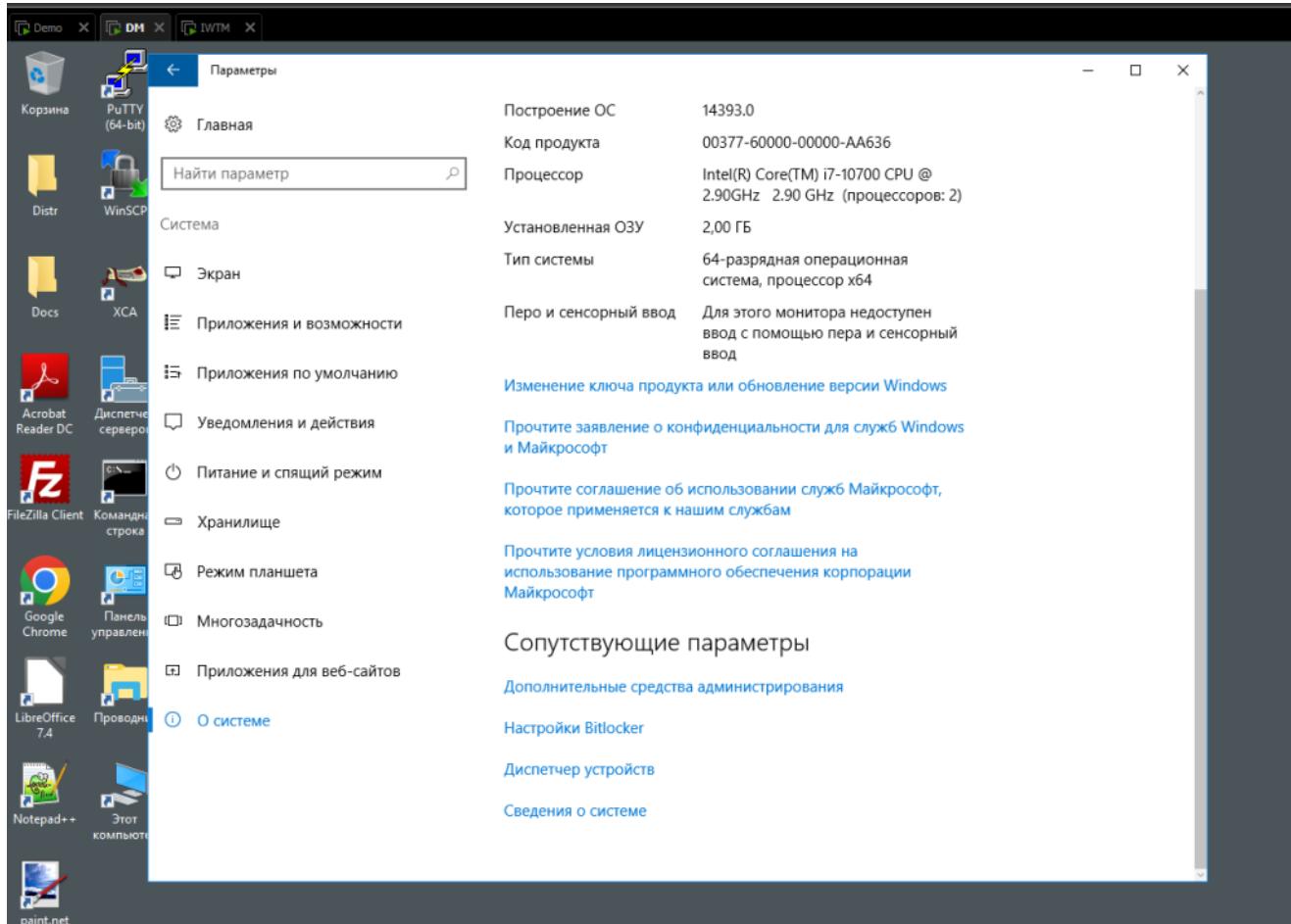
Установить сервер агентского мониторинга с параметрами по умолчанию, подключившись к ранее созданной БД.

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 xxXX5566

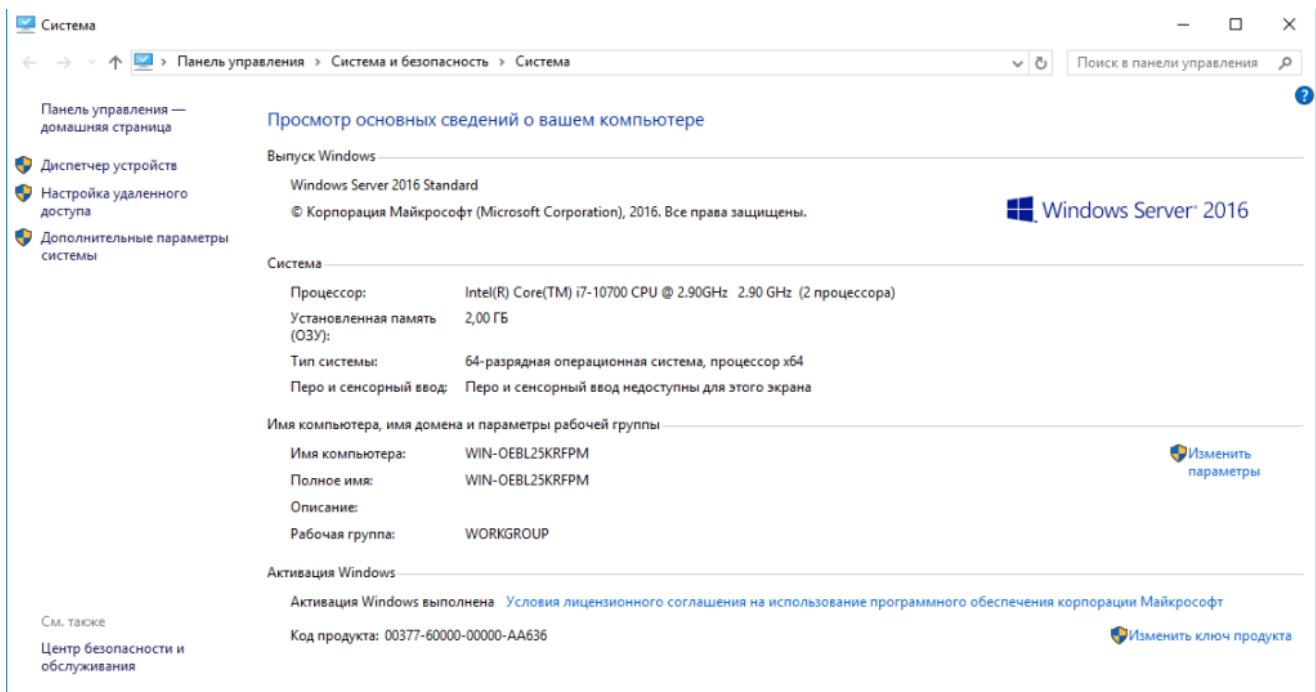
Синхронизировать каталог пользователей и компьютеров с Active Directory.

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

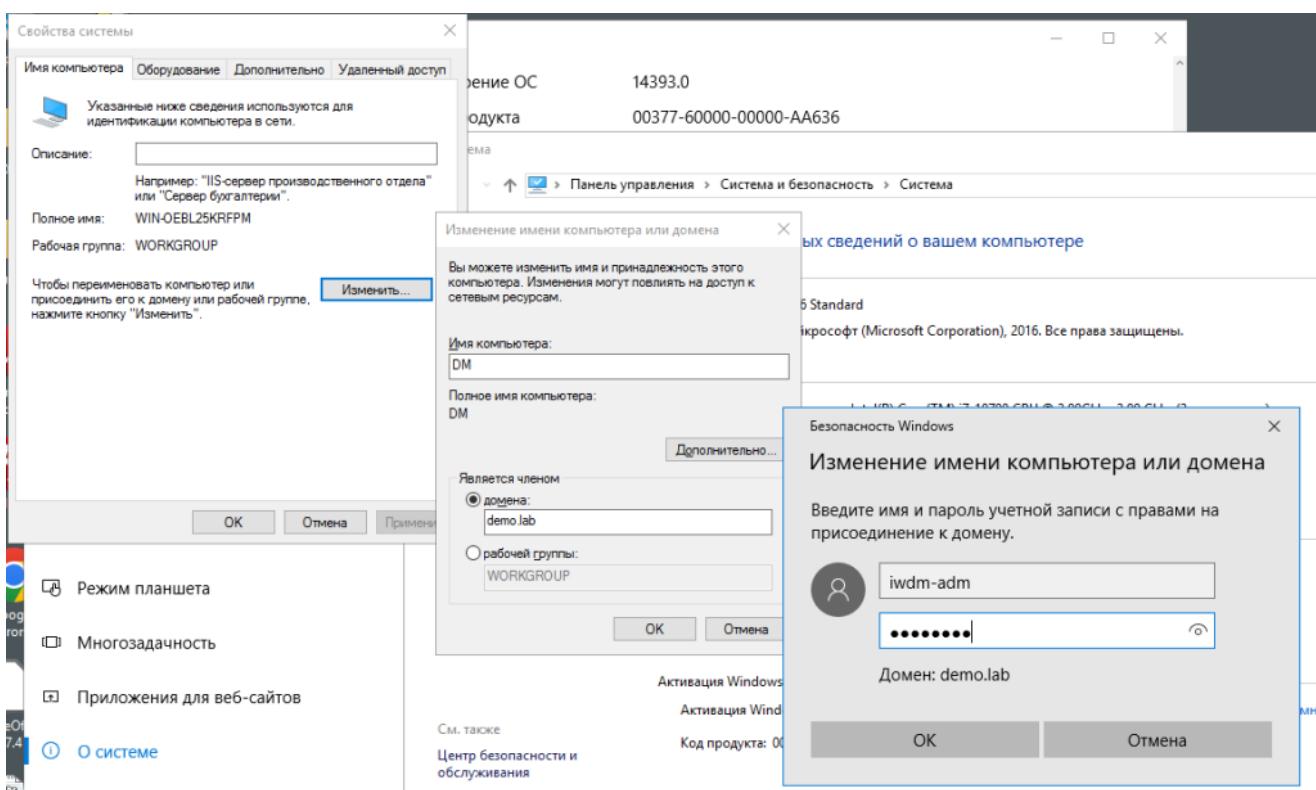
Проверить работоспособность входа в консоль управления без ввода пароля. Если сервер не введен в домен или работает от другого пользователя, данная опция работать не будет.



## Параметры → Система → О системе → Сведения о системе

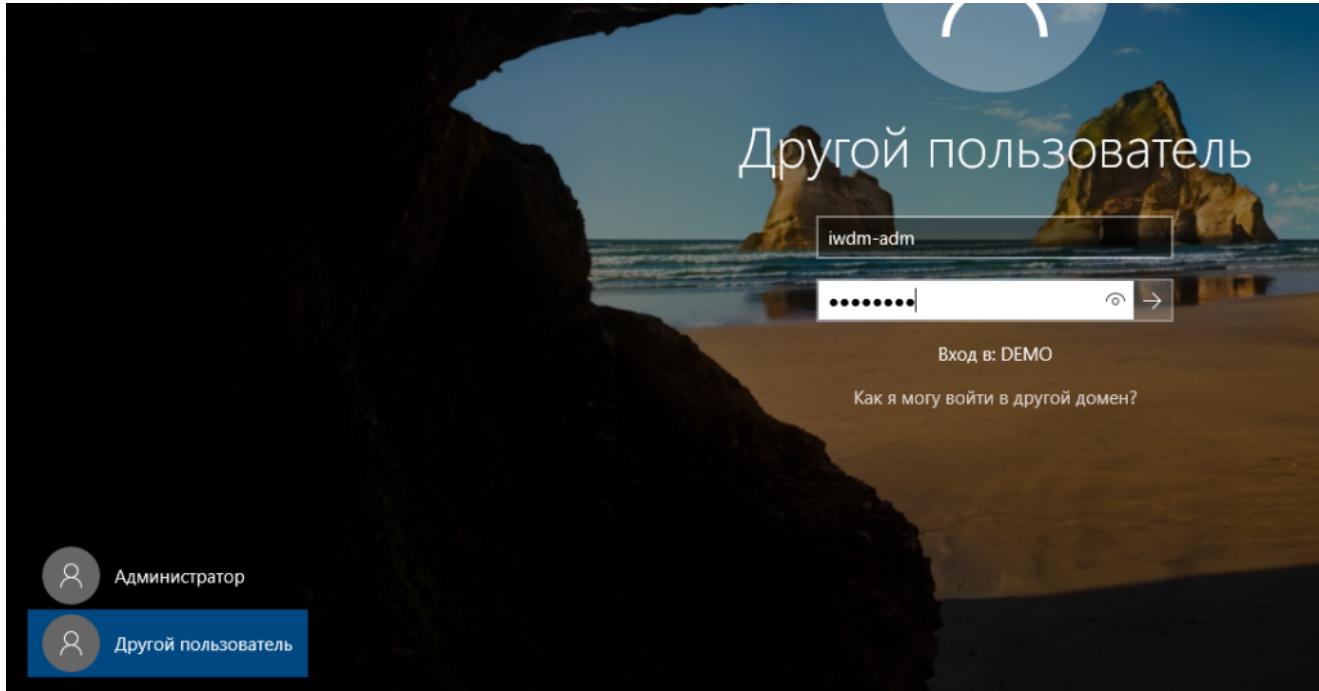


## Изменить параметры



## Изменить

Меняем имя и вносим в домен.



После перезагрузки входим в пользователя iwdm-adm (меняется в зависимости от задания)

в active directory переносим компьютер в подразделение delabs

Имя	Тип	Описание
DEMO-DC	Компьютер	
DM	Компьютер	

The screenshot shows the Windows Active Directory Users and Computers snap-in. On the left, the navigation pane displays the structure of the domain: 'Пользователи и компьютеры Active Direct' > 'Сохраненные запросы' > 'demo.lab' > 'Users'. A folder named 'delabs' is selected. On the right, a list of users is shown in a table format:

Имя	Тип	Описание
DM	Компьютер	
iwtm-root	Пользователь	
ldap-synch	Пользователь	
iwdm-adm	Пользователь	
user-wind	Пользователь	
user-gp	Пользователь	

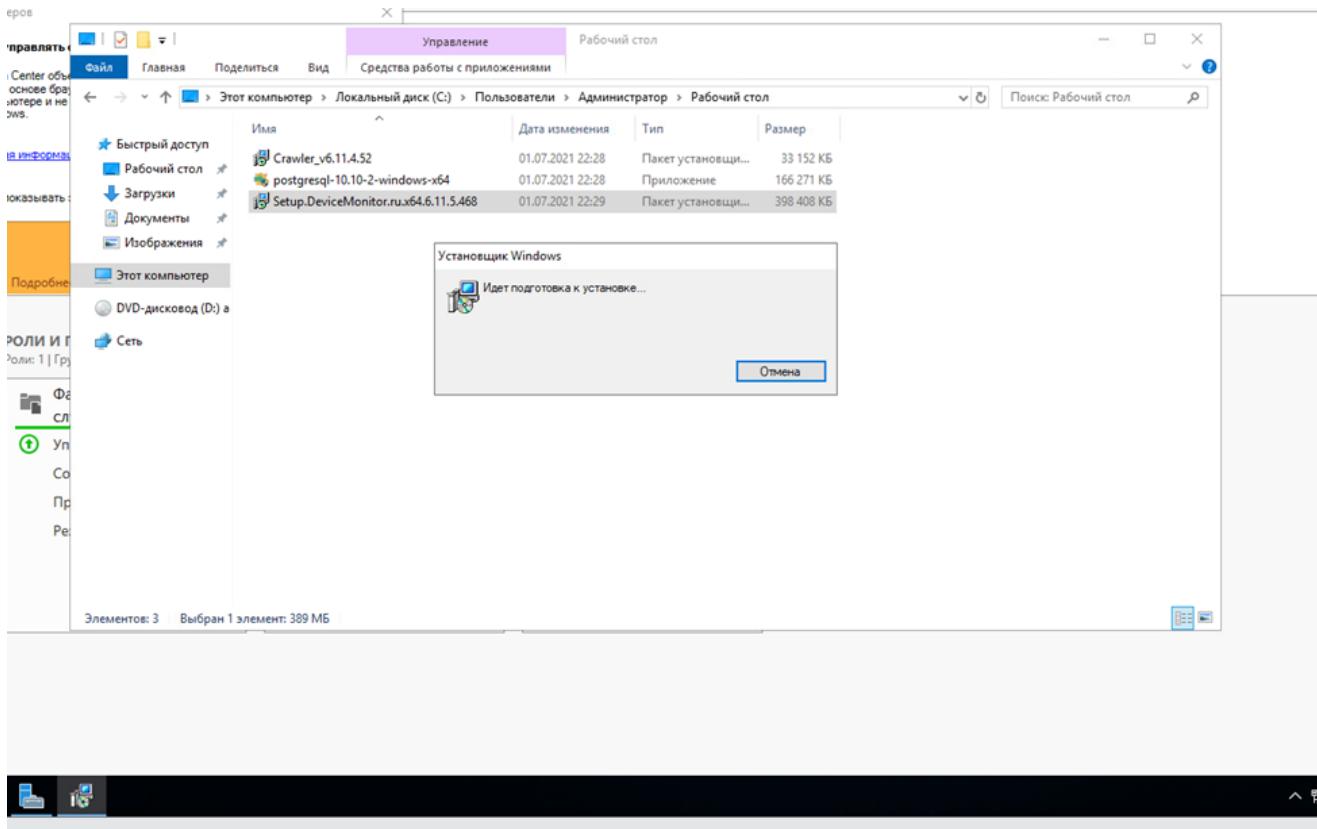
Подразделение будет отличаться, но принцип такой же (перетащить с папки где компьютеры в созданное ранее подразделение)

The screenshot shows the Windows Server Manager interface. The title bar reads 'Диспетчер серверов > Панель мониторинга'. The main pane displays the 'Мониторинга' tab. A file named 'Setup.DeviceMonitor.ru.x64.6.11.5.468' is being copied from the 'Локальный диск (C:)' to the 'Рабочий стол' of the 'Администратор' user. A progress dialog box for 'Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.40660' is visible, showing 'Processing: Microsoft Visual C++ 2013 x64 Minimum Runtime - 12.0.40660'.

## Установка базы данных

(При установке оставляем все без изменения, кроме пароля, и снять галку stack builder)

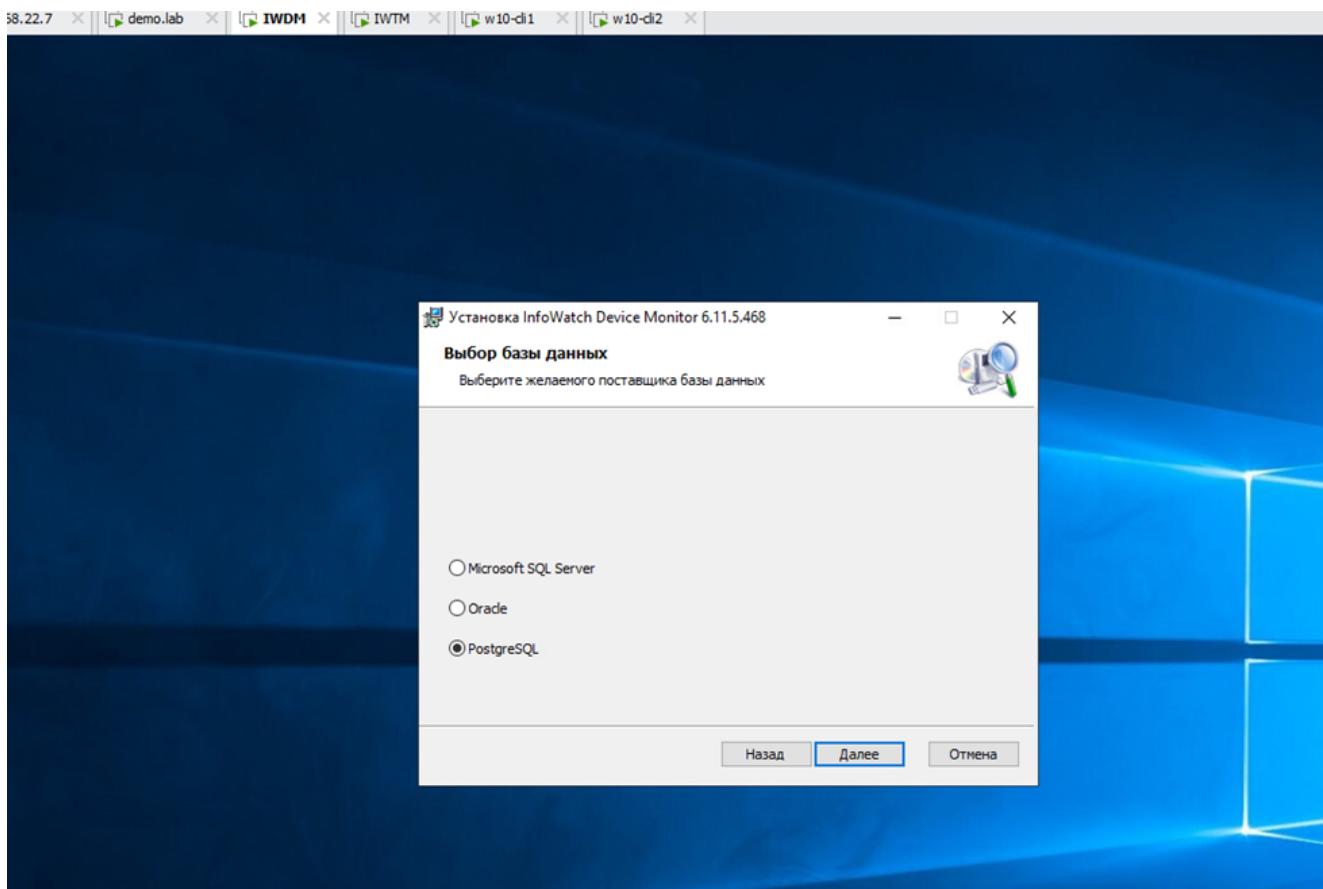
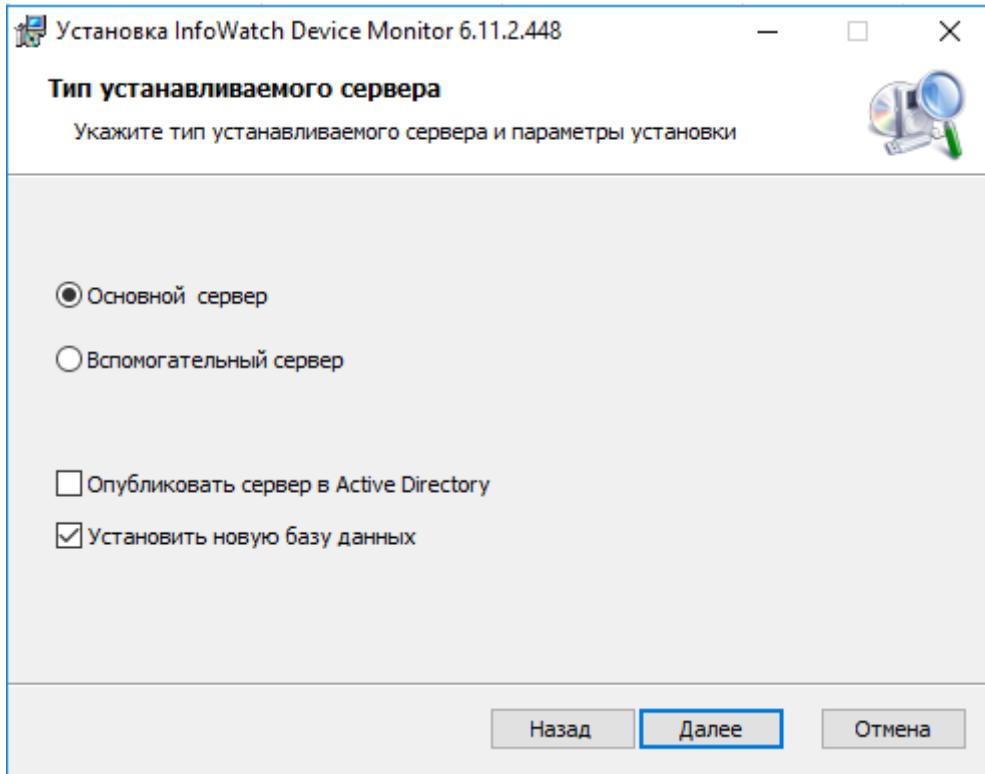
Устанавливаем базу (в случае возникновения ошибки при установке необходимо заново попробовать установить.).

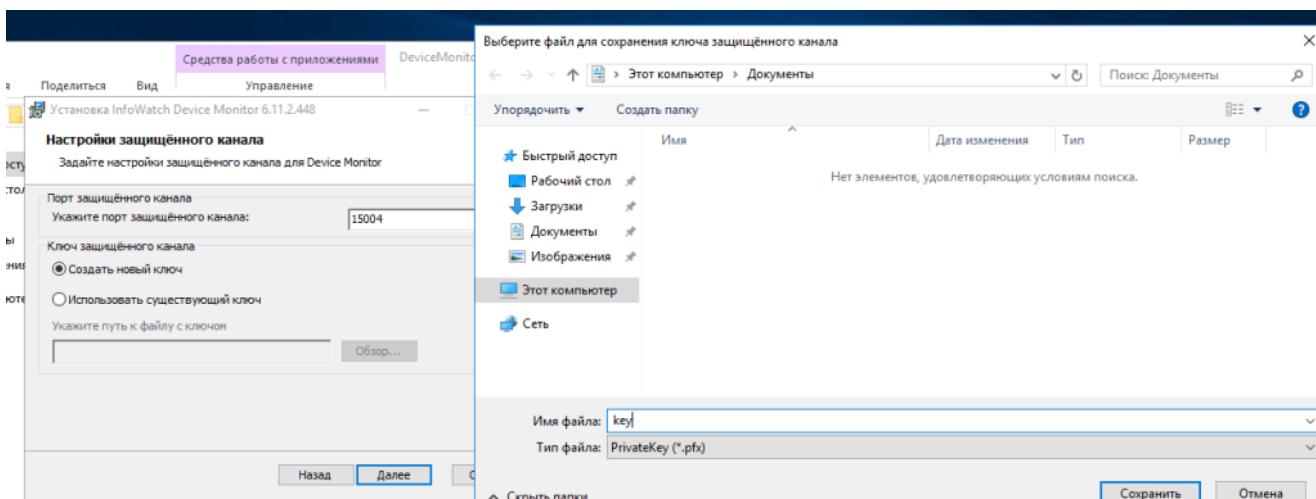
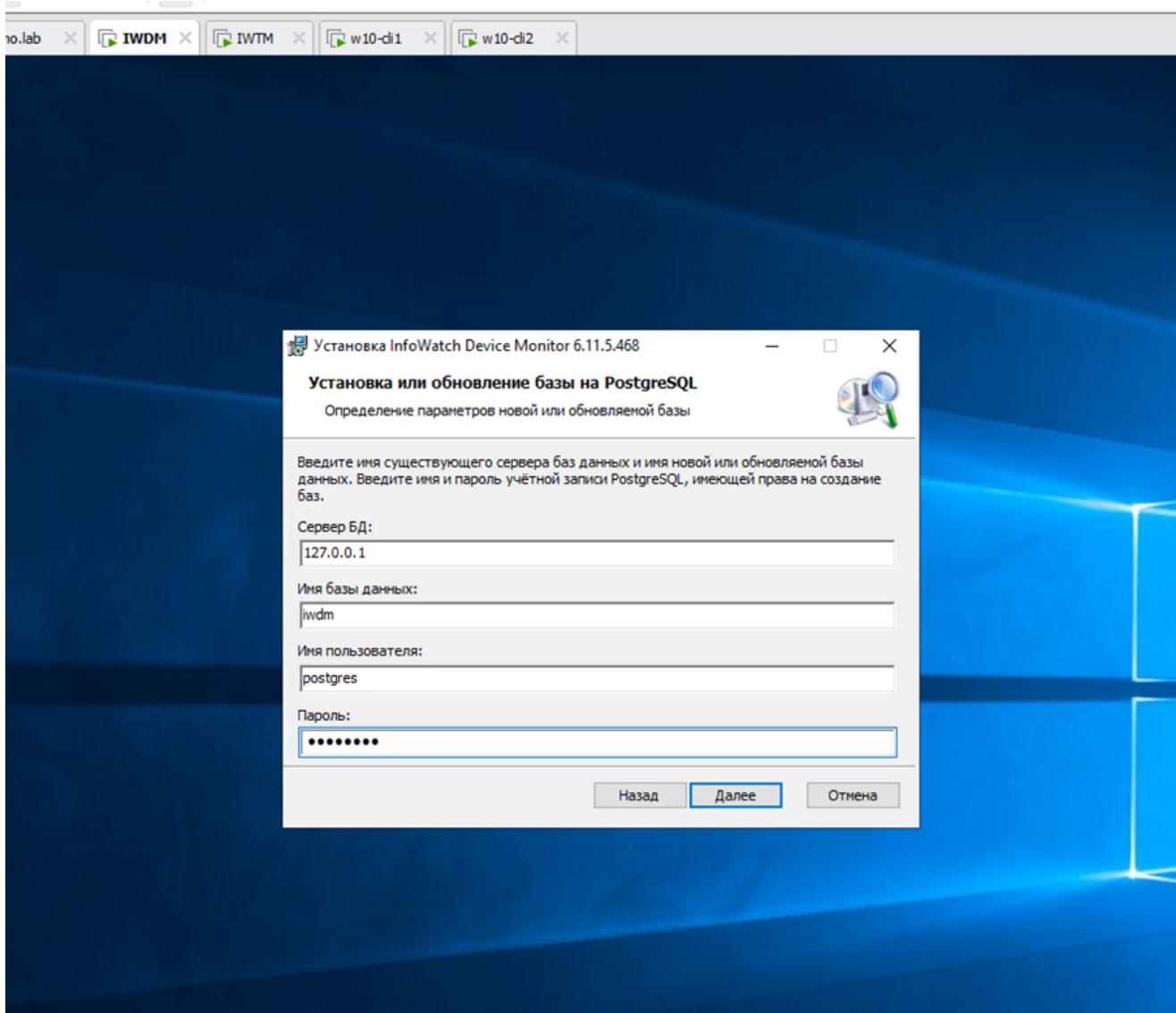


после установки базы данных начинаем установку (скриншоты только где происходит изменение)

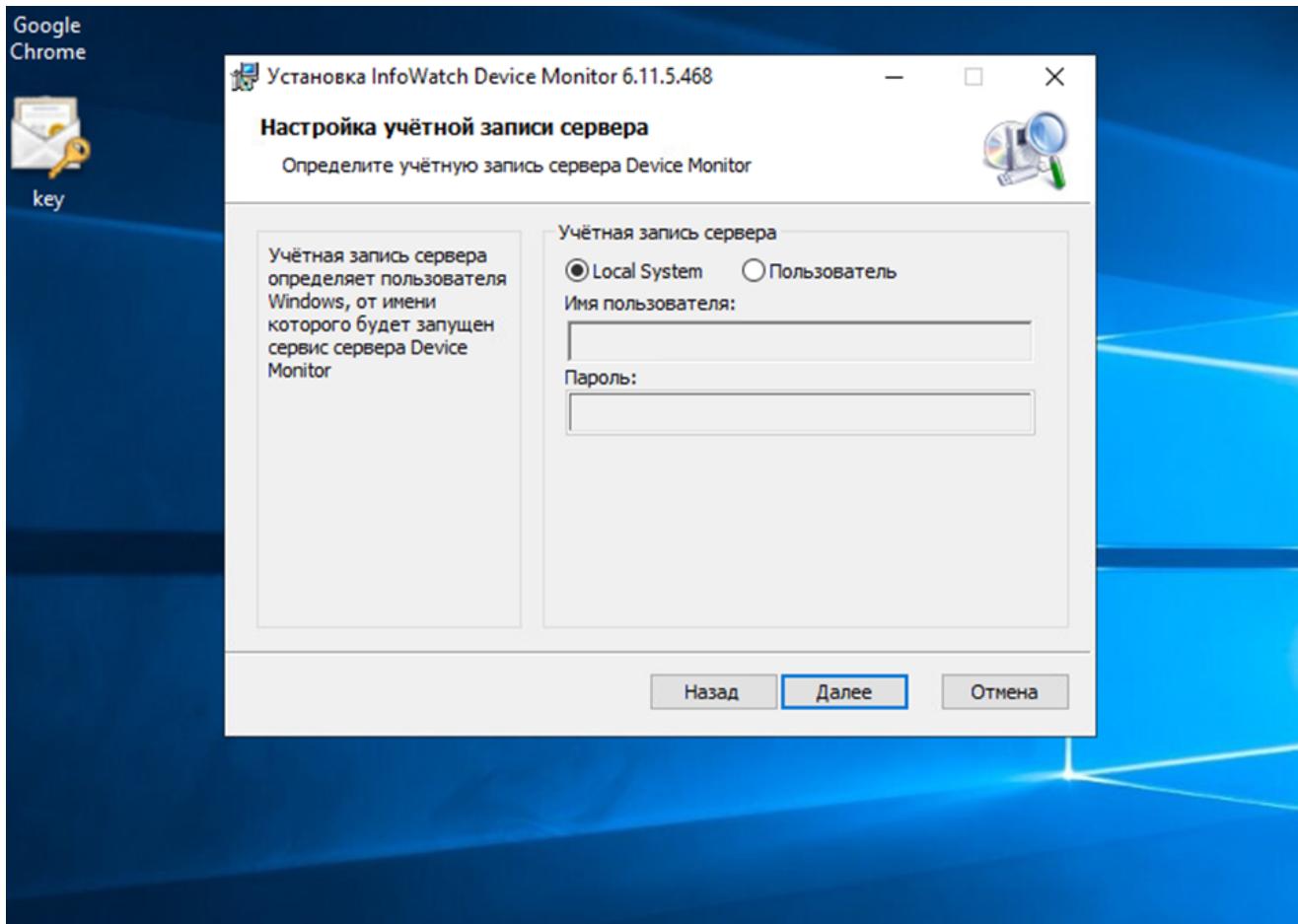
Статус	Имя	Содержание	Описание
Активный	Token-3	9bq0vugxxuej3fvr166h	

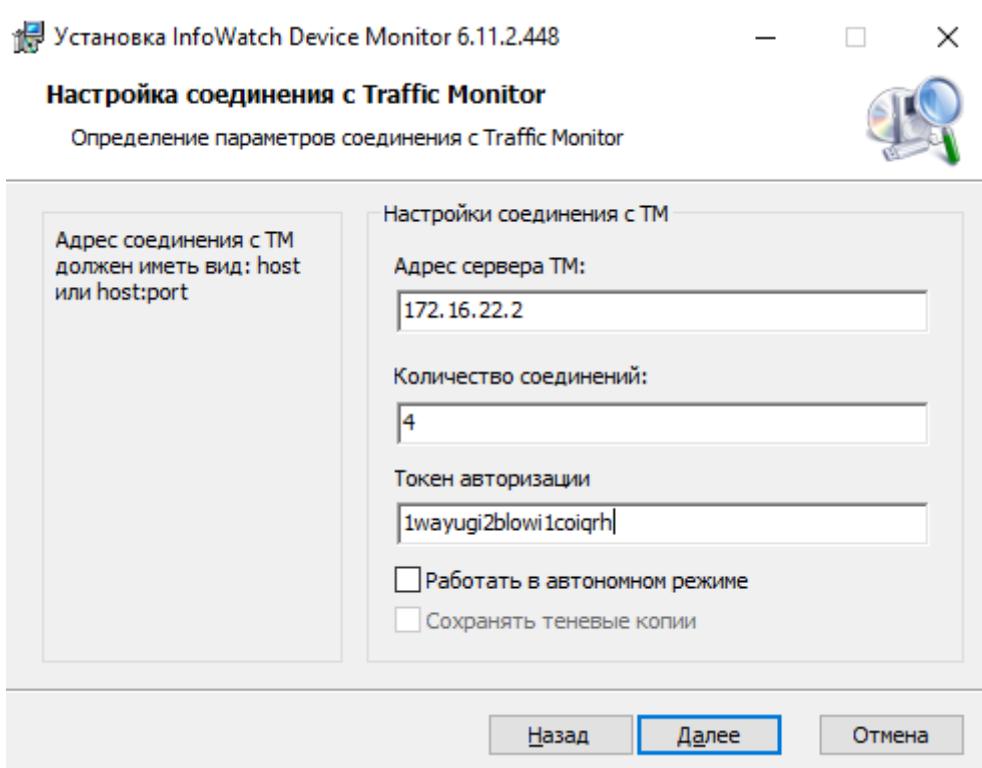
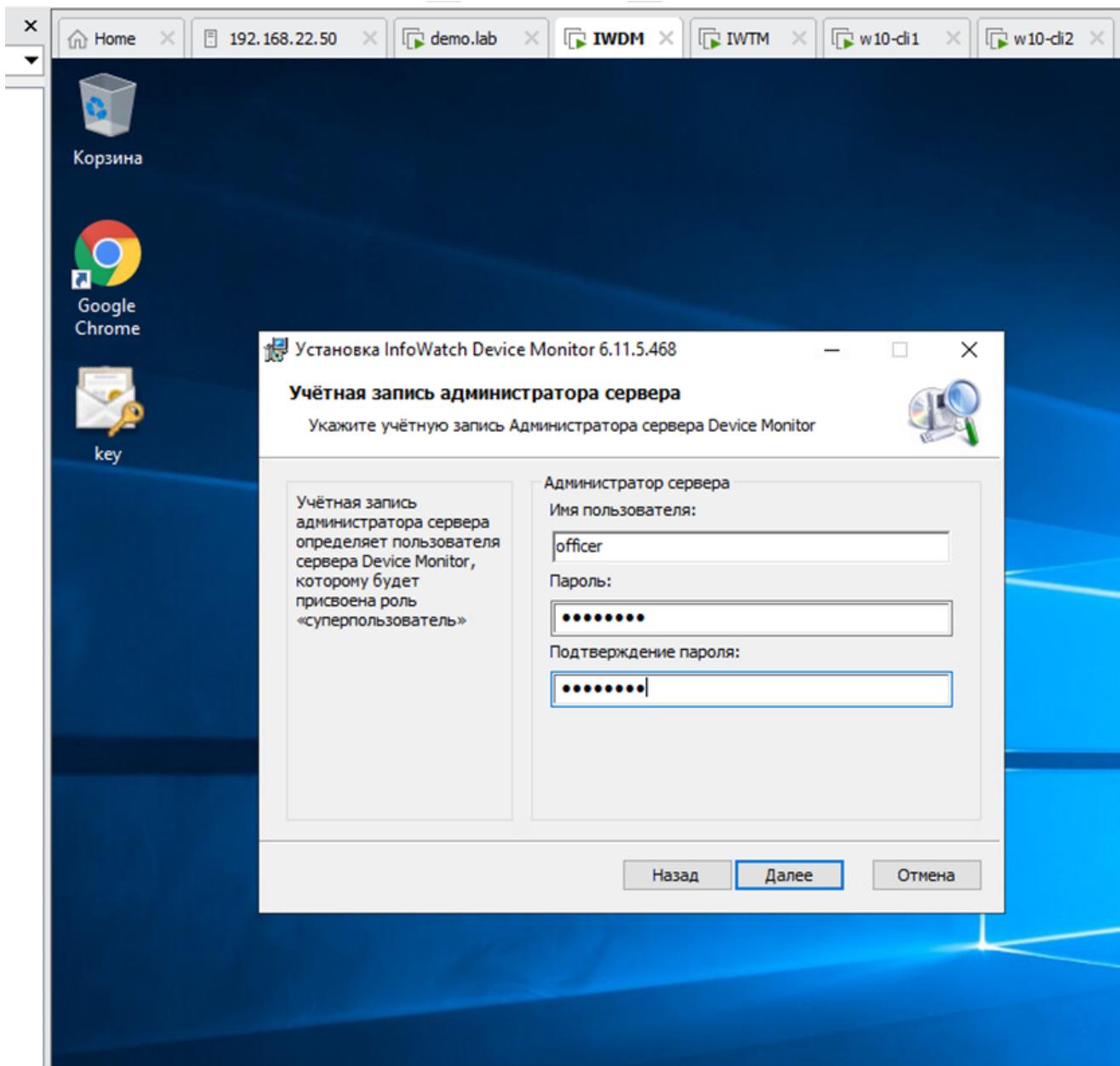
Управление → Плагины



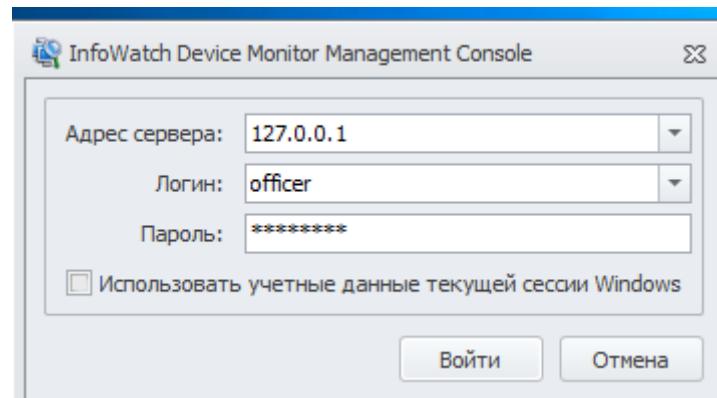


**любое имя и сохранить**

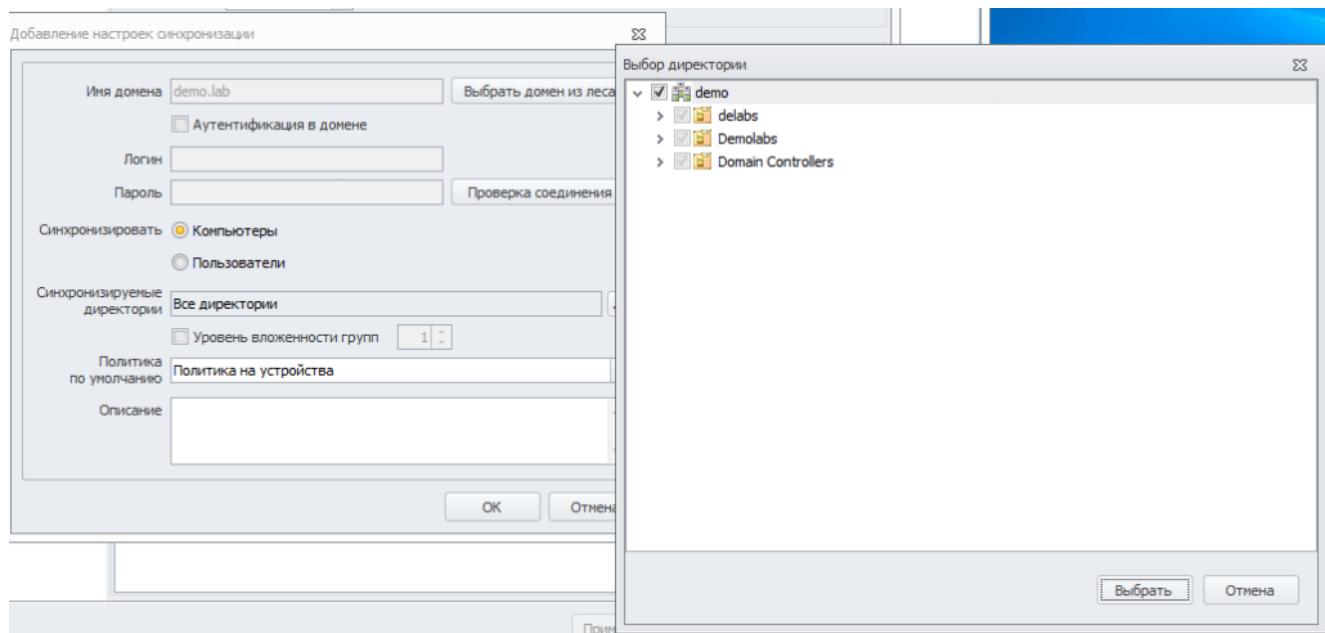


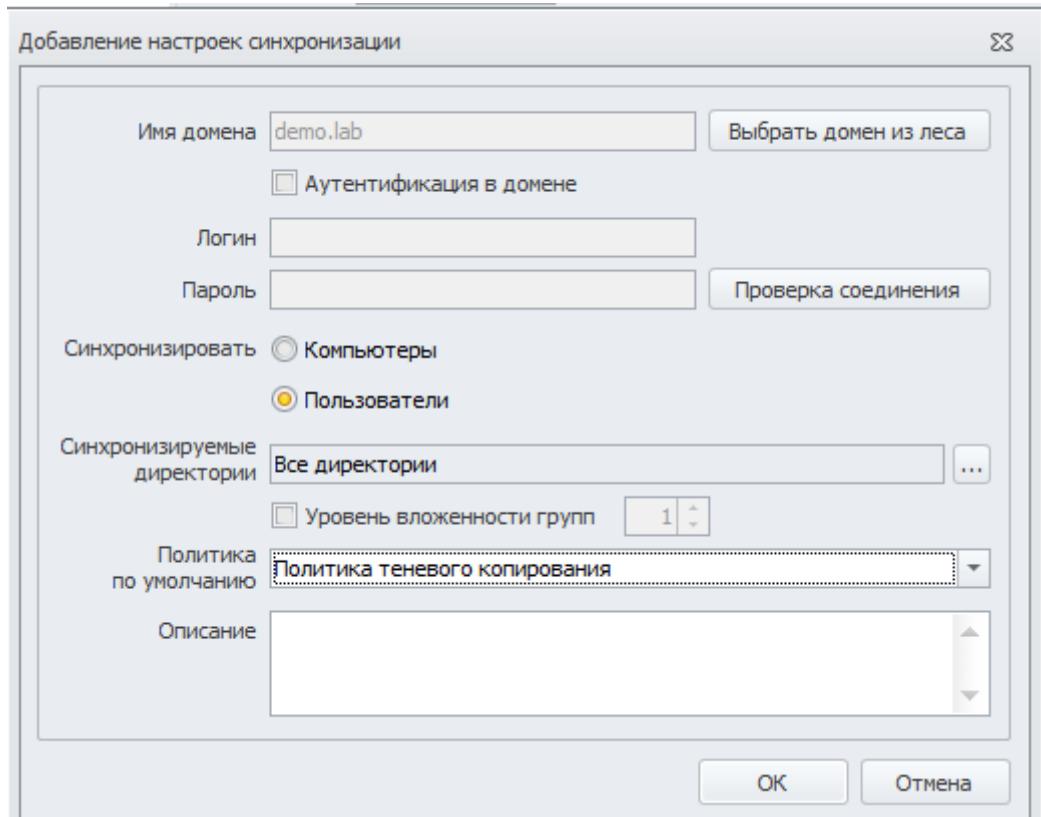


Далеее вход в консоль на рабочем столе



инструменты → настройки

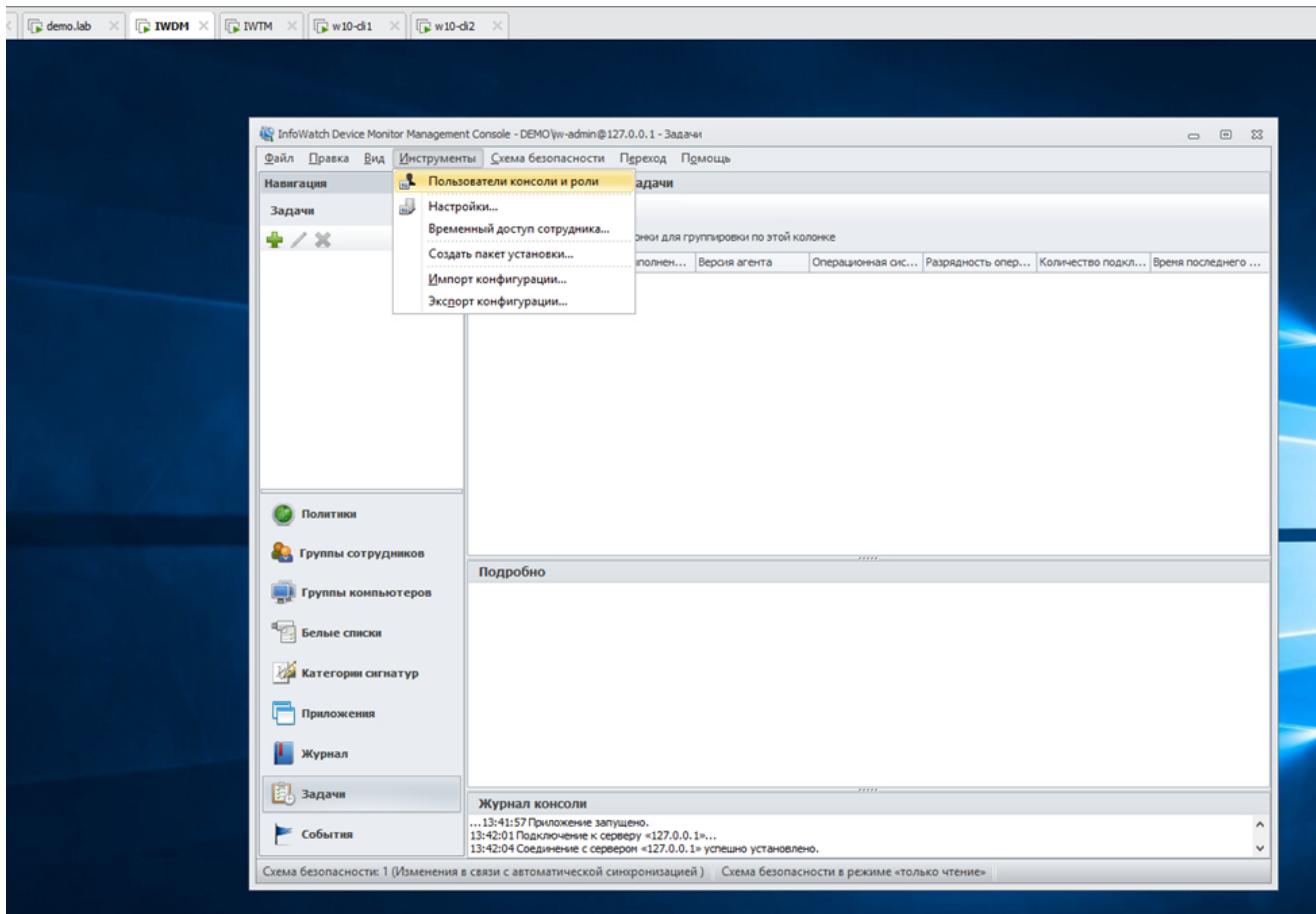




у компьютеров политика на устройства

у пользователей теневое копирование

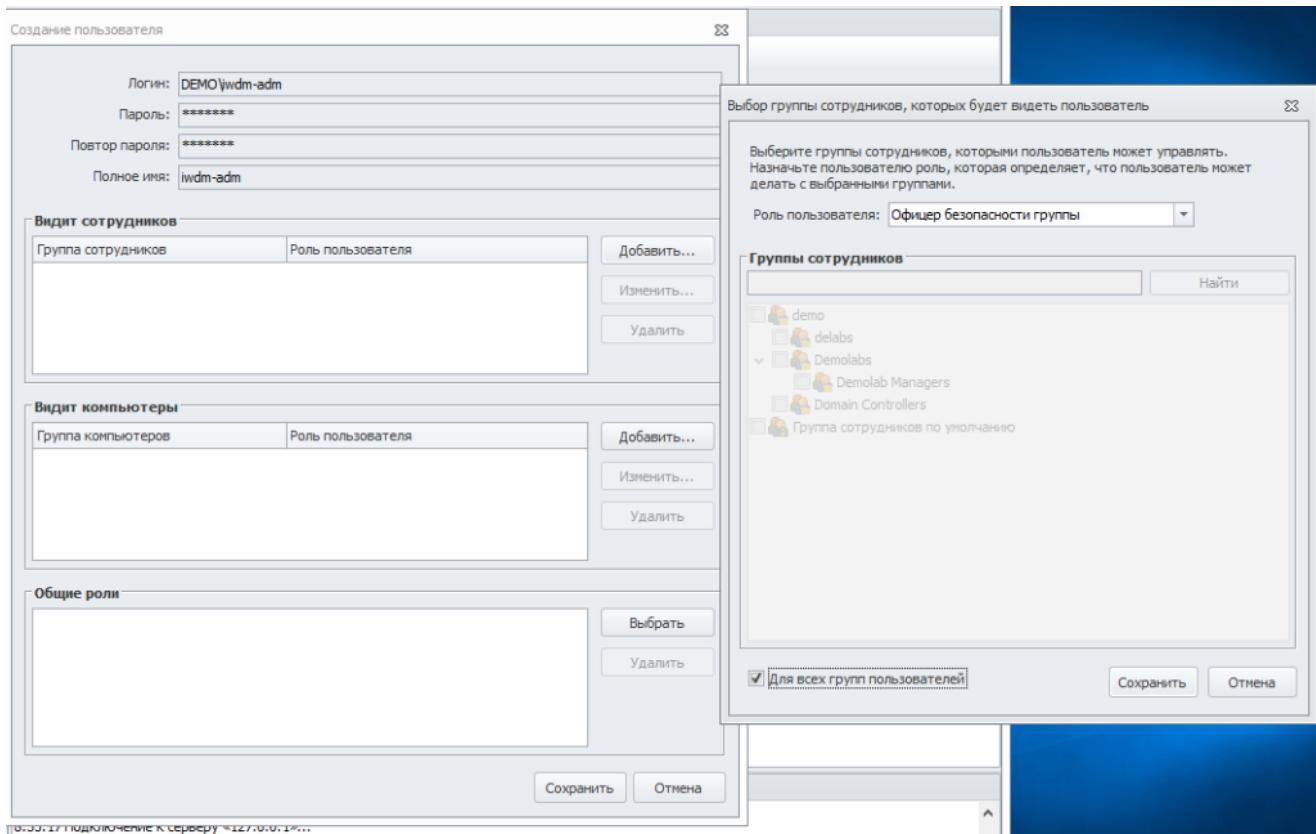
Домен	Синхронизировать	Директории	Статус синхронизации	Время синхронизации
demo.lab	Компьютеры	Все директории	Успешно	01.03.2023 8:37:14
demo.lab	Пользователи	Все директории	Успешно	01.03.2023 8:37:16



The screenshot shows a software interface for managing users. At the top, there's a header bar with the title 'Пользователи консоли' (Console Users) and a close button. Below the header, there are two tabs: 'Пользователи консоли' (Console Users) and 'Роли' (Roles). A dropdown menu labeled 'Показать записи:' with the option 'Все' (All) is visible. The main area is titled 'Пользователи:' (Users) and contains a table with columns: Статус (Status), Логин (Login), Группы (Groups), and Полное имя (Full Name). One row is shown: 'officer' under 'Логин' and 'Все группы' (All groups) under 'Группы'. To the right of the table are two buttons: 'Добавить из AD' (Add from AD) and 'Создать...' (Create...). Below this, a modal window titled 'Добавление пользователя из AD' (Adding user from AD) is open. It has a search bar with the text 'iwdm-adm' and a 'Найти' (Find) button. On the left, a tree view shows a 'Директория: demo.lab' (Directory: demo.lab) node expanded, with a 'delabs' folder selected. On the right, a table lists the found user: Account 'iwdm-adm@demo.lab', Last Name 'iwdm-adm', and First Name 'iwdm-adm'.

Выбираем добавить из AD

Далее из ранее созданного подразделения – iwdm-adm и жмем сохранить



добавляем видит сотрудников, видит компьютеры, общие роли.

Создание пользователя

Логин: DEMO\iwdm-adm

Пароль: \*\*\*\*\*

Повтор пароля: \*\*\*\*\*

Полное имя: iwdm-adm

**Видит сотрудников**

Группа сотрудников	Роль пользователя	
Все группы	Офицер безопасности группы	Добавить... Изменить... Удалить

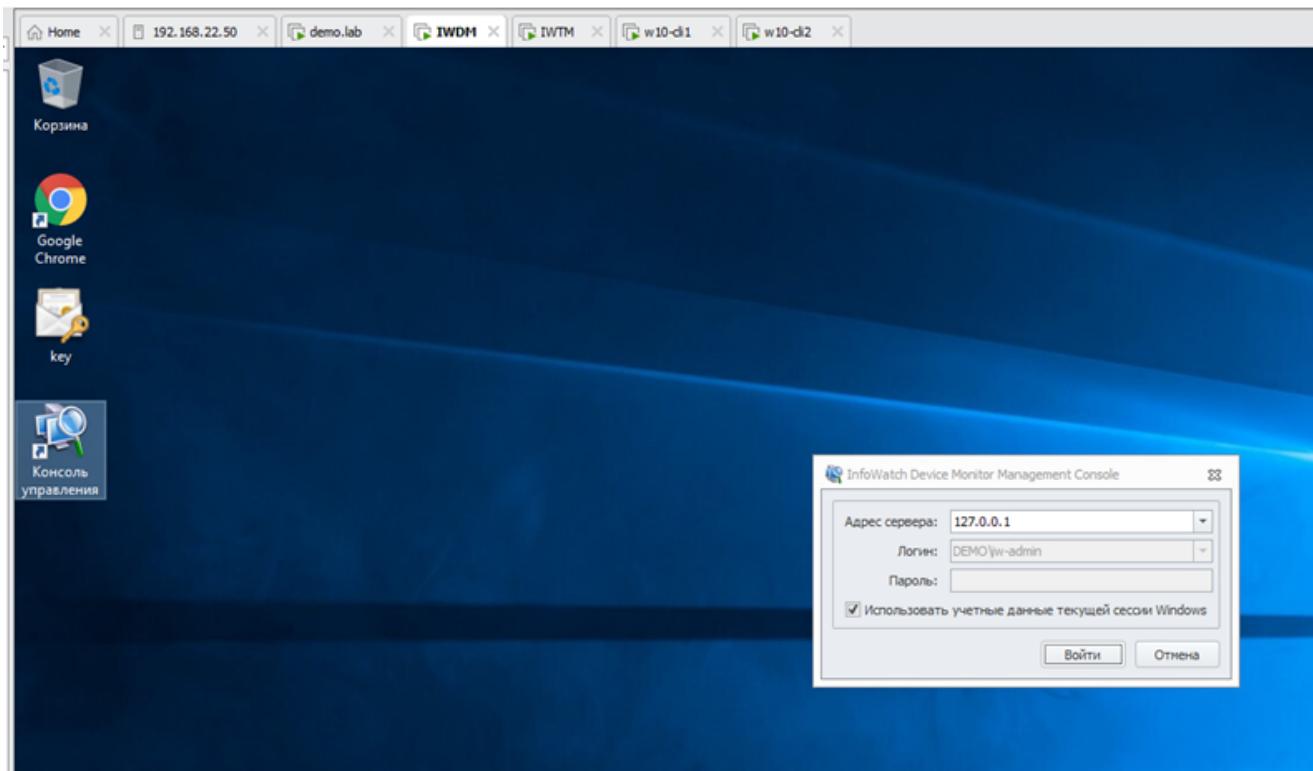
**Видит компьютеры**

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

**Общие роли**

Офицер безопасности	
Администратор	Выбрать Удалить

**Сохранить** **Отмена**



Теперь проверяем вход без пароля

#### 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-wind.

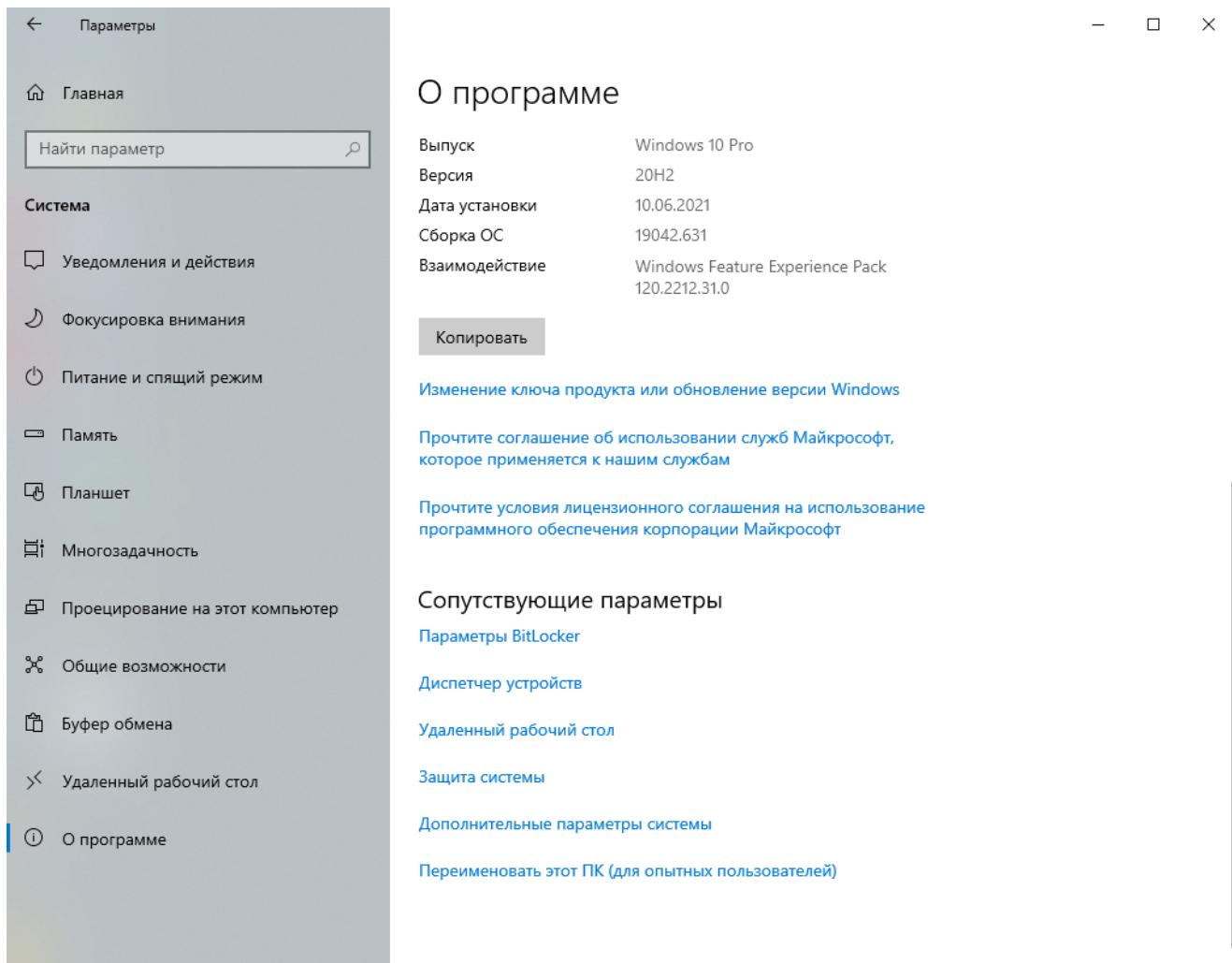
Необходимо ввести клиентскую машину 2 в домен, после перезагрузки войти в систему от ранее созданного пользователя user-grp.

После входа в систему необходимо переместить веденные в домен компьютеры в ранее созданное подразделение "Delabs" на домене.

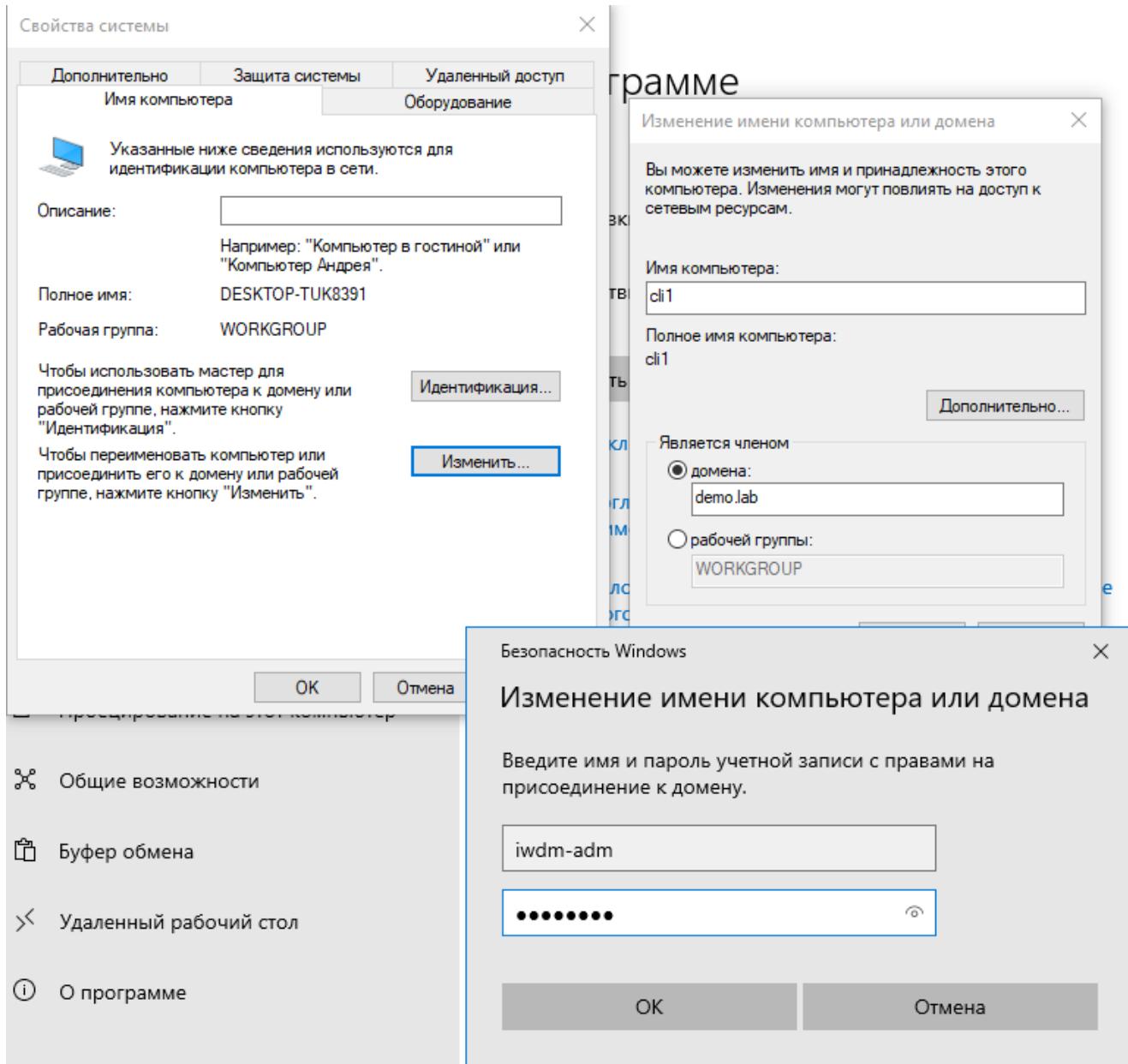
Установить агент мониторинга:

На машину 1 (user-wind) с помощью задачи первичного распространения с сервера агентского мониторинга. Необходимо учесть, что установка осуществляется только с правами администратора (доменного или локального). Ручная установка с помощью создания и переноса любым способом пакета установки является некорректным выполнением задания.

На машину 2 (user-gp) с помощью групповых политик домена. Допускается как удаленная установка созданного вручную пакета, так и с помощью удаленной установки компонента Deploy Agent с последующей установкой через задачи сервера агентского мониторинга.



параметры → о программе → переименовать пк (для опытных пользователей)



на клиенте 2 повторяем

The screenshot shows the Windows Active Directory Users and Computers management console. On the left, a tree view displays the domain structure under 'demo.lab', including 'Builtin', 'Computers', 'demo', 'Demolabs', 'Domain Controllers', 'ForeignSecurityPrincipals', 'Managed Service Accounts', and 'Users'. On the right, a table lists various objects with their names, types, and descriptions:

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	
user-agent2	Пользователь	

Просто перетаскиваем пк клиента с Computers в подразделение

после перезагрузки заходим под пользователями user-wind на клиенте 1 и user-gr на клиенте 2

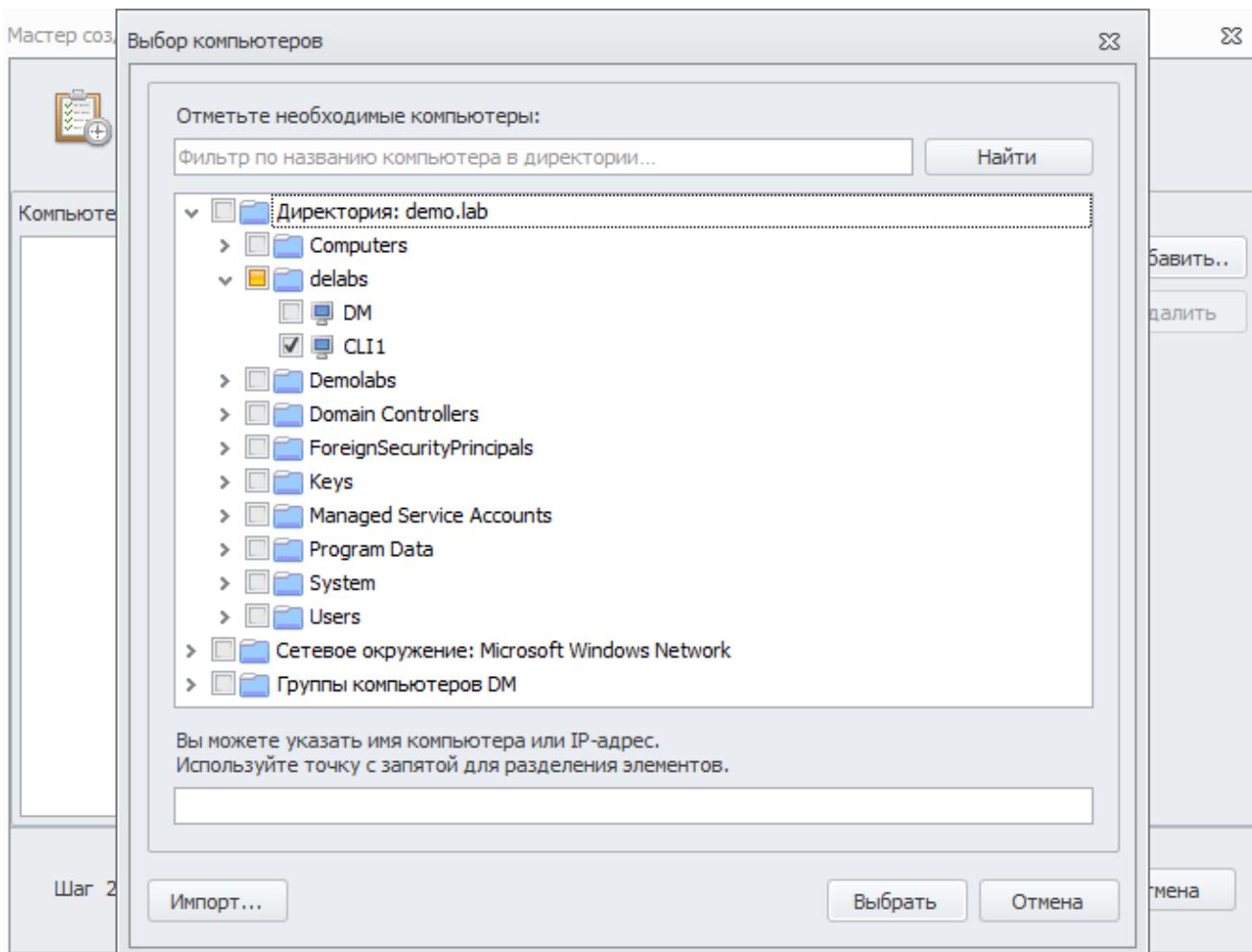
The screenshot shows the InfoWatch Device Management Console interface. The main window title is 'InfoWatch Device Management Console - officer@127.0.0.1 - Задачи'. The left sidebar navigation includes 'Политики', 'Группы сотрудников', 'Группы компьютеров', 'Белые списки', 'Категории сигнатур', 'Приложения', 'Журнал', 'Задачи', and 'События'. A central window titled 'Мастер создания задачи' (Task Creation Wizard) is open, showing the first step: 'Вас приветствует мастер создания задачи' (The wizard greets you). It asks to 'Задайте основные параметры задачи' (Define basic task parameters). The fields shown are 'Назначение:' (Name: Install) and 'Тип:' (Type: Задача первого распространения). Below the wizard is a 'Журнал консоли' (Console Log) pane with the following entries:

```

...13:14:26 Приложение запущено.
13:14:42 Подключение к серверу «127.0.0.1»...
13:14:46 Соединение с сервером «127.0.0.1» успешно установлено.

```

## В задачах добавляем новую



**Мастер создания задачи**

**Укажите параметры настройки агентского модуля и запуска задачи**

Зашитить от удаления:

Пароль:  Подтвердить:

Скрывать присутствие агента на компьютере до получения конфигурации с сервера ДМ

Устанавливать компонент перехвата сетевого трафика

Устанавливать компонент контроля сетевых соединений

Параметры запуска задачи:

Количество запусков:  Каждые:  минут

Запустить задачу сразу после сохранения

Запуск задачи от имени учётной записи:

Логин:  Пароль:

Шаг 5 из 7

< Назад    Далее >    Отмена

**Мастер создания задачи**

**Укажите параметры перезагрузки**

Ожидать перезагрузки без уведомления сотрудника:

- Не ожидать
- Ожидать  час(ов)
- Ожидать бесконечно

Уведомлять сотрудника о необходимости перезагрузки и ожидать перезагрузки:

- Не уведомлять
- Уведомлять в течение  час(ов) каждые  минут(ы)
- Уведомлять бесконечно каждые  минут(ы)

Текст уведомления:

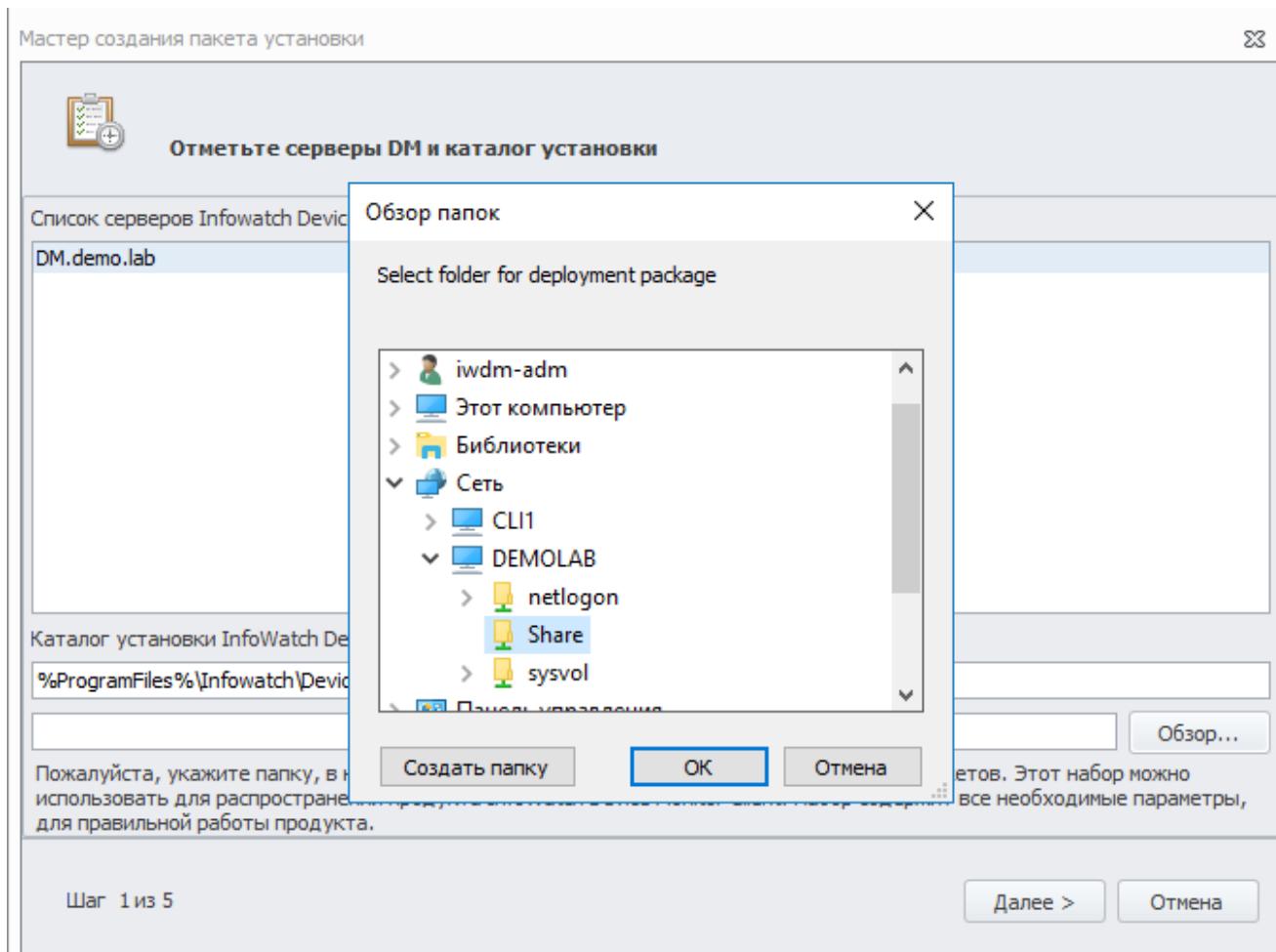
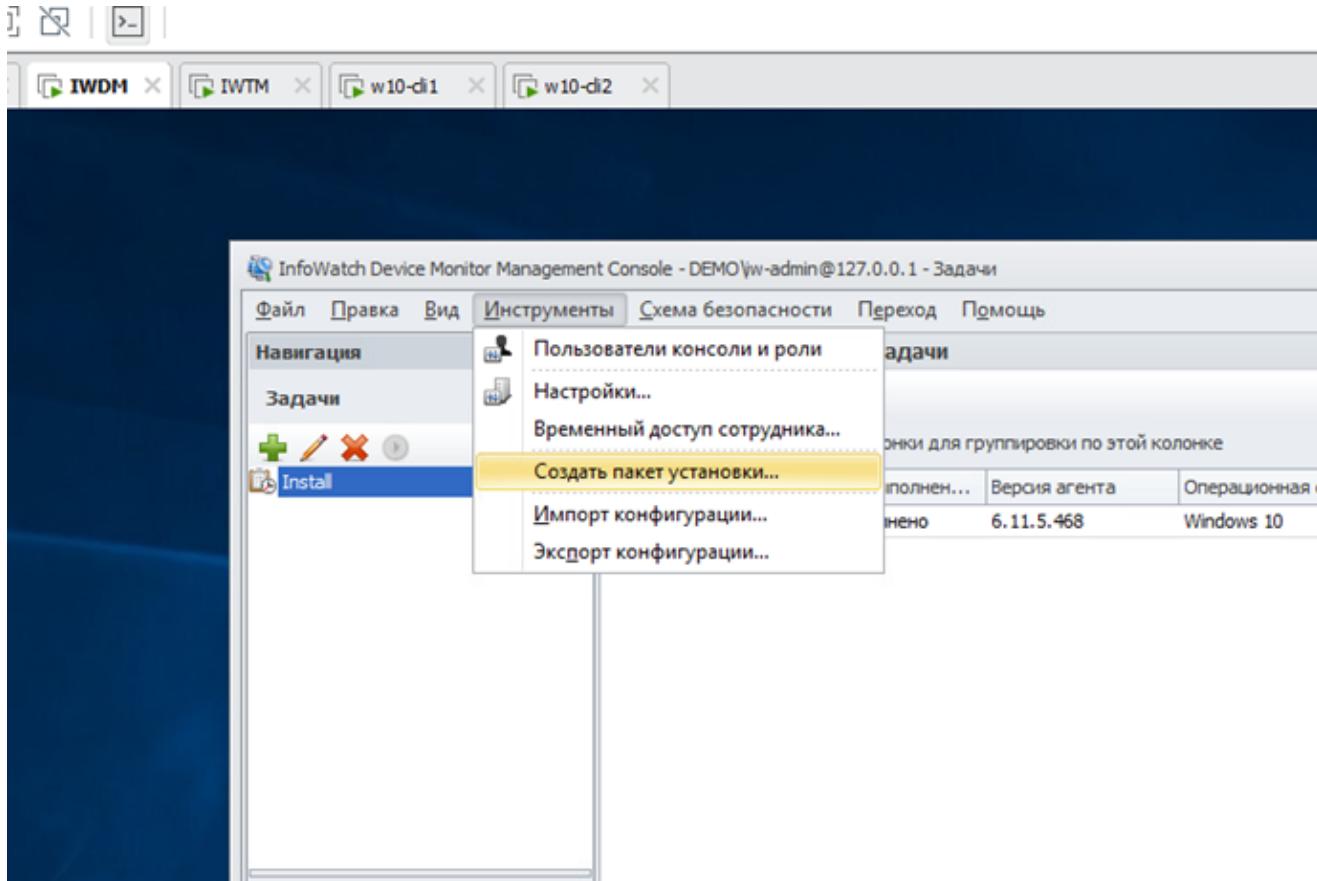
Показать предупреждение перед принудительной перезагрузкой

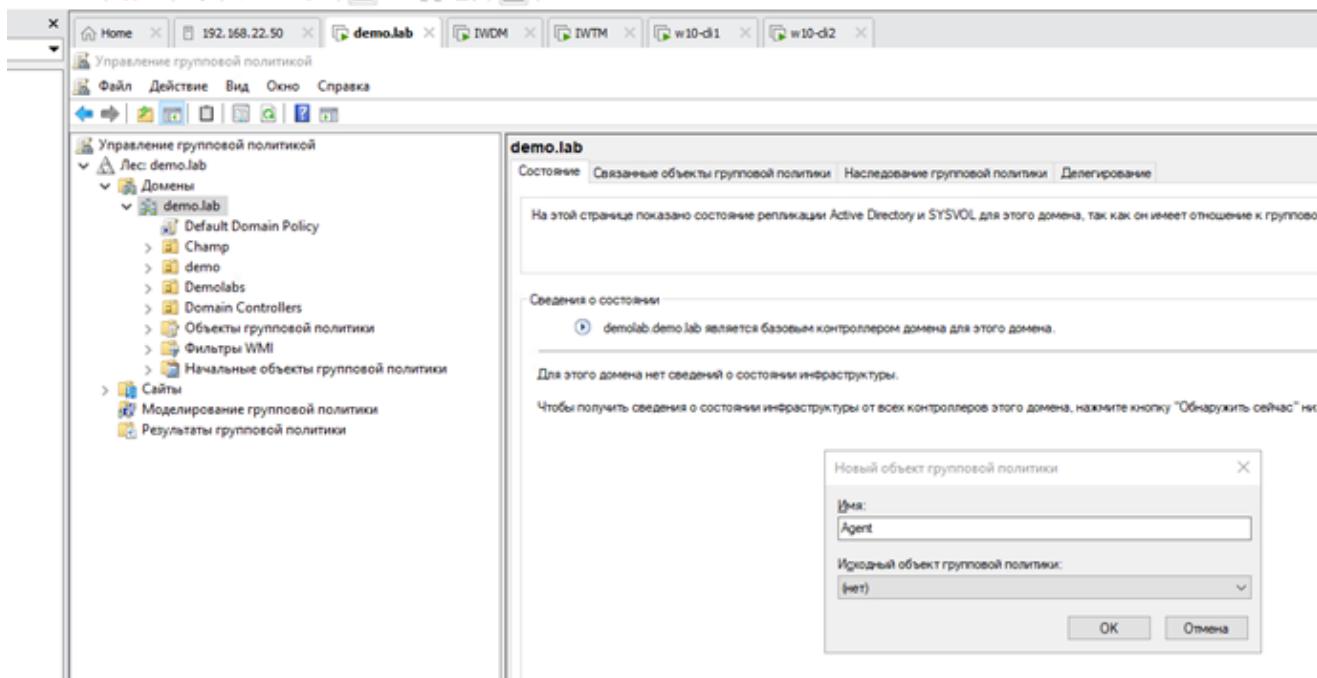
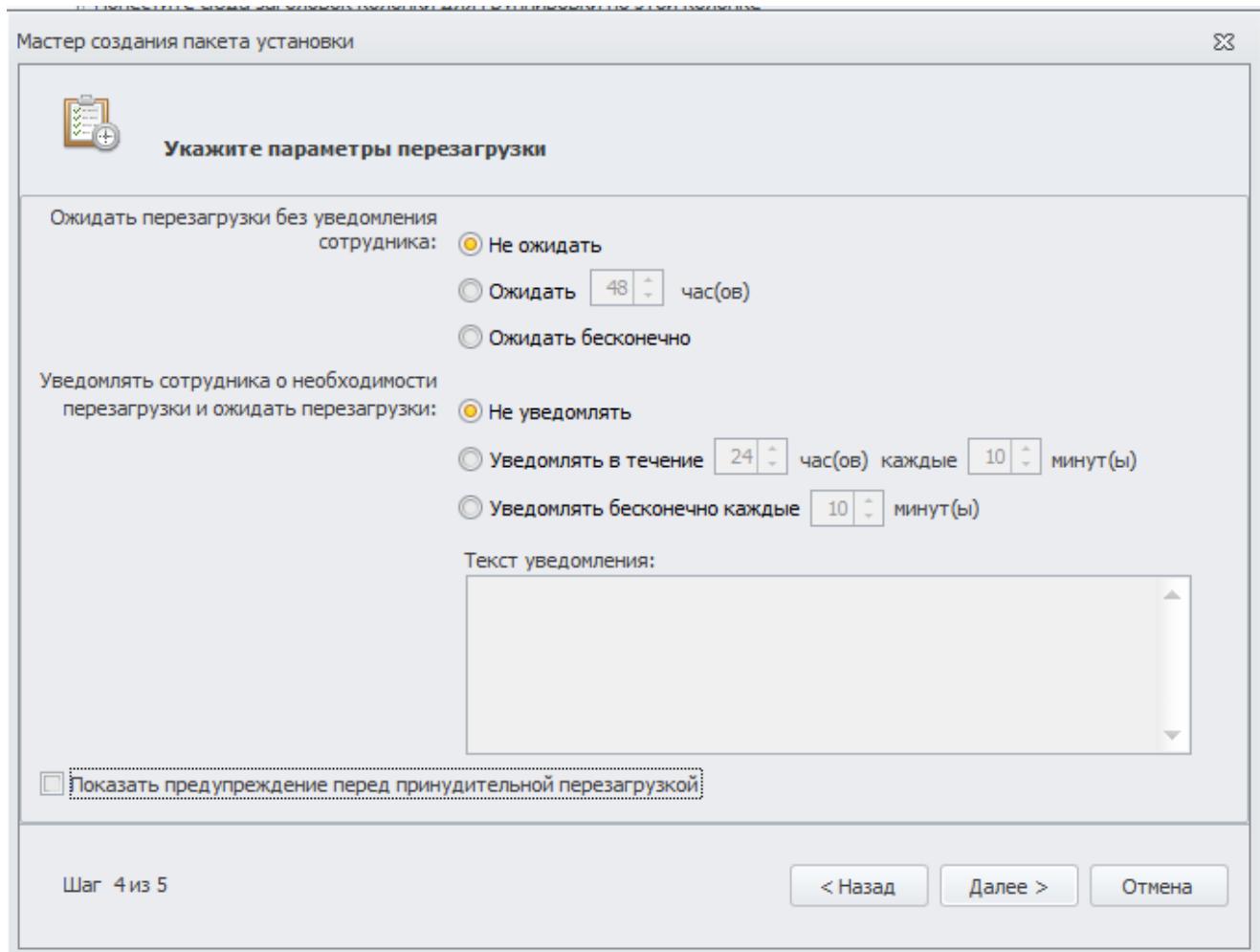
Шаг 6 из 7

< Назад    Далее >    Отмена

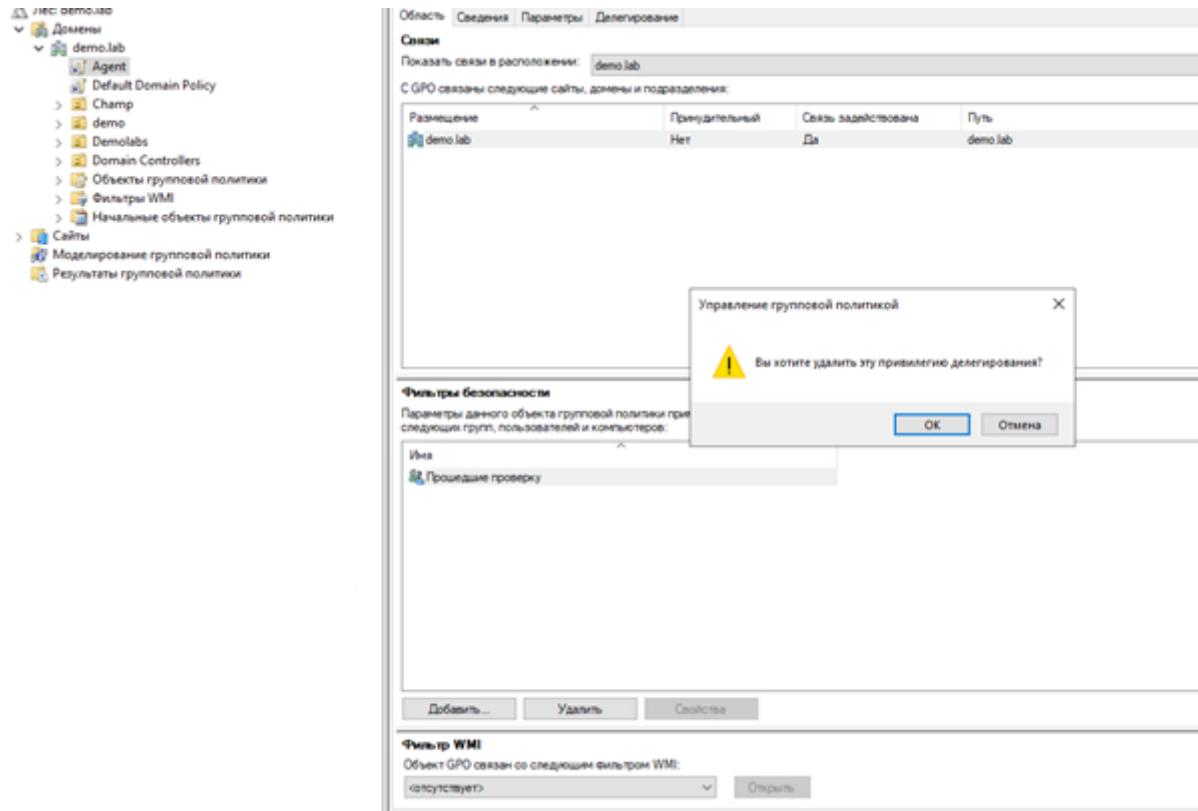
Далее запускаем созданную задачу (после завершения нужно перезагрузить ПК и проверить на клиенте агента)

## 2 агент

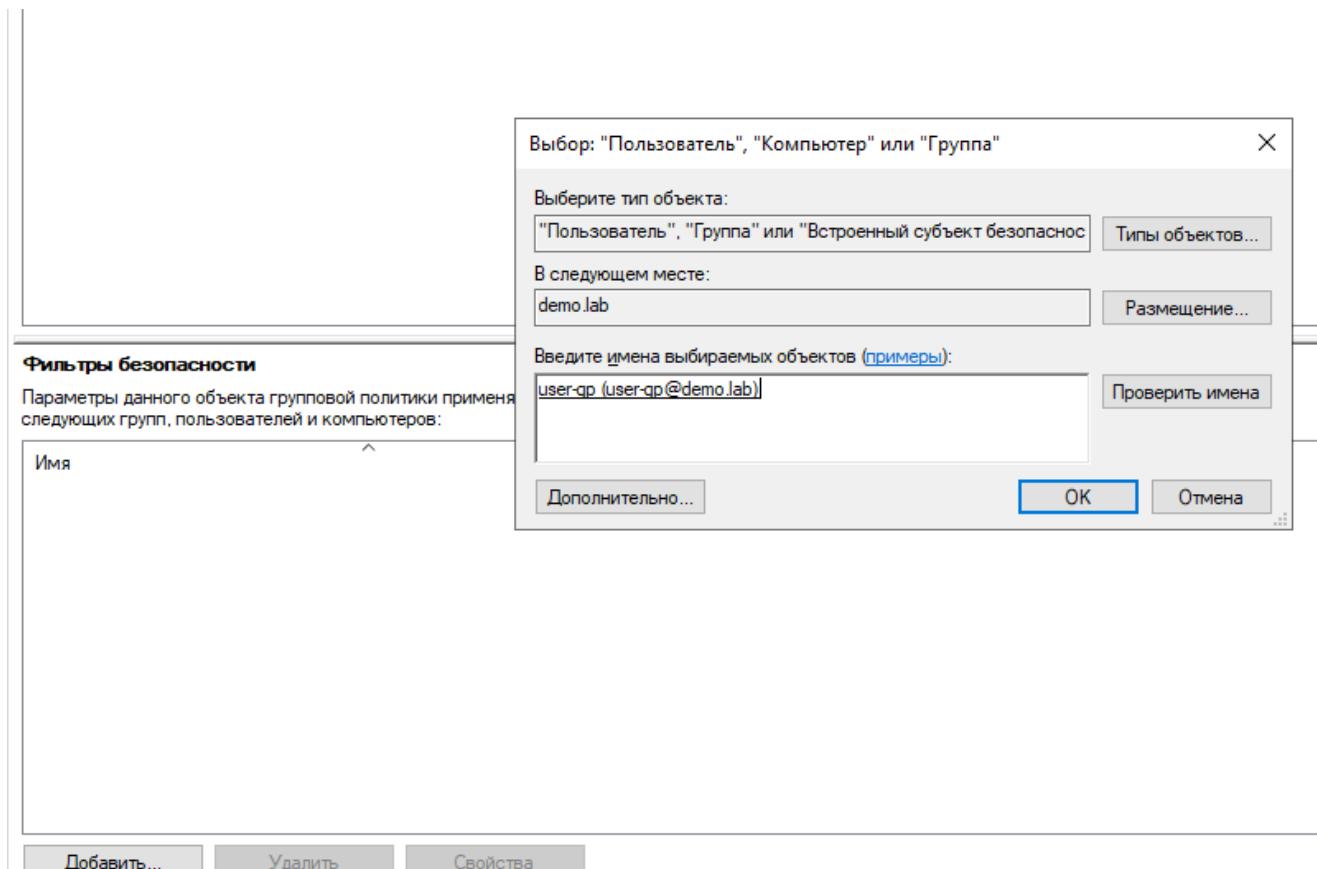




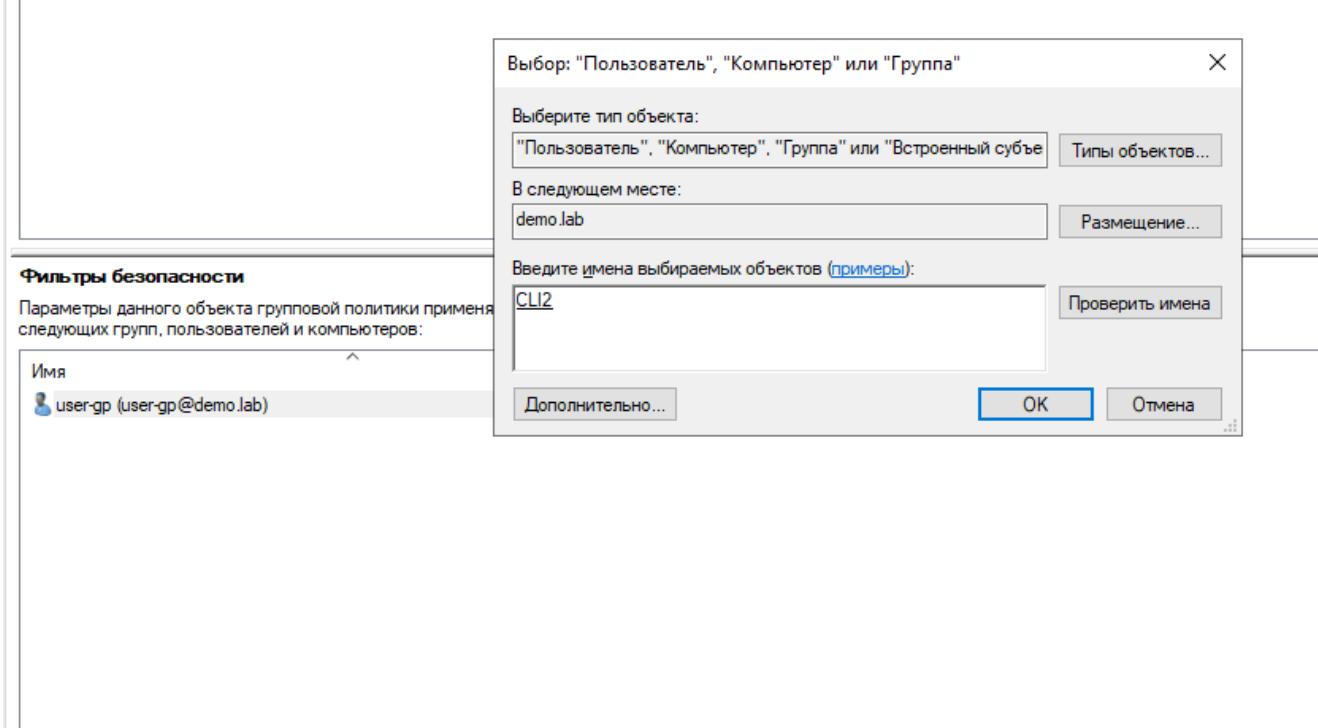
правой кнопкой на demo.lab и первый пункт



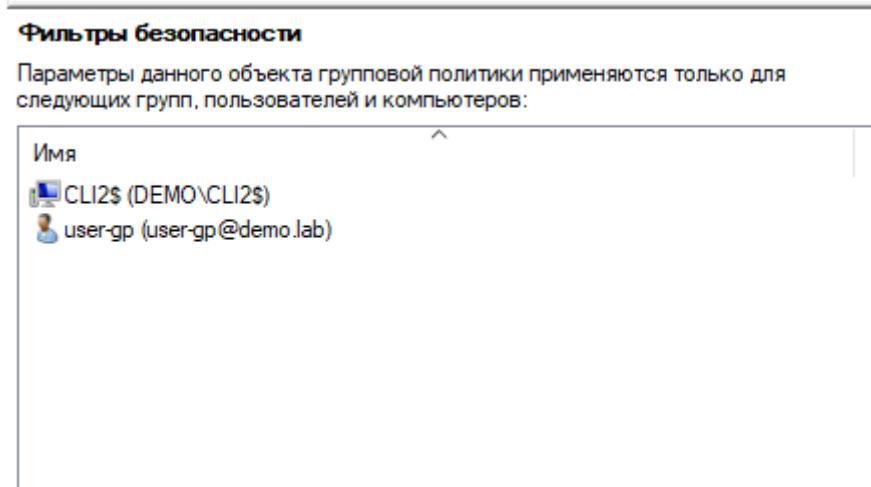
(Удалить – фильтр безопасности)



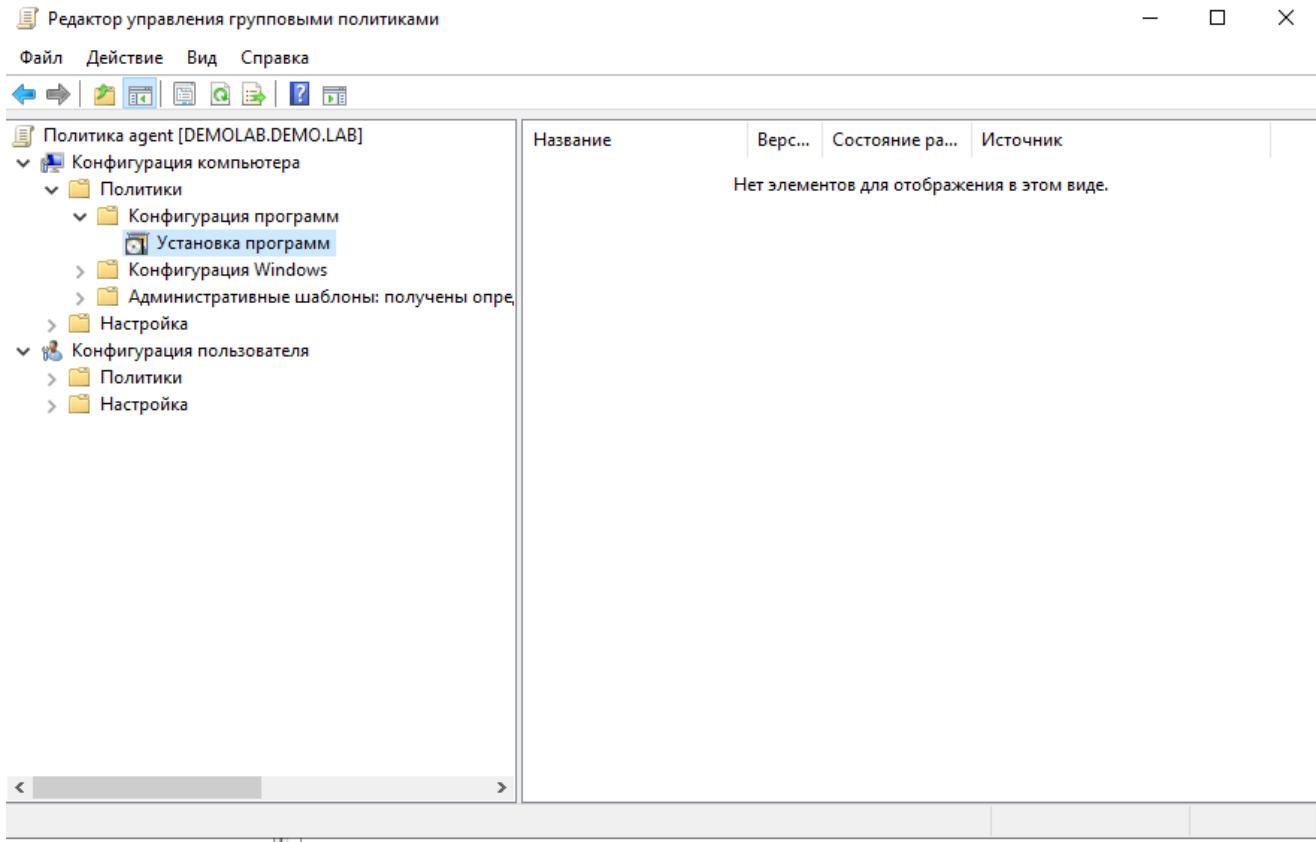
(добавить)



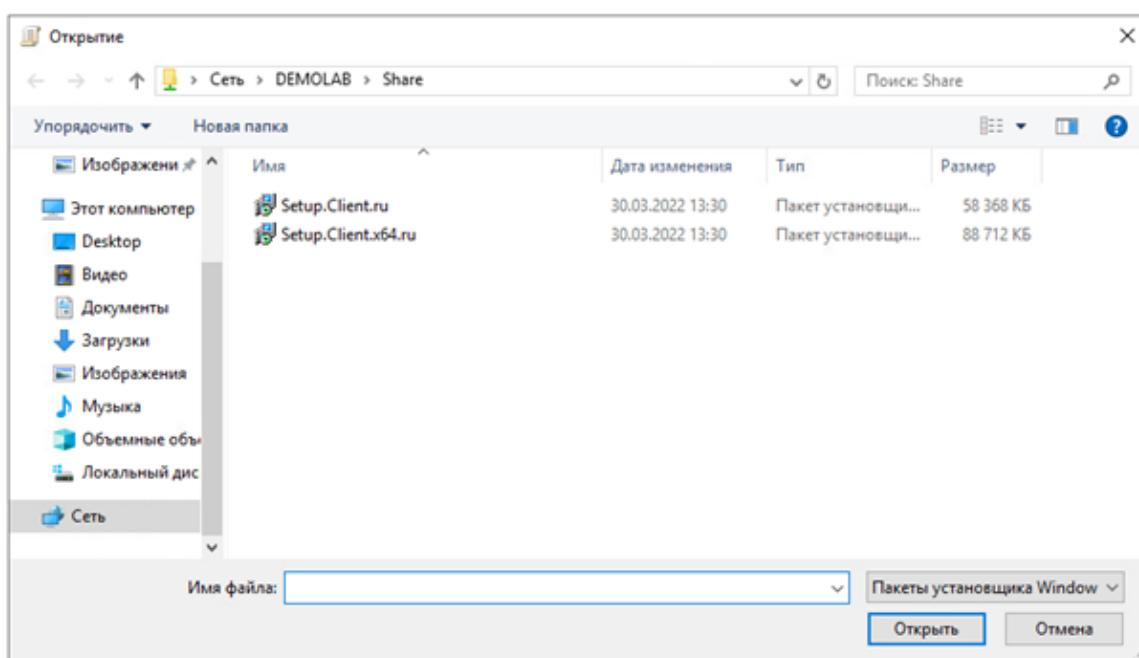
## Убедитесь, что в типах объекта добавлены компьютеры



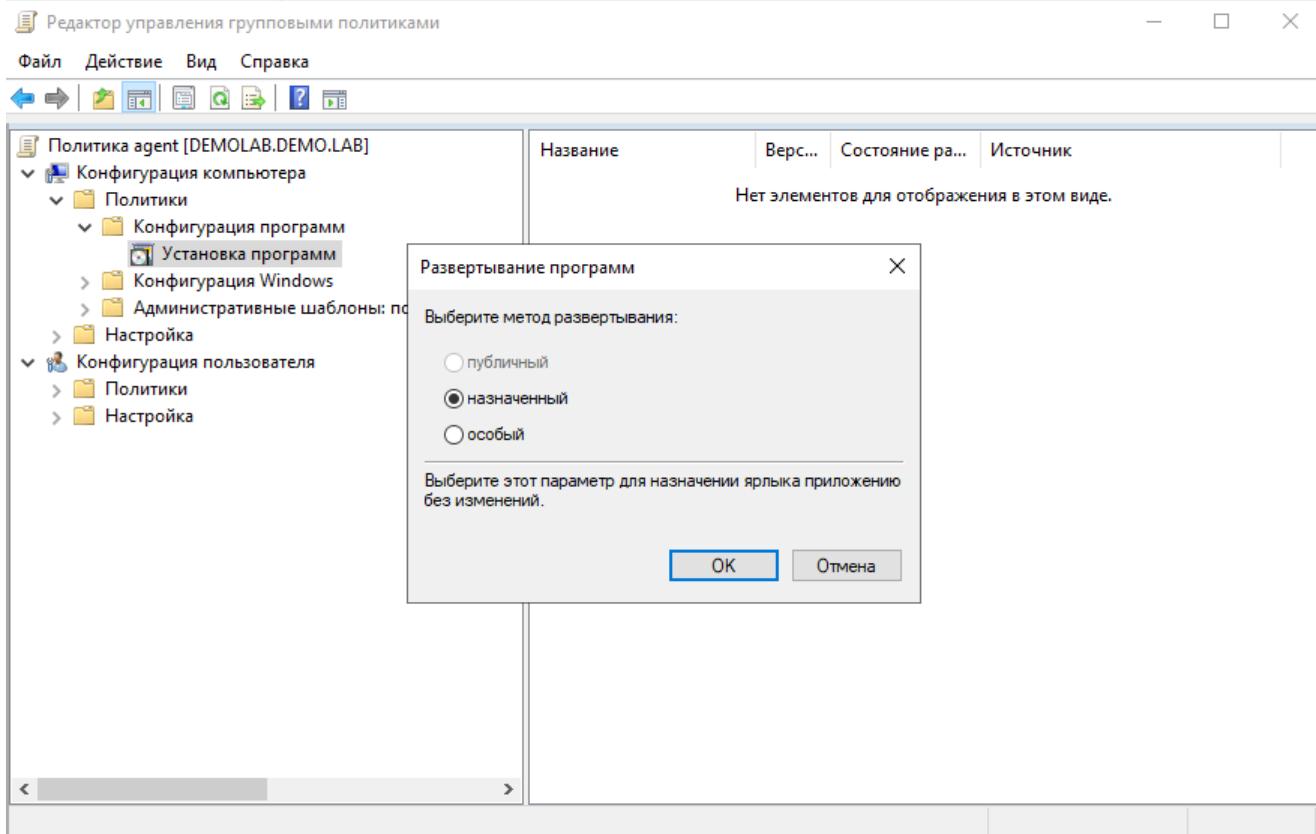
правой кнопкой на политику и изменить



Необходимо создать пакет (нажатие правой кнопки мыши)



Выбрать второй (x64)



**закрыть окно**

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 GPRERESULT /H GPREReport.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))у
```

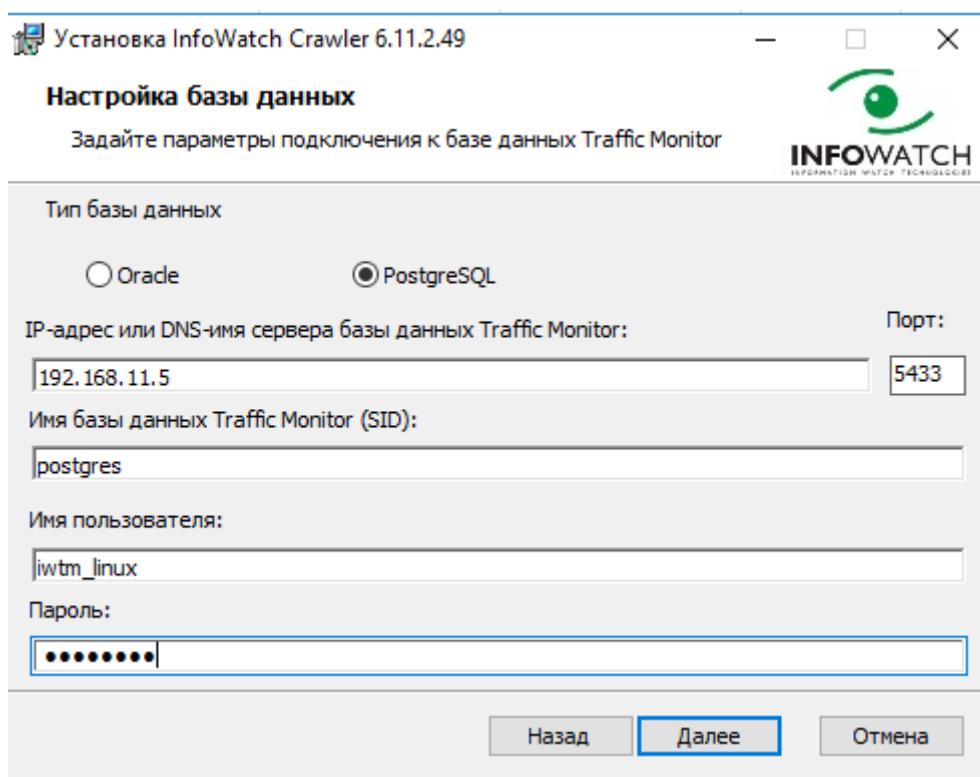
**gpupdate /force**

## Задание 5: Установка и настройка подсистемы сканирования сетевых ресурсов (Crawler)

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

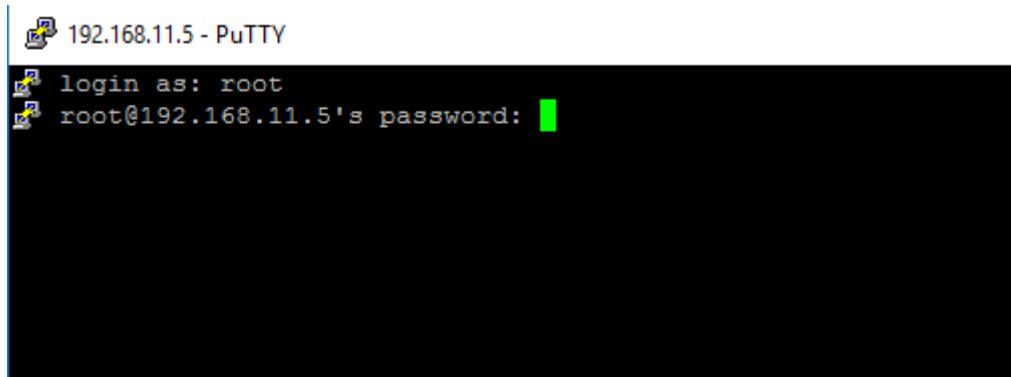
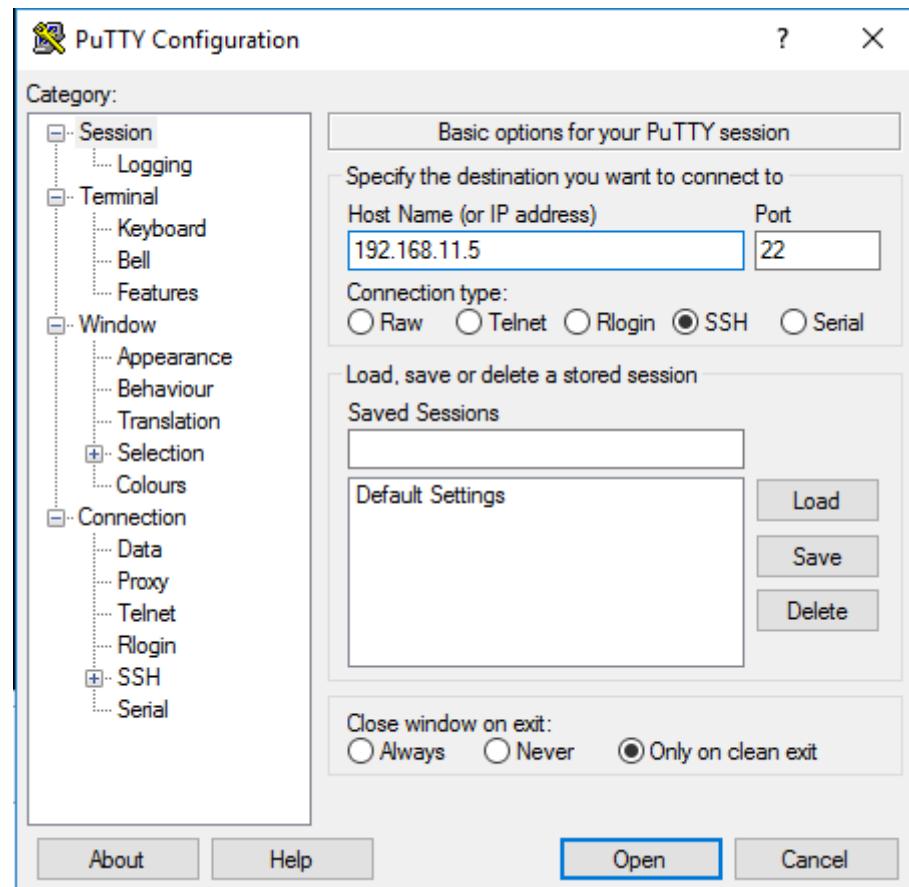
Необходимо создать общий каталог MainShare в корне диска сервера и установить права доступа на запись и чтение для всех пользователей домена.

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).

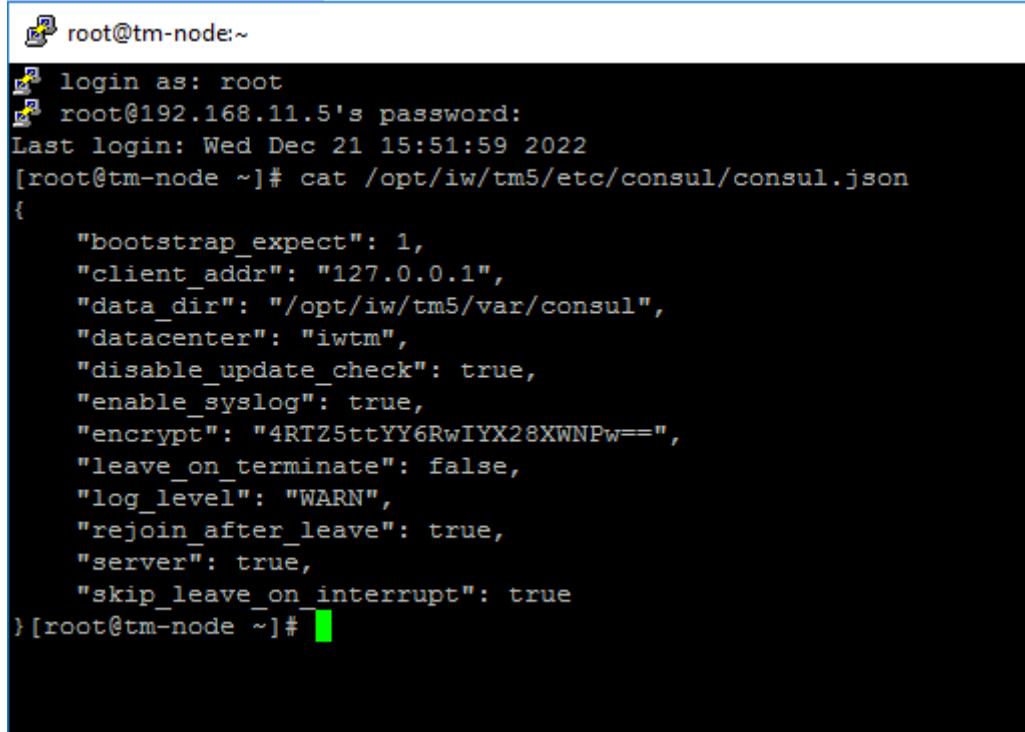


пароль xxXX1234

Далее с iwdm необходимо зайти в putty для получения информации о Consul



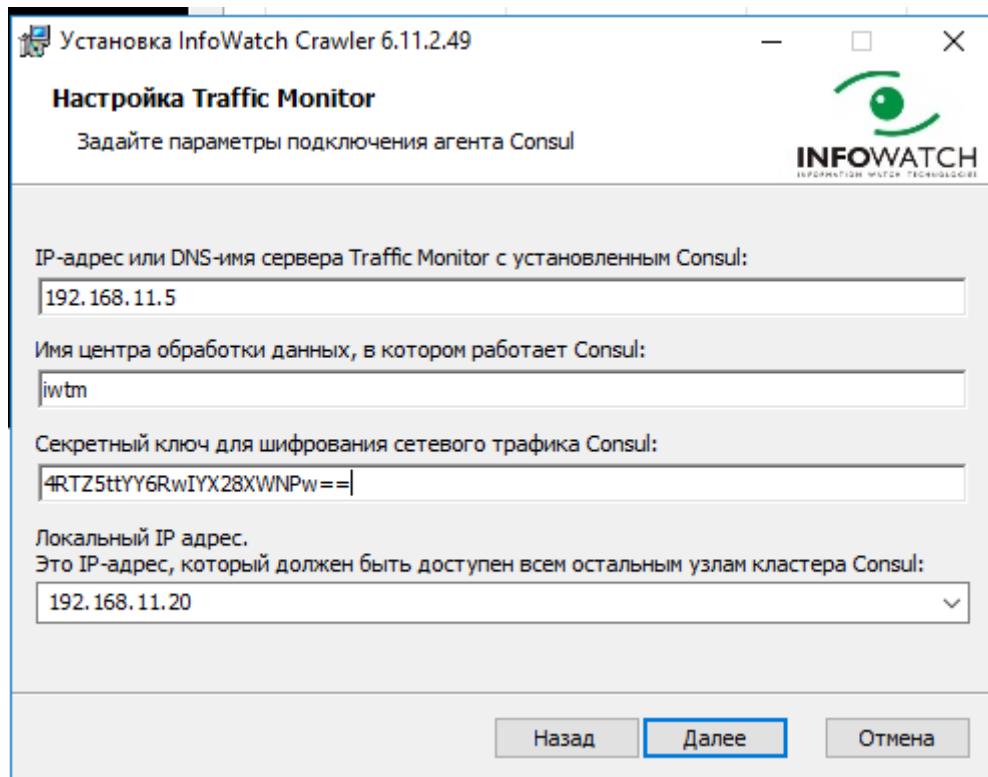
пароль xxXX1234



```

root@tm-node:~#
root@tm-node:~# login as: root
root@192.168.11.5's password:
Last login: Wed Dec 21 15:51:59 2022
[root@tm-node ~]# cat /opt/iw/tm5/etc/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@tm-node ~]#

```



Плагины

InfoWatch Crawler

InfoWatch Device Monitor

InfoWatch Sample documents Autoupda...

InfoWatch Crawler

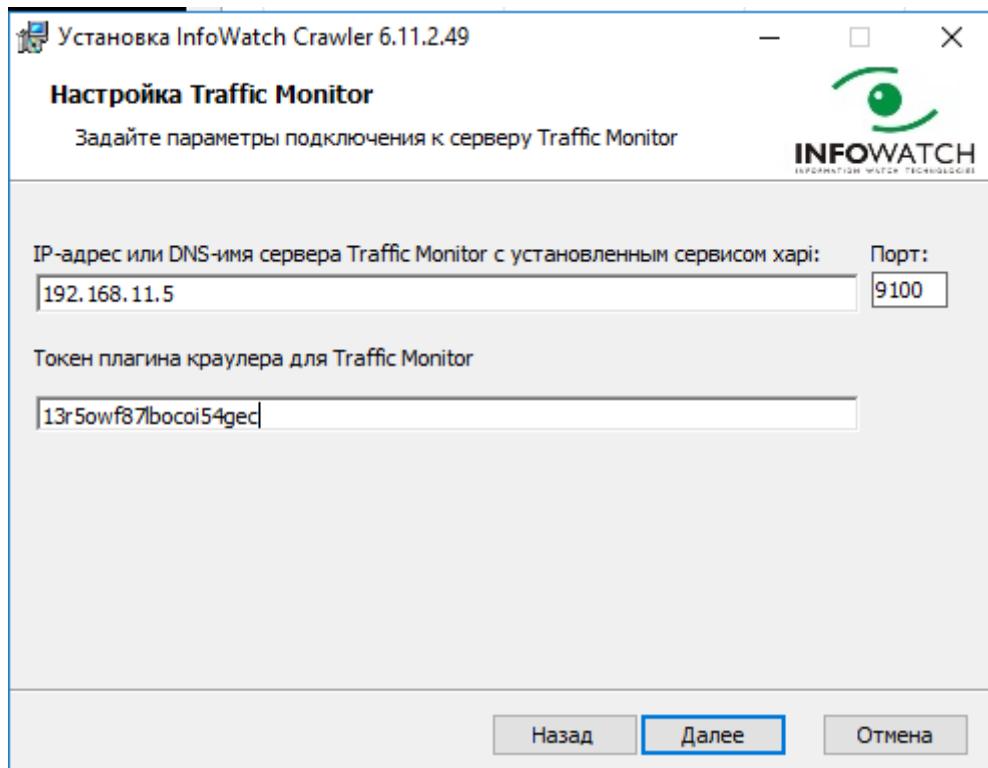
Прием событий Краулер  
Производитель: IW  
Версия 6.11.5

Плагины   Лицензии   Токены

+   -   X   edit

Статус	Имя	Содержание
Активный	Token-2	1aq4dn5nw7ltz1nrwfxm

управление → плагины



далъше все оставляем по умолчанию

Имя	Дата измене
Logs	12.09.2016 15
PerfLogs	16.07.2016 16
Program Files	01.03.2023 8:1
Program Files (x86)	01.03.2023 8:1
Windows	20.12.2022 12
Пользователи	28.02.2023 18
MainShare	01.03.2023 9:2

правой кнопкой на папку → свойства → доступ → общий доступ

выбрать «все» и добавить

Имя	Уровень разрешений
iwdm-adm	Владелец
Все	Чтение и запись

[Проблемы при предоставлении общего доступа](#)

Поделиться    Отмена

разрешение по заданию

## вкладка краулера

**Создание задачи**

**Объект сканирования**

- Цель сканирования: Разделяемые сетевые ресурсы
- Сканируемые группы и компьютеры: DM
- Режим сканирования: Только папки
- Фильтр: MainShare\*
- Исключая системные папки

**Авторизация**

Авторизация сканера:

**Расписание:**

- Период сканирования: Ежедневно
- Начало действия: 01/03/2023
- Время: 0:00

**Искать файлы**

- Минимальный размер (КБ): 0
- Максимальный размер (КБ): 10000

**Сохранить** **Отменить**

в папке создать файлы и написать что-то в них

Имя	Дата изменения	Тип	Размер
Новый текстовый документ	01.03.2023 9:27	Текстовый докум...	1 КБ

## запустить сканирование

The screenshot shows the Krauler software interface. On the left, there's a sidebar with a toolbar and a list of 'Разделляемые сетевые ресурсы' (Shareable network resources). A message at the bottom says 'Новых файлов: 1'. On the right, there's a main window titled 'scan' with a table showing the status of a scan. The table has columns: Статус (Status), Дата запуска (Start date), Дата остановки (Stop date), Обработано к... (Processed by...), Не обработа... (Not processed by...), Всего файлов/размер (Total files/size), and Новых файлов/размер (New files/size). One row is shown with the following values: ✓, 1.03.2023, 9:28:17, 1.03.2023, 9:28:20, 1, 0, 1 / 0.00 MB, 1 / 0.00 MB.

Статус	Дата запуска	Дата остановки	Обработано к...	Не обработа...	Всего файлов/размер	Новых файлов/размер
✓	1.03.2023, 9:28:17	1.03.2023, 9:28:20	1	0	1 / 0.00 MB	1 / 0.00 MB

## 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 термин «Test exam» (в любом регистре), установить низкий уровень угрозы для всех событий, добавить тег «DE».

Для отработки правил через сервер агентского мониторинга необходимо создавать правила в отдельной политике «Модуль 1». После отработки политик необходимо оставить политику и открепить ее от групп компьютеров или выключить правила, но не удалять.

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 (суммарно 4 события: передачи, копирования, хранения и буфера обмена), настроив конструктор выборки вручную.

### Создать тег

Название DE

Цвет

Описание

**Сохранить** **Отменить**

## Списки → теги

Сводка События Отчеты Технологии Объекты защиты Персоны Политики Списки Управление Краулер

Конфигурация свободна и доступна для редактирования

Категории

+ / \ X ▾

Поиск по категориям

- Все элементы
  - Договоры и контракты
  - Конкурсная документация
  - Маркетинг
  - Отдел кадров
  - Система безопасности
  - Управление компаний
  - Финансы

Создать

Название категории Задание б. Проверка работоспособности системы

Параметры терминов, входящих в категорию

Вес 5 Язык Русский Учитывать морфологию  Учитывать регистр

Описание

Добавить описание

**Создать** **Отменить**

### Создание термина

Текст термина

Характеристический

Вес

Язык

Учитывать морфологию

Учитывать регистр

**Создать** **Отменить**

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

Конфигурация свободна и доступна для редактирования

Каталоги объектов защиты

Название: б. Проверка работоспособности системы

Статус

Описание

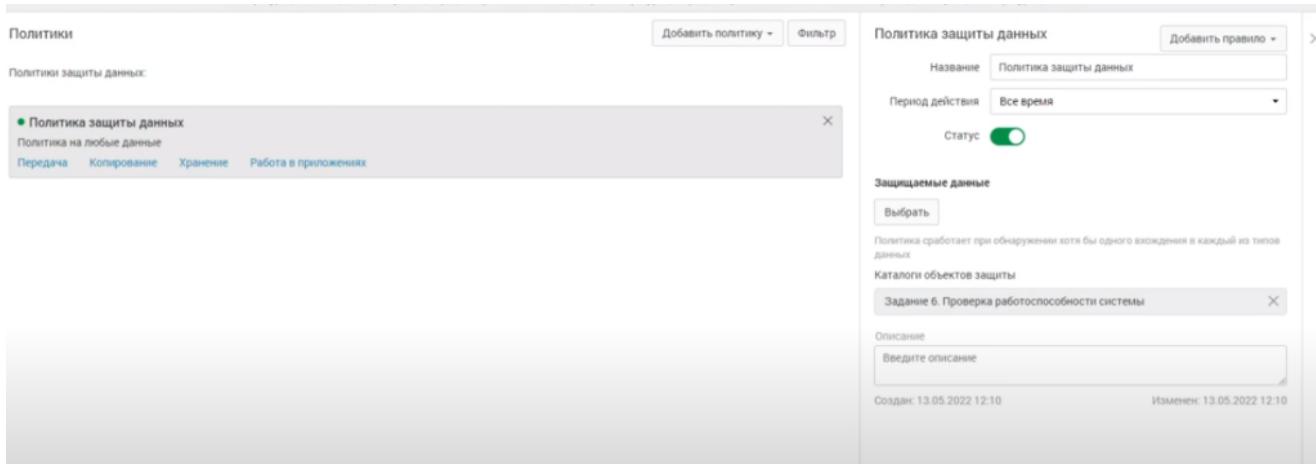
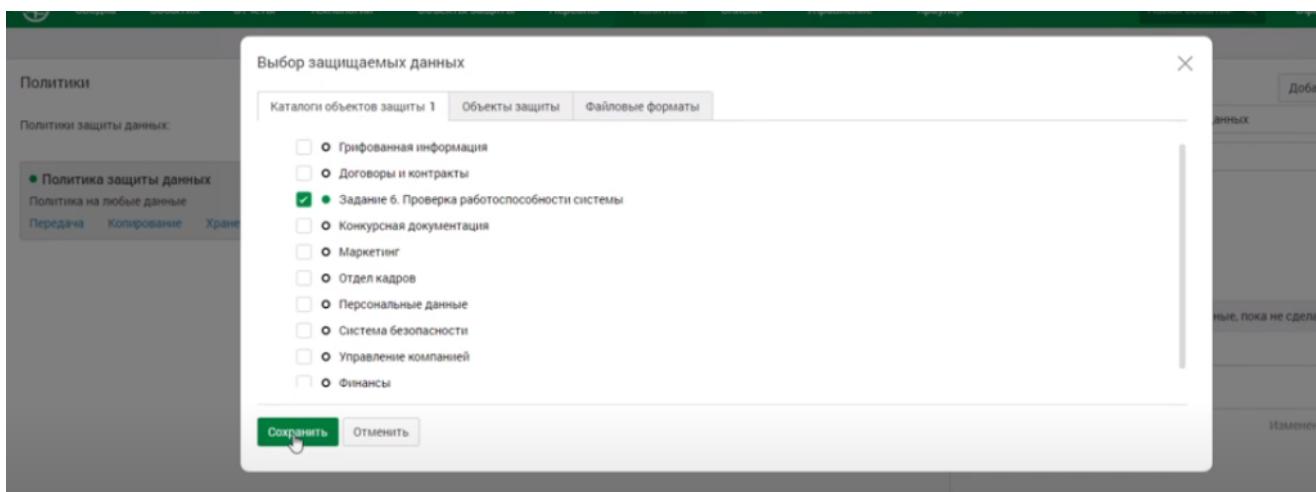
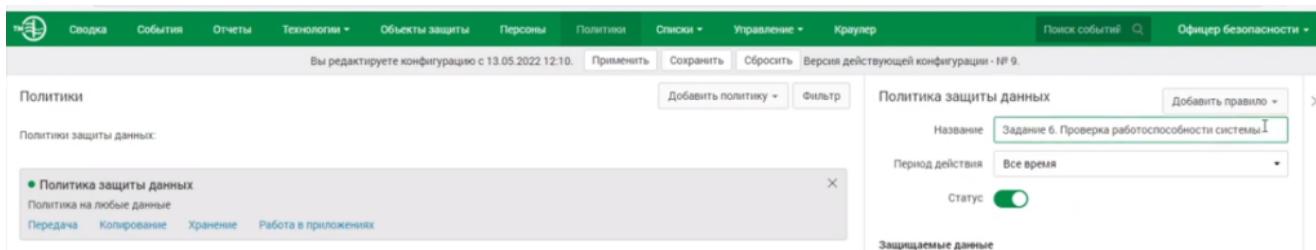
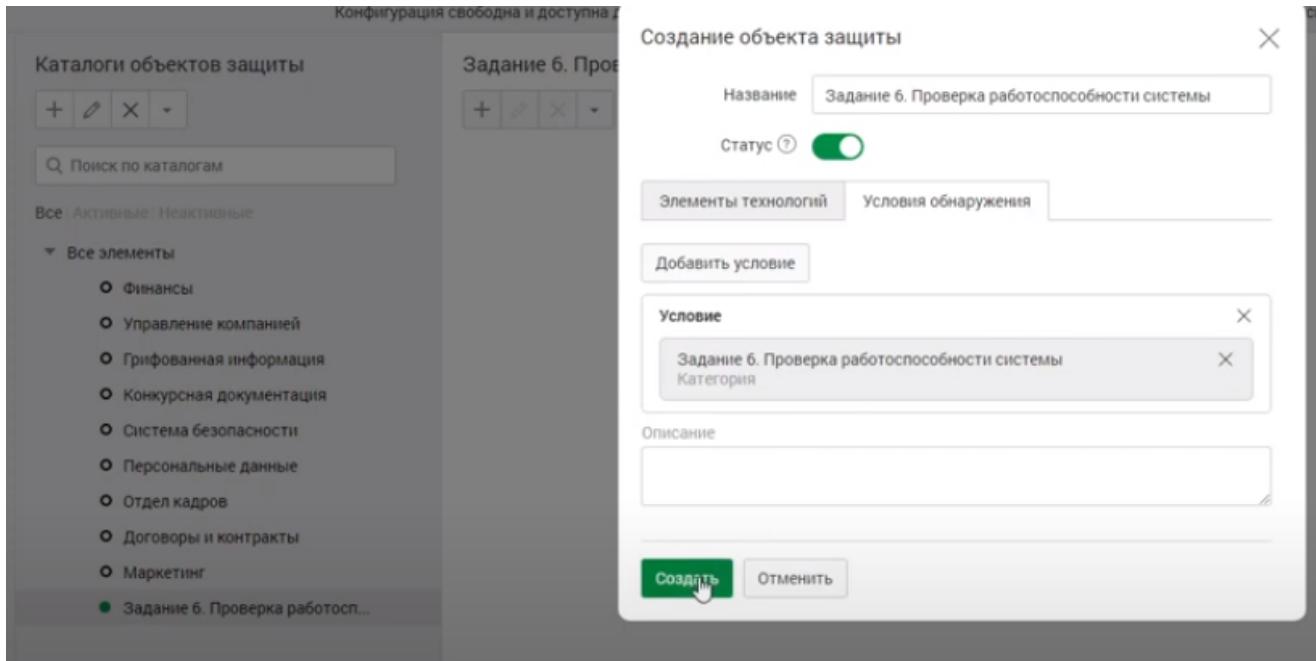
**Создать** **Отменить**

Создание объекта защиты

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

Договоры и контракты  
 Задание б. Проверка работоспособности системы  
 Конкурсная документация  
 Маркетинг  
 Отдел кадров  
 Информация по кадрам  
 Резюме  
 Система безопасности  
 Охрана организации  
 Информационная безопасность

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



## Политики

Политики защиты данных:

**● Политика защиты данных**  
Каталог объектов защиты: Задание 6: Проверка работоспособности системы  
Передача 1 Копирование Хранение Работа в приложениях

**Добавить правило**

Отправители Любой отправитель  
Направление маршрута ↓  
Получатели Любой получатель  
Действия

Действия по умолчанию не заданы

**● Договоры и контракты**  
Каталог объектов защиты: Договоры и контракты  
Передача 2 Копирование 1 Хранение Работа в приложениях

**● Отдел кадров**  
Каталог объектов защиты: Отдел кадров  
Передача 2 Копирование 1 Хранение Работа в приложениях

**● Маркетинг**  
Каталог объектов защиты: Маркетинг  
Передача 2 Копирование 1 Хранение Работа в приложениях

Добавить политику ▾ Фильтр

## Правило передачи

Направление маршрута → В одну сторону ⇔ В оба направления

Тип события Тип

Компьютеры Начните вводить текст +

Отправители = Начните вводить текст +

Получатели = Начните вводить текст +

Дни действия правила Любой день недели

Часы действия правила 0:00 - 0:00

## Действия при срабатывании правила

Отправить почтовое(?) уведомление Начните вводить текст +

Назначить событию вердикт Разрешить

Назначить событию уровень нарушения Низкий

Назначить событию теги DE

Назначить отправителю статус Выберите статус

Удалить событие

Сохранить Отменить

## Политики

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

Действия по умолчанию не заданы

**● Договоры и контракты**  
Каталог объектов защиты: Договоры и контракты  
Передача 2 Копирование 1 Хранение Работа в приложениях

**● Отдел кадров**  
Каталог объектов защиты: Отдел кадров  
Передача 2 Копирование 1 Хранение Работа в приложениях

**● Маркетинг**  
Каталог объектов защиты: Маркетинг  
Передача 2 Копирование 1 Хранение Работа в приложениях

Добавить политику ▾ Фильтр

## Правило копирования

Направление маршрута → В одну сторону ⇔ В оба направления

Тип события Тип

Компьютеры Начните вводить текст +

Отправители = Начните вводить текст +

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

Отправить почтовое(?) уведомление Начните вводить текст +

Назначить событию вердикт Разрешить

Назначить событию уровень нарушения Низкий

Назначить событию теги DE

Назначить отправителю статус Выберите статус

Сохранить Отменить

## Политики

Политики защиты данных:

**● Политика защиты данных**  
Каталог объектов защиты: Задание 6: Проверка работоспособности системы  
Передача 1 Копирование 1 Хранение 1 Работа в приложениях

**Добавить правило**

Место хранения Любой место хранения  
Владельцы файла Любой владелец  
Кому доступен файл Доступно всем  
Действия

Действия по умолчанию не заданы

**● Договоры и контракты**  
Каталог объектов защиты: Договоры и контракты  
Передача 2 Копирование 1 Хранение Работа в приложениях

**● Отдел кадров**  
Каталог объектов защиты: Отдел кадров  
Передача 2 Копирование 1 Хранение Работа в приложениях

**● Маркетинг**  
Каталог объектов защиты: Маркетинг  
Передача 2 Копирование 1 Хранение Работа в приложениях

Добавить политику ▾ Фильтр

## Правило хранения

Тип события Тип

Место хранения Начните вводить текст +

Владельцы файла = Начните вводить текст +

Кому доступен файл = Начните вводить текст +

## Действия при срабатывании правила

Отправить почтовое(?) уведомление Начните вводить текст +

Назначить событию вердикт Разрешить

Назначить событию уровень нарушения Низкий

Назначить событию теги DE

Назначить отправителю статус Выберите статус

Удалить событие

Сохранить Отменить

Политики

Политики защиты данных:

**• Политика защиты данных**

Каталог объектов защиты: Задание 6: Проверка работоспособности системы

Передача 1 Копирование 1 Хранение 1 Работа в приложениях

Добавить правило

Тип события: Буфер обмена  
 Приложение-источник: Любое приложение  
 Приложение-приемник: Любое приложение  
 Действия: не заданы

Действия по умолчанию:

**• Договоры и контракты**

Каталог объектов защиты: Договоры и контракты

Передача 2 Копирование 1 Хранение Работа в приложениях

**• Отдел кадров**

Каталог объектов защиты: Отдел кадров

Передача 2 Копирование 1 Хранение Работа в приложениях

**• Маркетинг**

Каталог объектов защиты: Маркетинг

Передача 2 Копирование 1 Хранение Работа в приложениях

Добавить политику

Фильтр

Правило работы в приложениях

Компьютеры: Начните вводить текст  
 Приложения: Начните вводить текст  
 Только для терминальной сессии: вкл.  
 Приложение-источник: Начните вводить текст  
 Приложение-приемник: Начните вводить текст  
 Дни действия правила: Любой день недели  
 Часы действия правила: 0:00 - 0:00

Действия при срабатывании правила

Отправить почтовое уведомление: Начните вводить текст  
 Назначить событию вердикт: Разрешить  
 Назначить событию уровень нарушения: Низкий  
 Назначить событию теги: DE | Выберите статус

Сохранить

Отменить

## Модуль 2

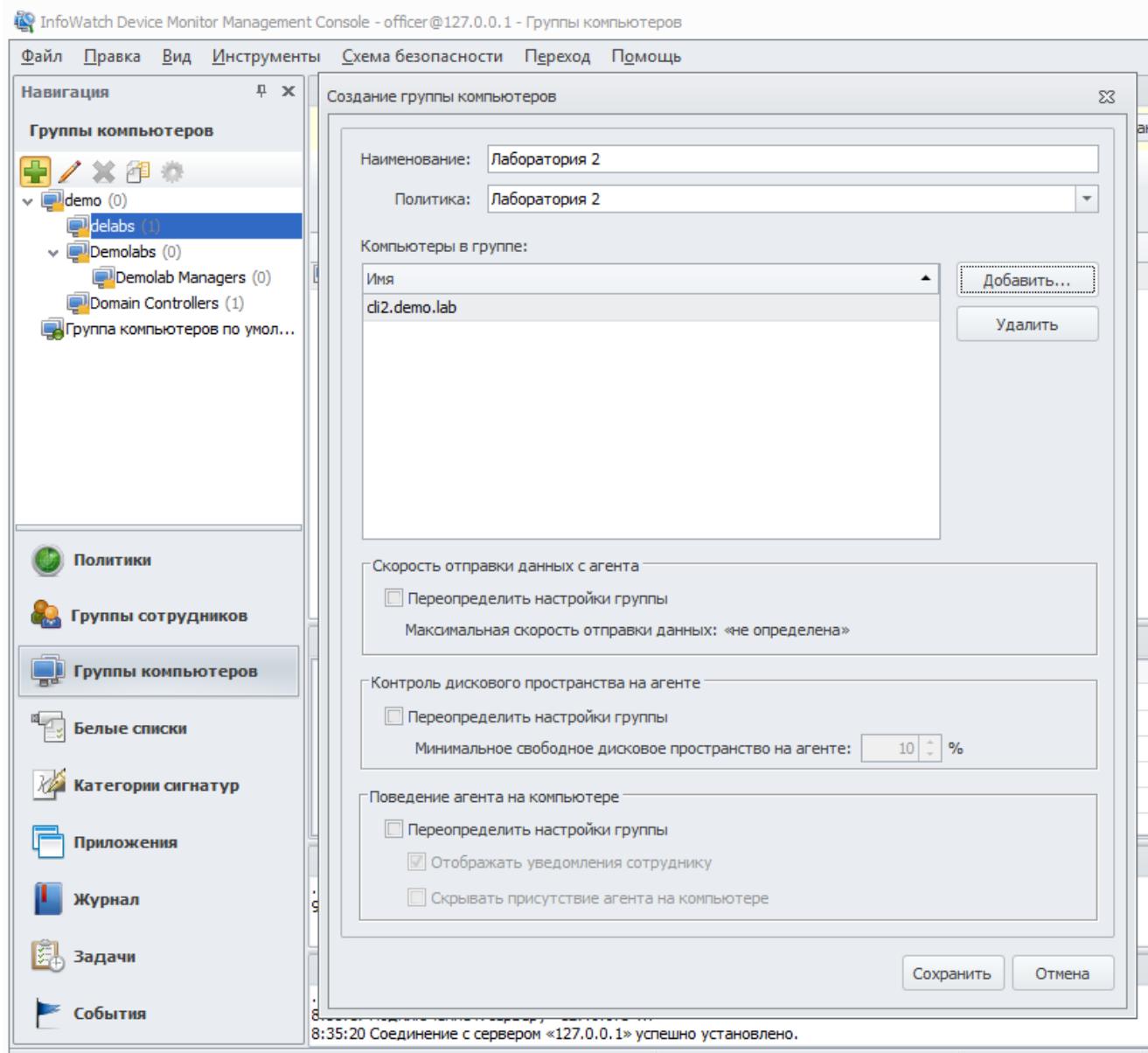
**Задание 1** Необходимо создать 2 новых группы компьютеров: «Лаборатория 1» и «Лаборатория 2», а также создать 2 новых политики: «Лаборатория 1» и «Лаборатория 2». Каждая из политик должна применяться только на соответствующие группы. Компьютер 1 (user-wind) необходимо перенести в Лаборатория 1, а компьютер 2 (user-gp) – в Лаборатория 2. Зафиксировать выполнение скриншотом.

The screenshot shows the InfoWatch Device Monitor Management Console interface. The main window title is "InfoWatch Device Monitor Management Console - officer@127.0.0.1 - Политики". The menu bar includes "Файл", "Правка", "Вид", "Инструменты", "Схема безопасности", "Переход", and "Помощь". The left sidebar has a "Навигация" section with icons for "Политики", "Группы сотрудников", "Группы компьютеров", "Белые списки", "Категории", "Приложения", "Журнал", "Задачи", and "События". The "Политики" section is selected and shows a list with a green plus sign icon, a pencil icon, and a red X icon. Below it are two items: "Политика на устройство" and "Политика теневого". A central panel titled "Правила" contains a message: "Поместите сюда заголовок колонки для группировки по этой колонке". A modal dialog titled "Создание политики" is open, prompting the user to "Создайте новое правило для политики или выберите из других правил в системе:". It has columns for "Наименование", "Операция", and "Период действия". On the right of the dialog are buttons for "Создать...", "Изменить...", and "Удалить". At the bottom are buttons for "Сохранить" and "Отмена". The status bar at the bottom shows "Схема безопасности: 1 (Изменения в связи с автоматической синхронизацией) || Схема безопасности в режиме «только чтение»".

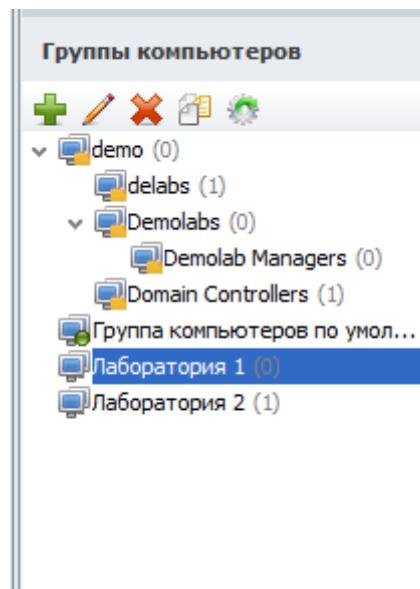
Политики. создаем две

The screenshot shows the "Политики" section of the navigation pane. It lists two policies: "Лаборатория 1 (0)" and "Лаборатория 2 (0)". Each item has a green plus sign icon, a pencil icon, and a red X icon.

Переходим во вкладку «группы компьютеров»

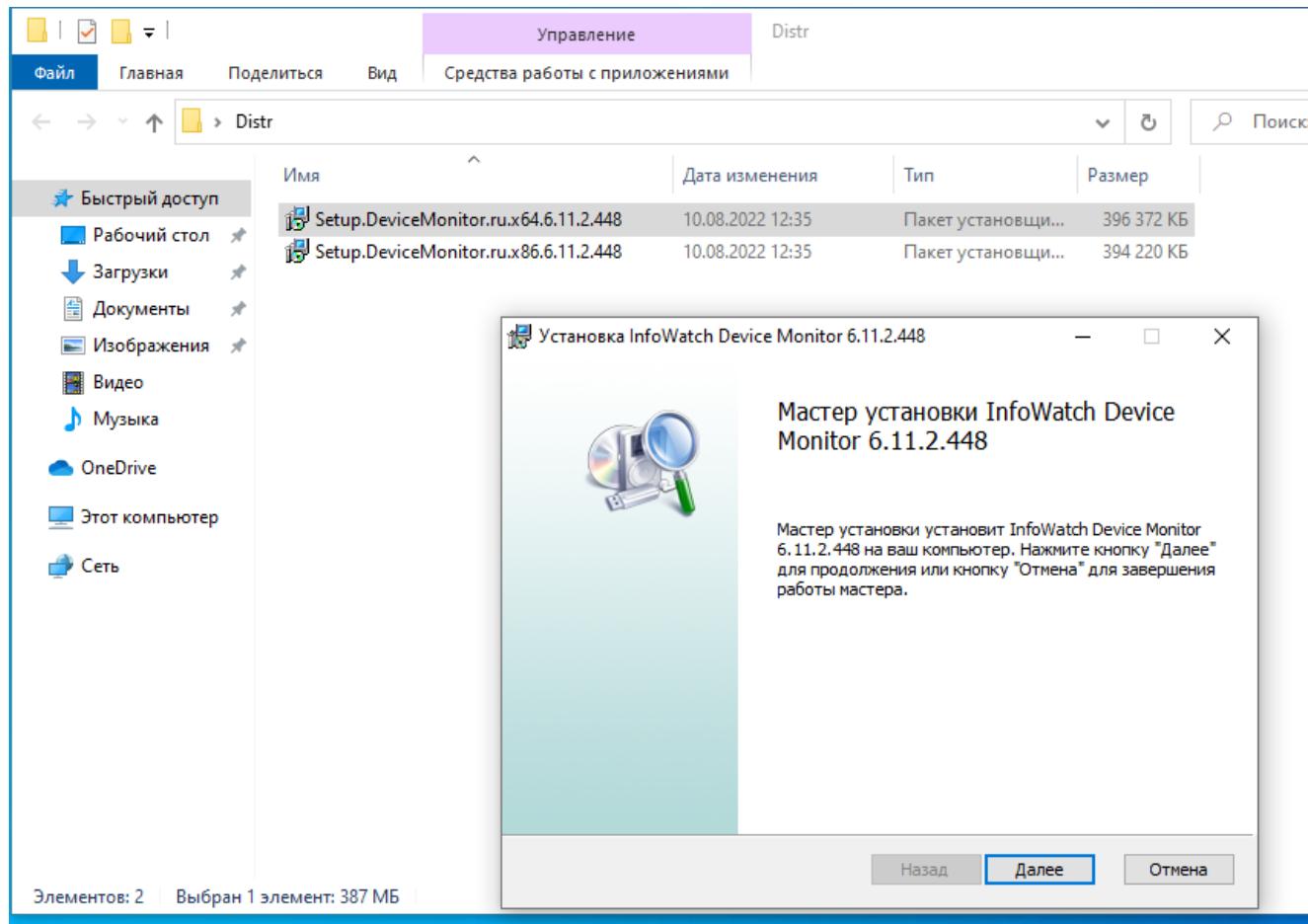


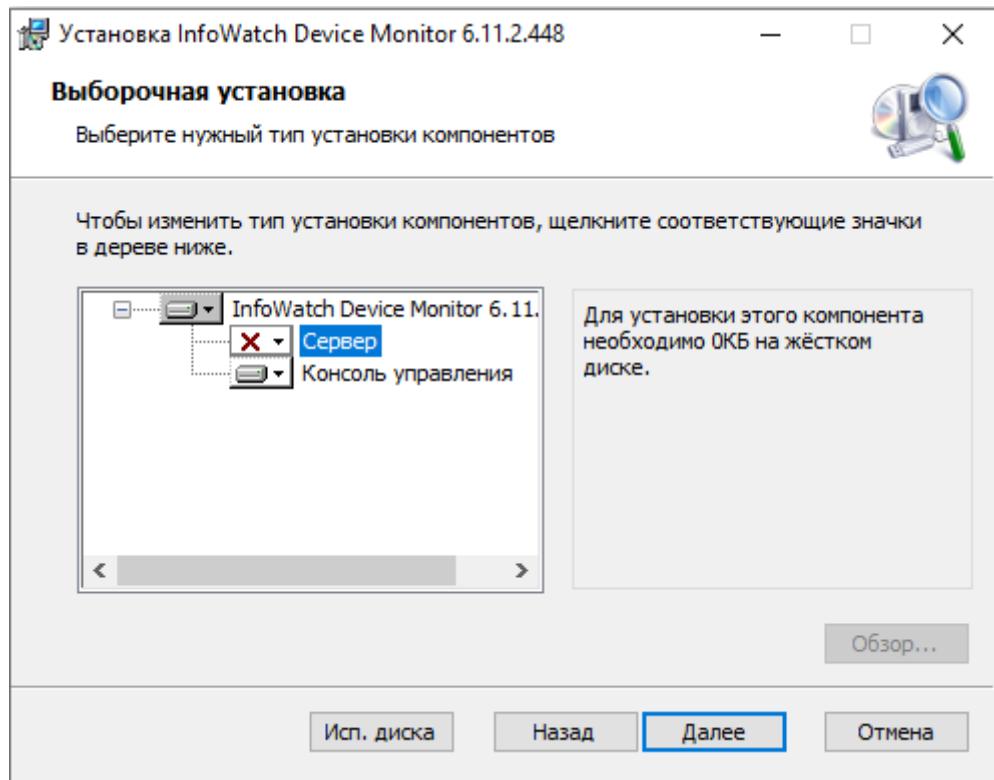
создаем лаб 1 и 2, ставим политики и добавляем компьютеры. клиент 1 в лаб 1  
клиент 2 в лаб2



Задание 2 Для удобства работы офицера безопасности необходимо установить дополнительную консоль управления сервером агентского мониторинга на любую машину нарушителя

на клиенте запустить установку





через командную строчку узнать ip компьютера dm

```
Командная строка
Microsoft Windows [Version 10.0.14393]
(c) Корпорация Майкрософт (Microsoft Corporation), 2016. Все права защищены.

C:\Users\iwdm-adm>ipconfig

Настройка протокола IP для Windows

Адаптер Ethernet Ethernet0:

    DNS-суффикс подключения . . . . . :
    IPv4-адрес . . . . . : 192.168.11.20
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . : 192.168.11.2

Туннельный адаптер Teredo Tunneling Pseudo-Interface:

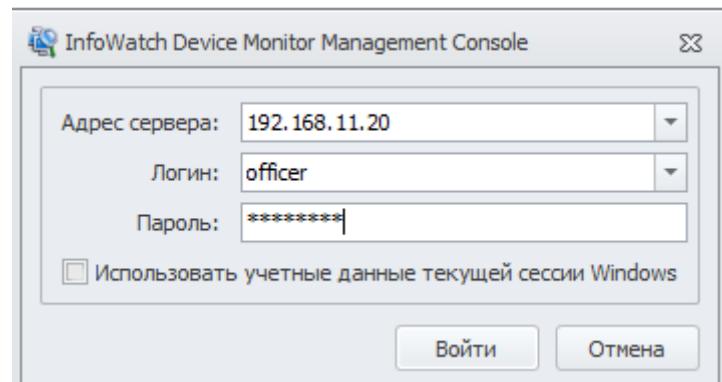
    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :

Туннельный адаптер isatap.{A8A274AD-6672-4373-8464-7801CE281987}:

    Состояние среды. . . . . : Среда передачи недоступна.
    DNS-суффикс подключения . . . . . :

C:\Users\iwdm-adm>
```

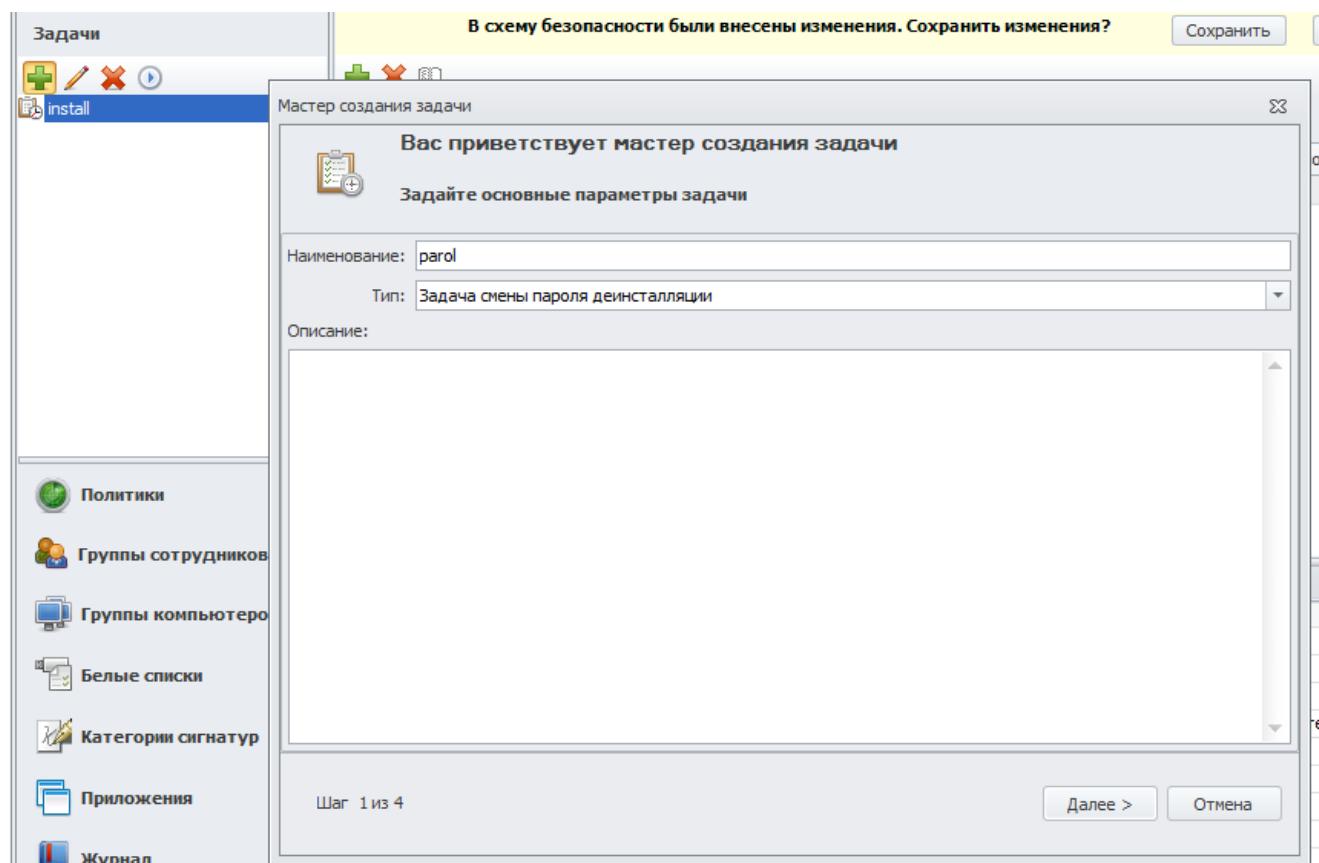
после этого заходим в консоль на машине клиента

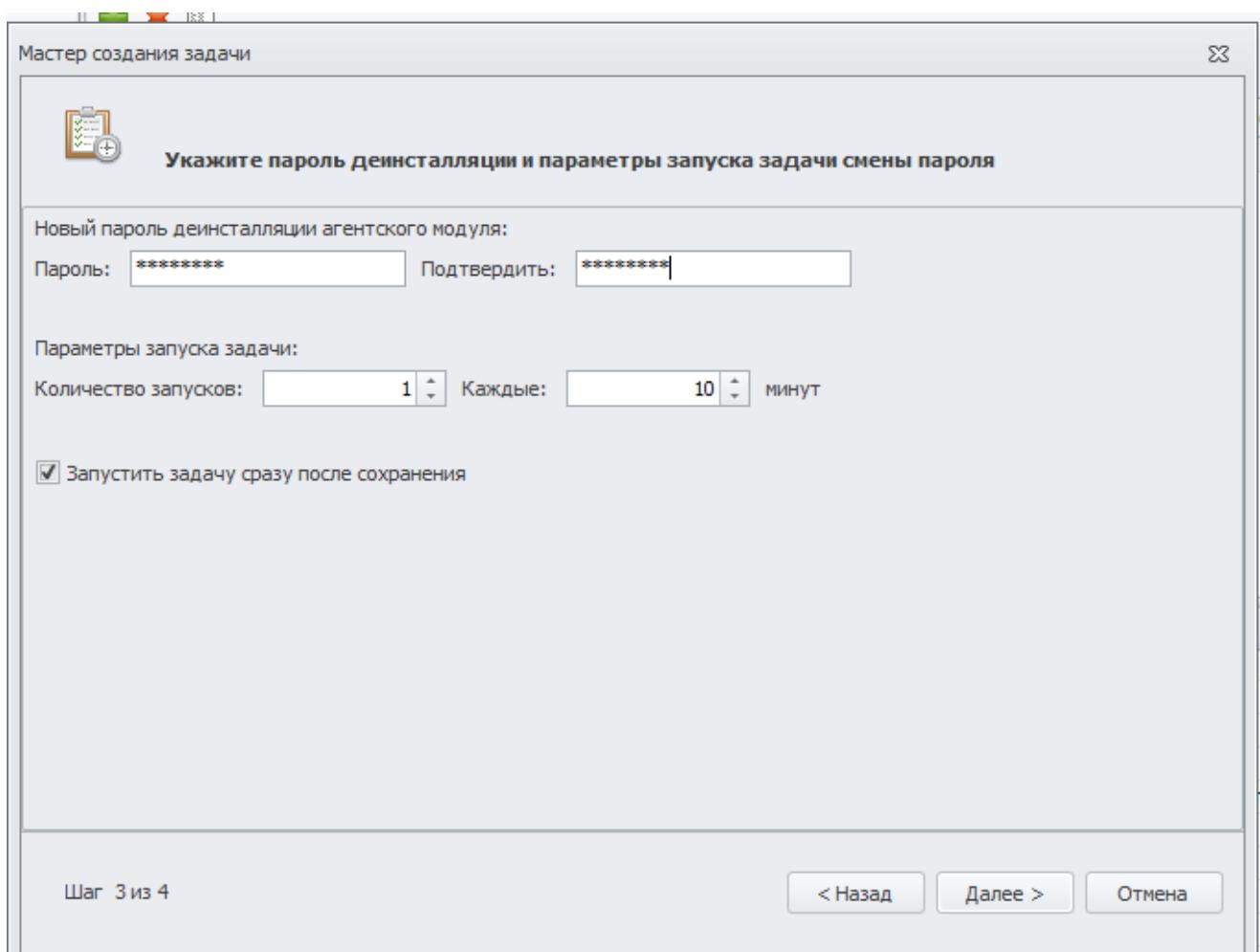
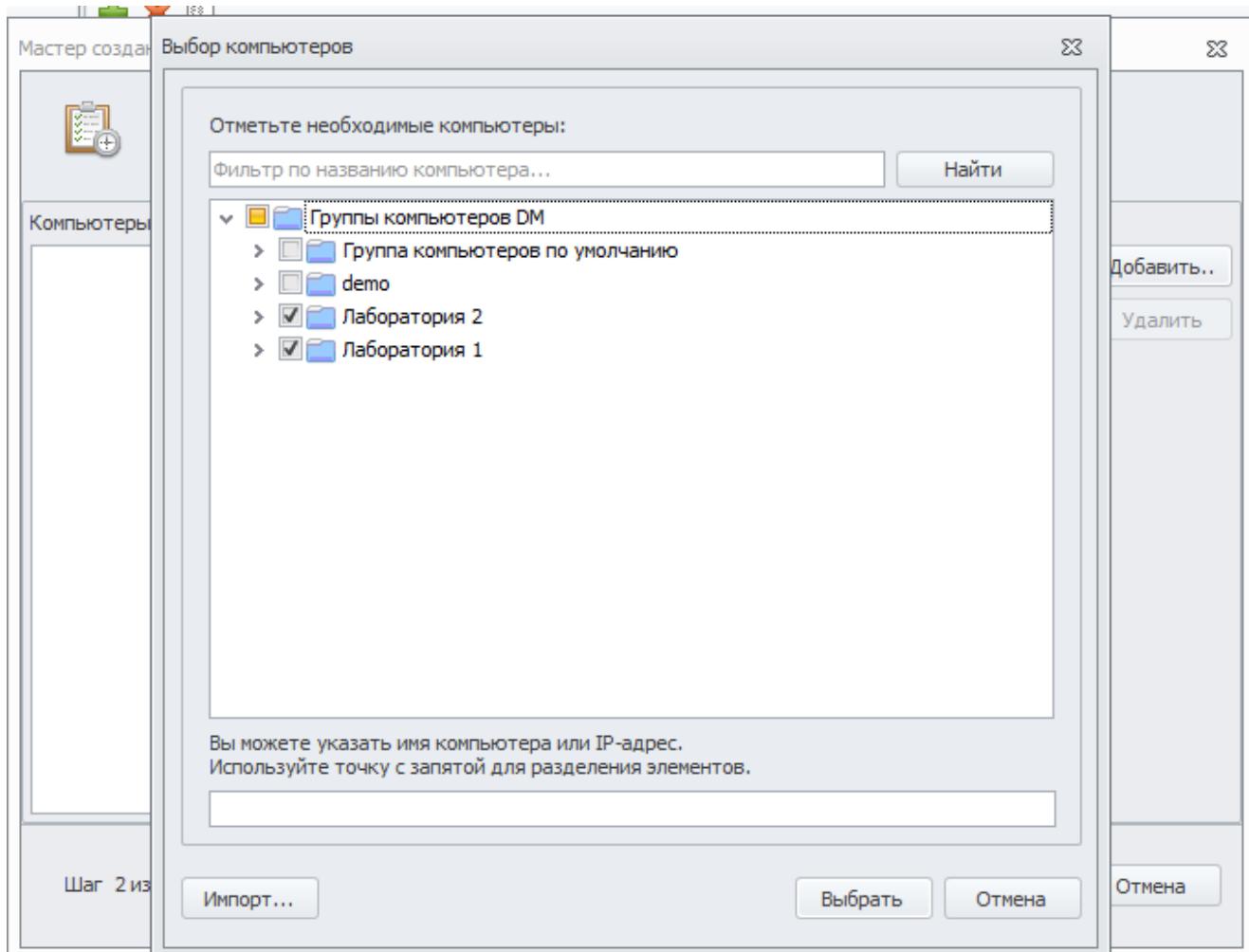


### Задание 3

Необходимо установить (сменить) пароль для удаления агента мониторинга на всех машинах нарушителей с помощью средств сервера агентского мониторинга (удаленно). Пароль: xxXX5566

заходим в задачи и создаем новую



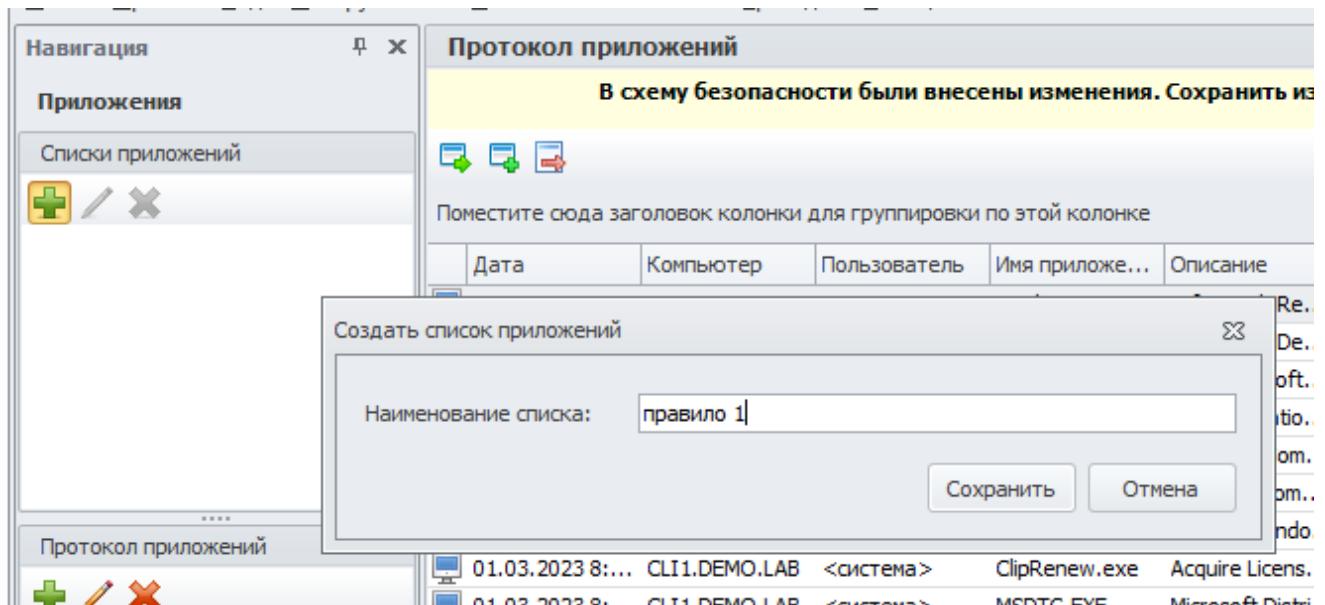


## Правило 1

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

Проверить работоспособность и зафиксировать выполнение скриншотом.

Создание списков приложений. На каждое правило отдельный список желательно.



просто запустить и закрыть приложение на клиенте, потом обновить протокол приложений f5, найти его в списке и перетащить в тот список который был создан

Наименование: Правило 1

Перехватчик: Application Monitor

Правило применяется на ОС: Windows

**Запрет запуска приложений**

Запретить запуск приложений с использованием списков

Белые списки (неактивны)

Запрет всех приложений, кроме указанных в списке

Черные списки (активны) Правило 1

Блокируются приложения из списка

Смена режима белые/черные списки [здесь](#)

**Запрет буфера обмена**

В терминальной сессии между различными рабочими станциями (для любых приложений)

В приложениях из списка

**Запрет печати**

В приложениях из списка

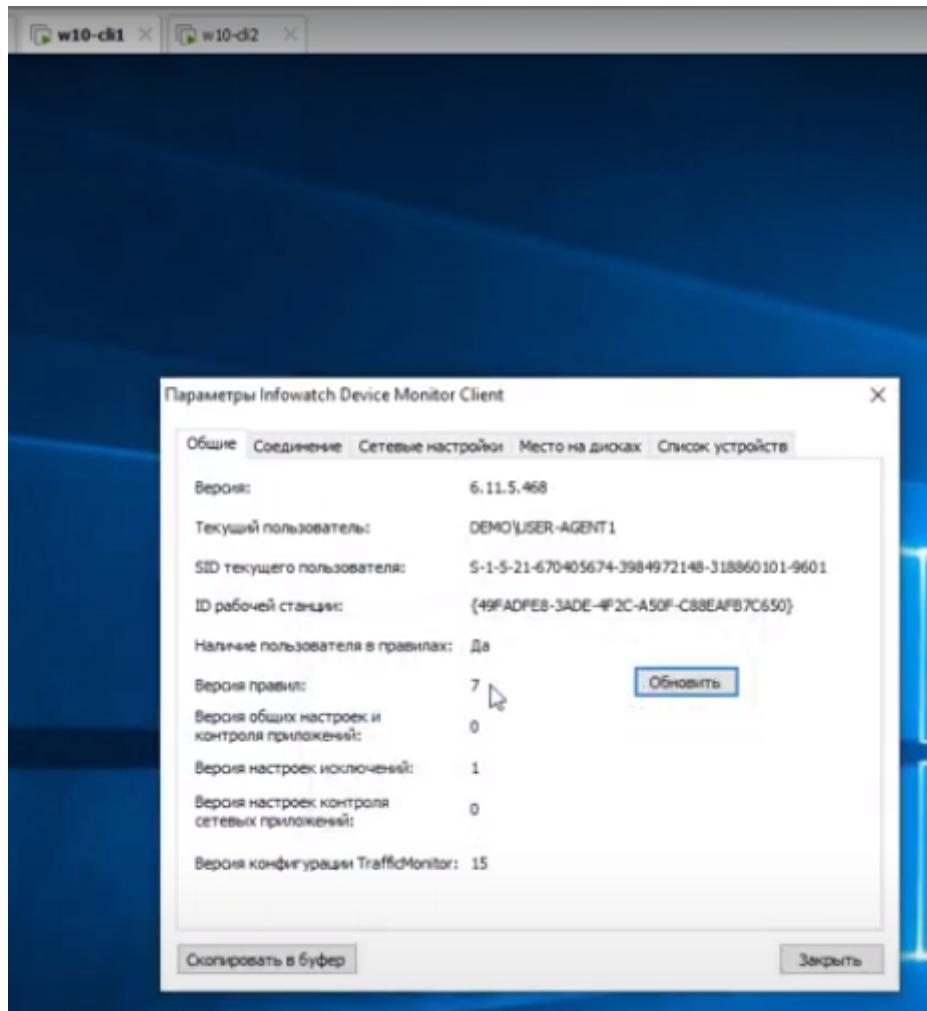
Тип принтера

Локальный

Сетевой

Терминальный

Сделать такой скрин

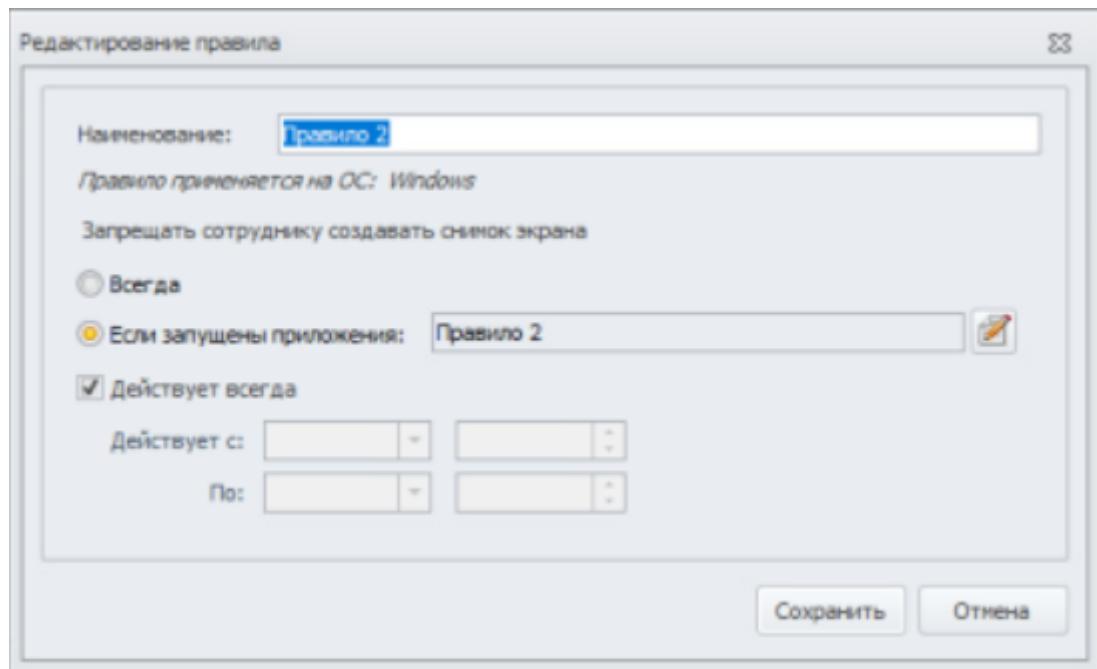


Проверка правила – обновить и попробовать запустить paint, после каждого правила обновлять

## 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 и табличный процессор – перед этим нужно запустить это приложения найдя его в поисковике windows

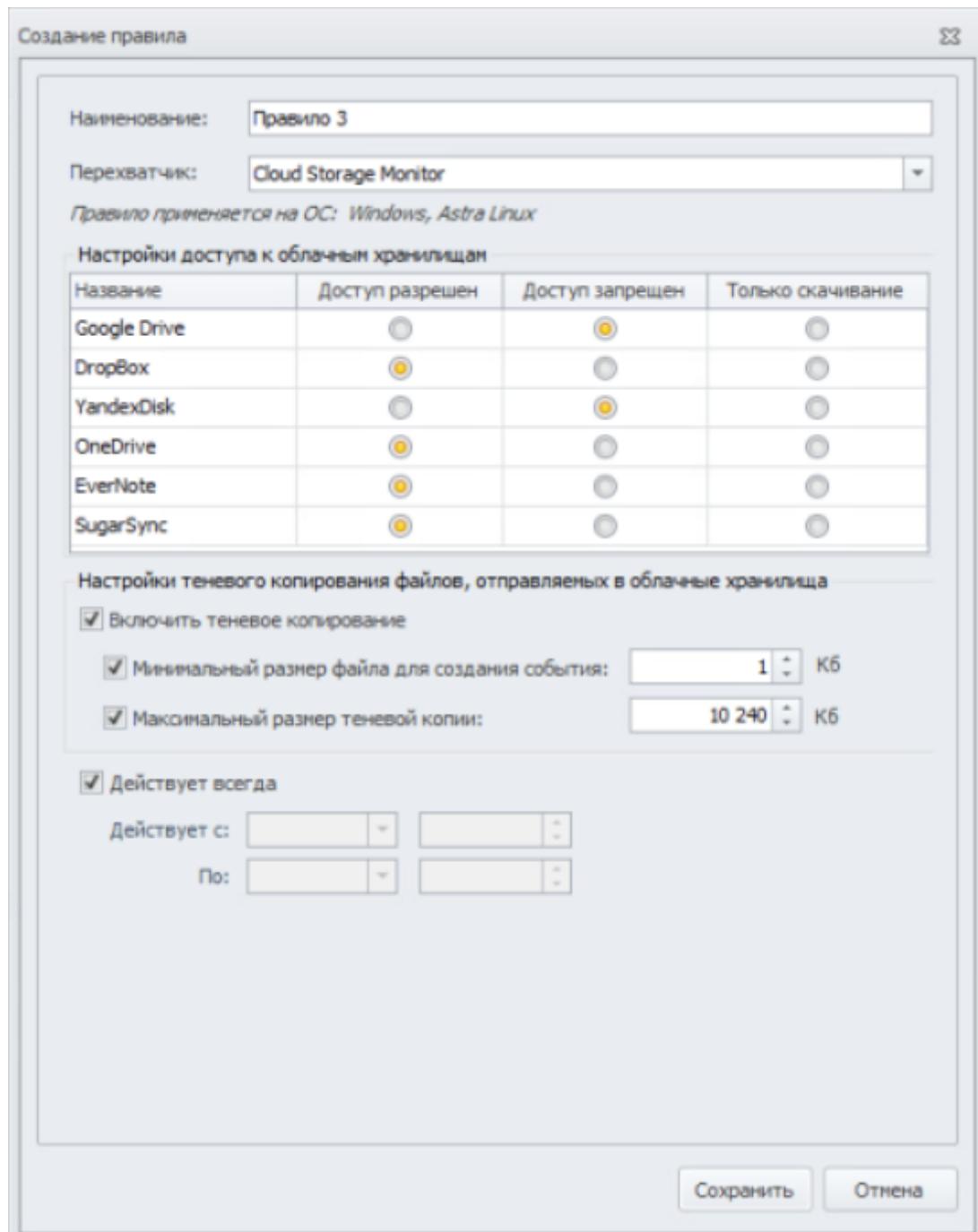


Сделать такой скрин

Правило 3

Ограничить доступ к облачным хранилищам GoogleDrive и YandexDisk.

Проверить работоспособность и зафиксировать выполнение



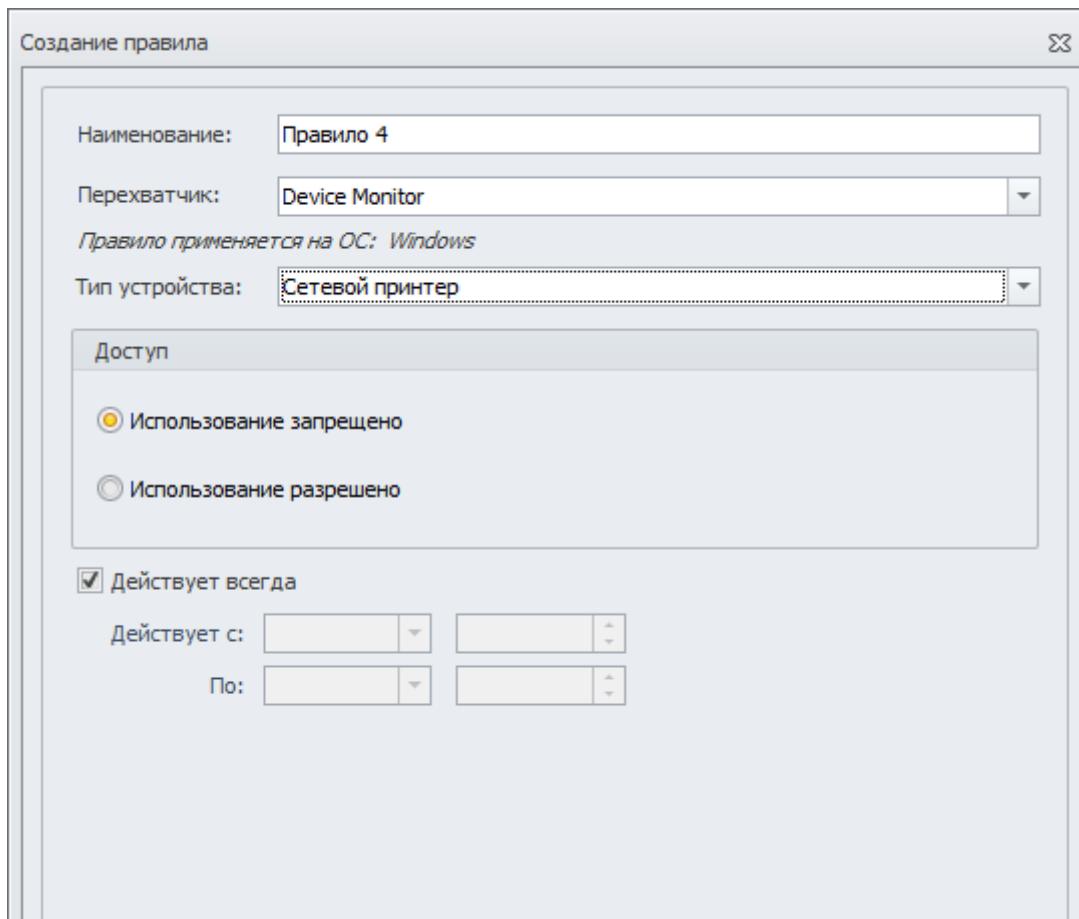
Здесь не создаем список, а сразу переходим в политику. **Сделать такой скрин**

#### Правило 4

Необходимо запретить печать на сетевых принтерах.

Зафиксировать создание политики скриншотом.

Создаем список и добавляем в него все приложения есть

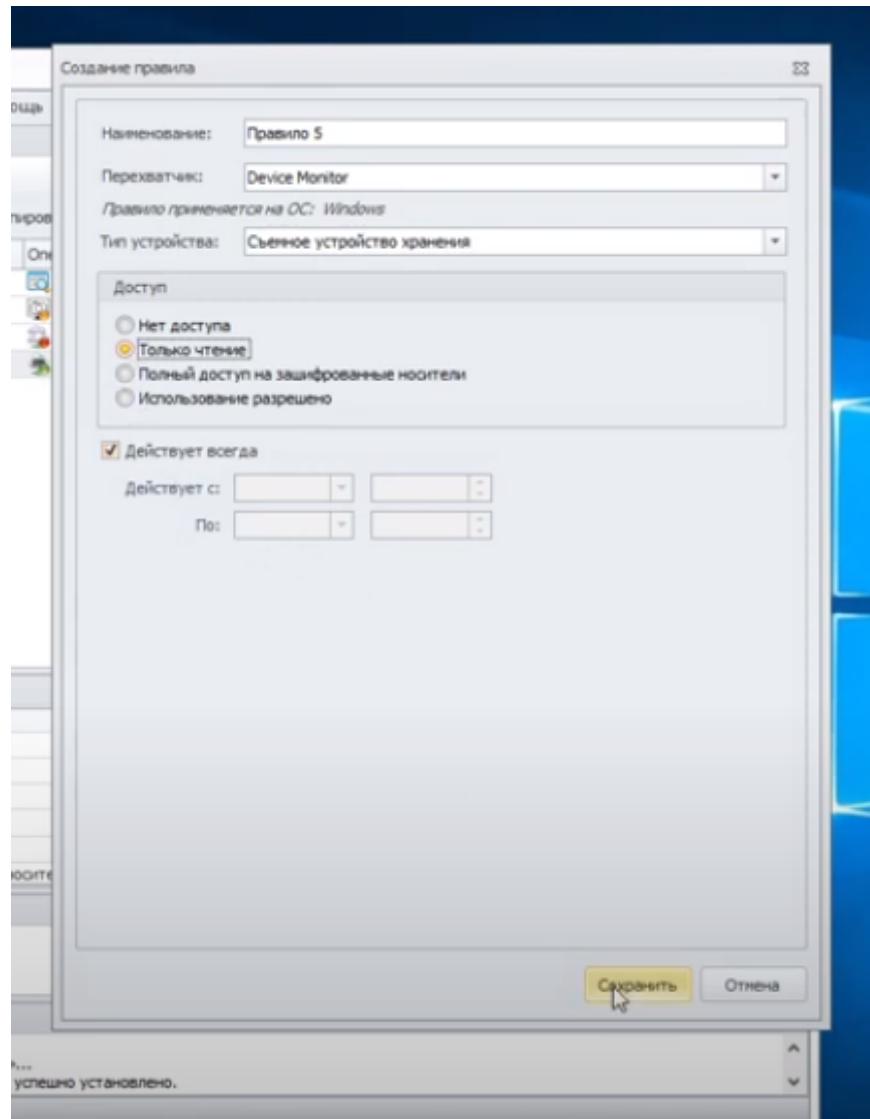


## Сделать такой скрин

### Правило 5

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

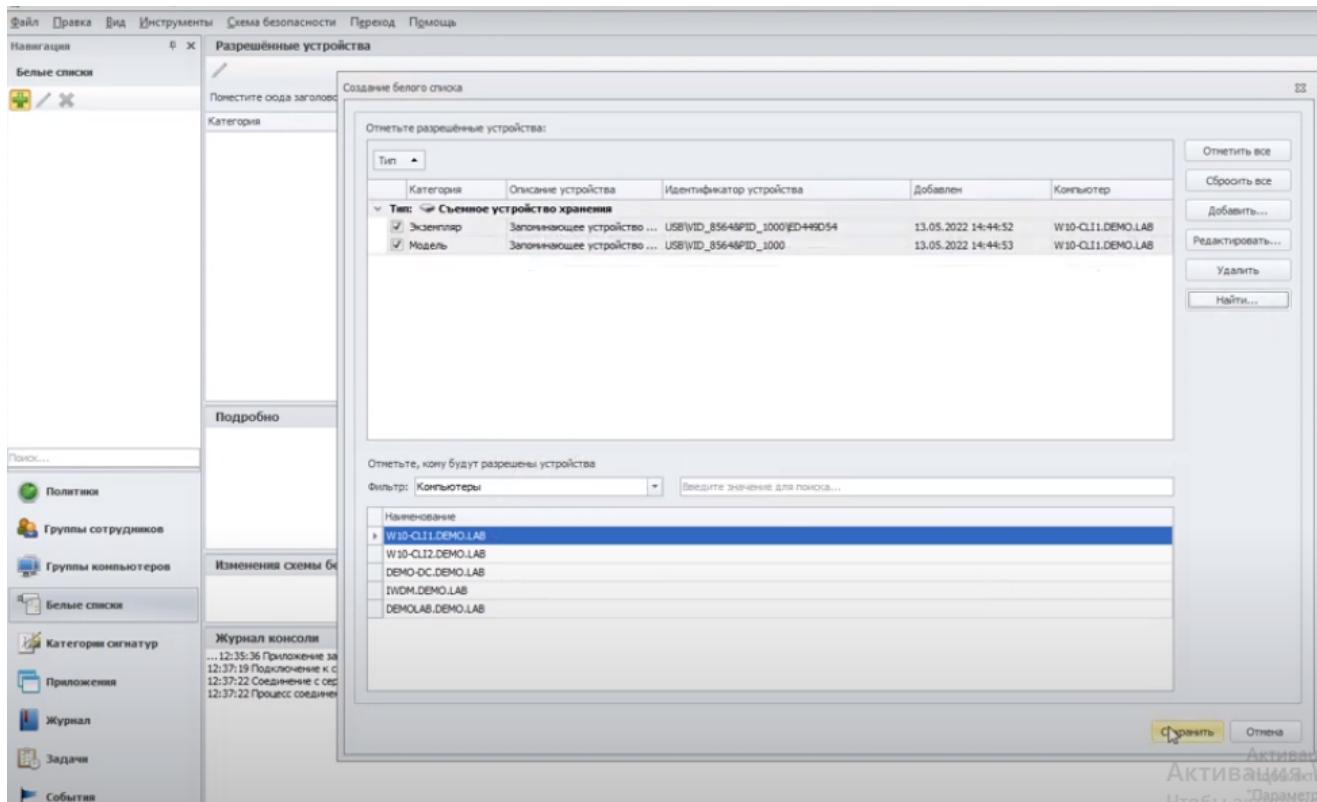
Проверить работоспособность и зафиксировать выполнение



## Правило 6

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

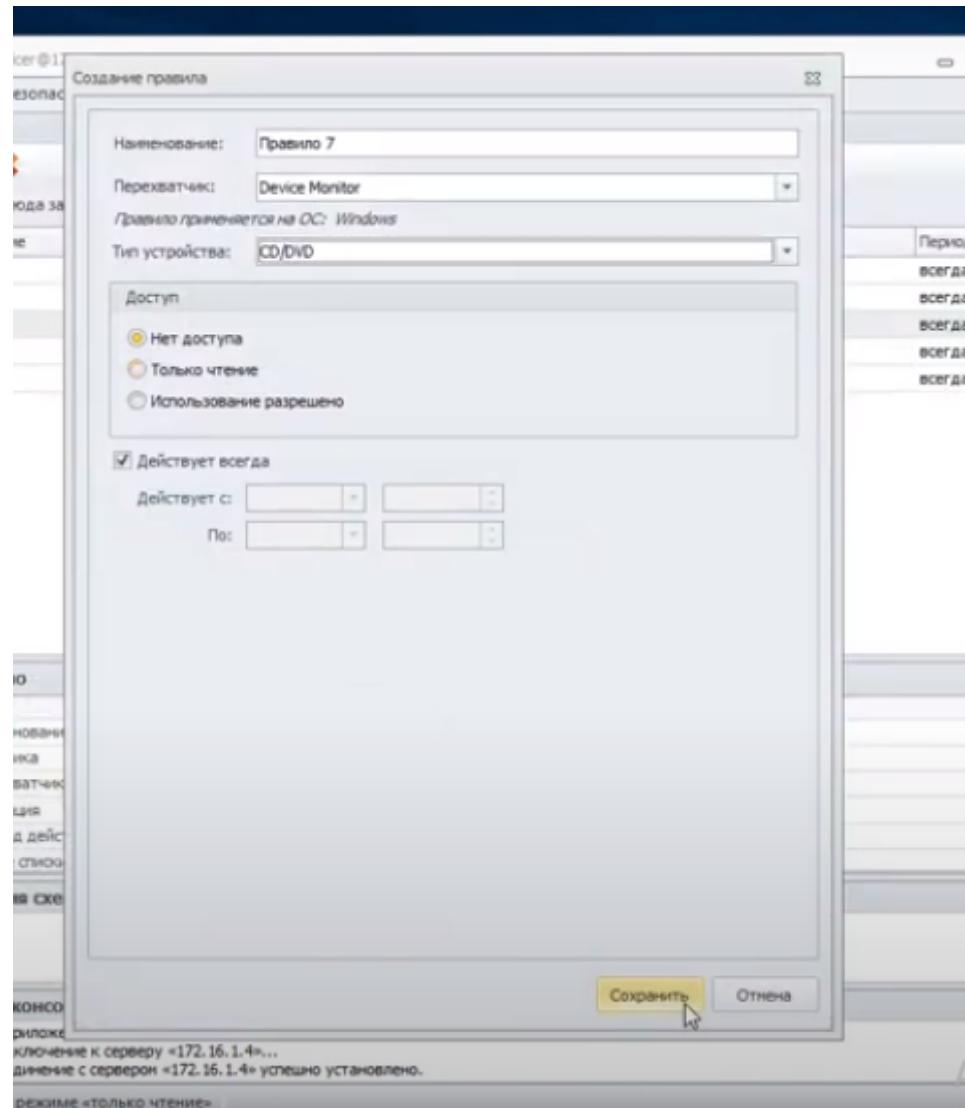
Проверить работоспособность и зафиксировать выполнение



## Правило 7

Полностью запретить использование CD/DVD-дисковода.

Проверить работоспособность и зафиксировать выполнение

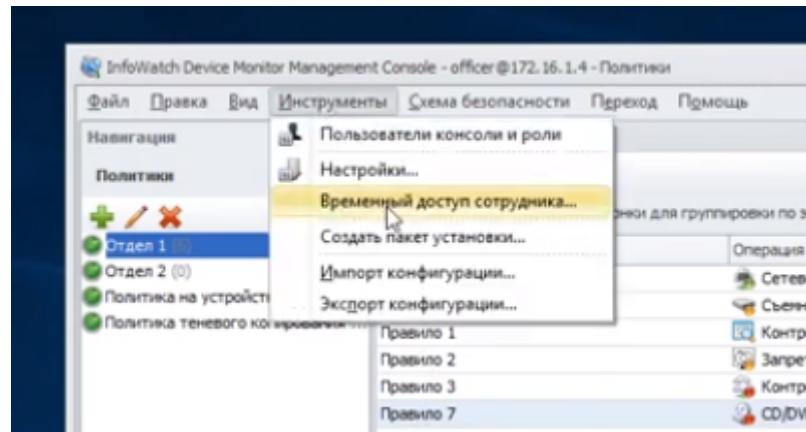


## Правило 8

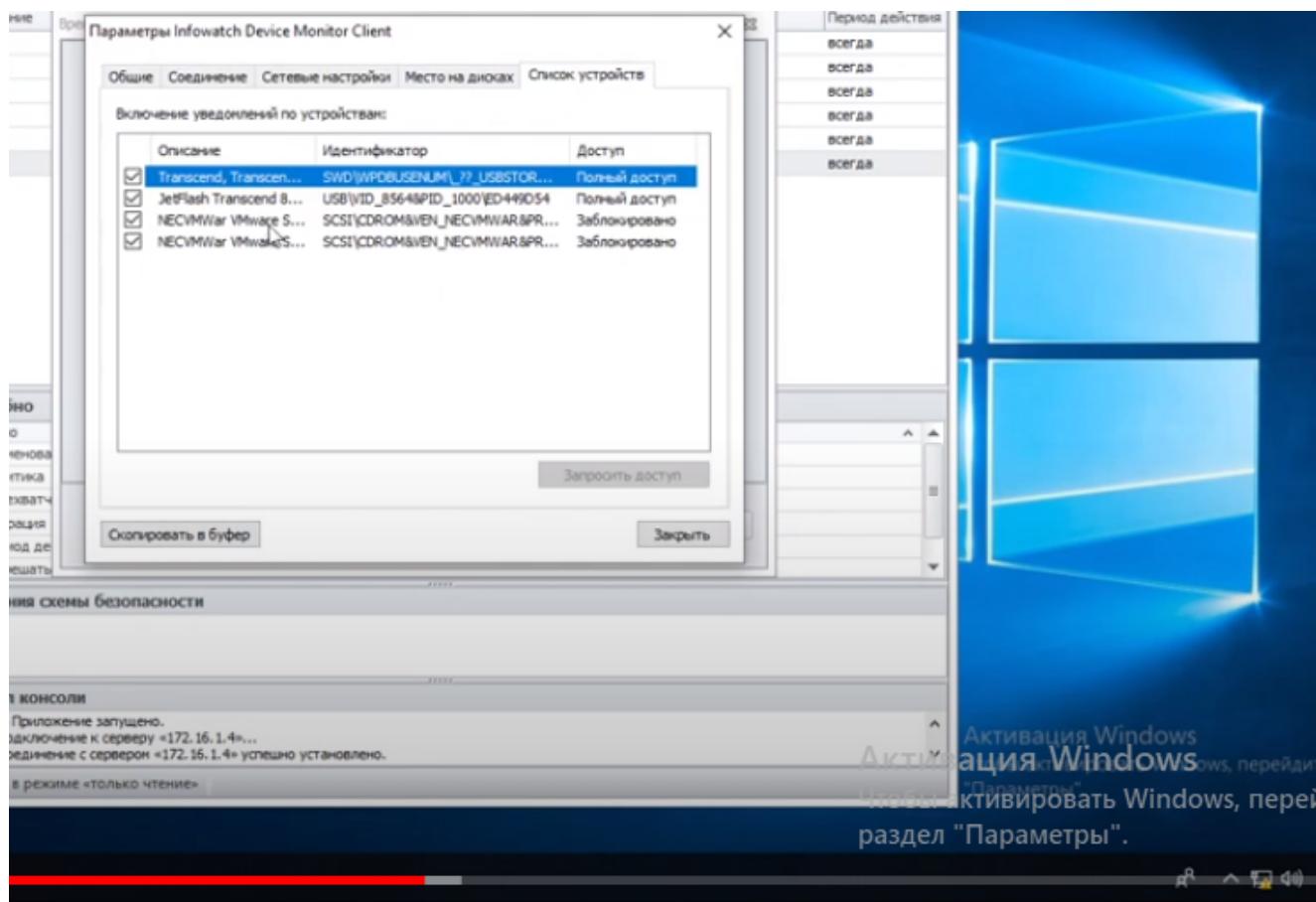
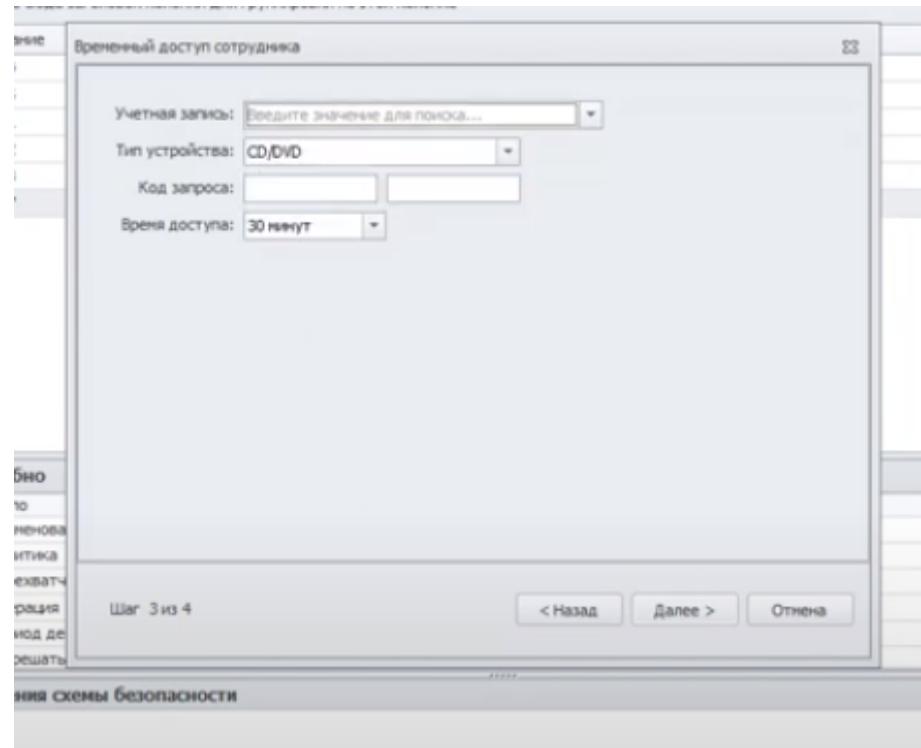
С учетом ранее выполненного запрета необходимо предоставить временный доступ для устройства на 7 минут для пользователя.

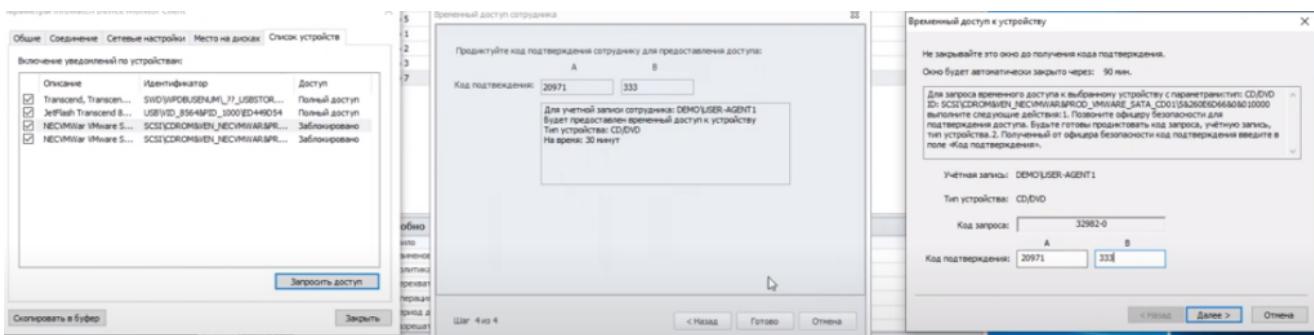
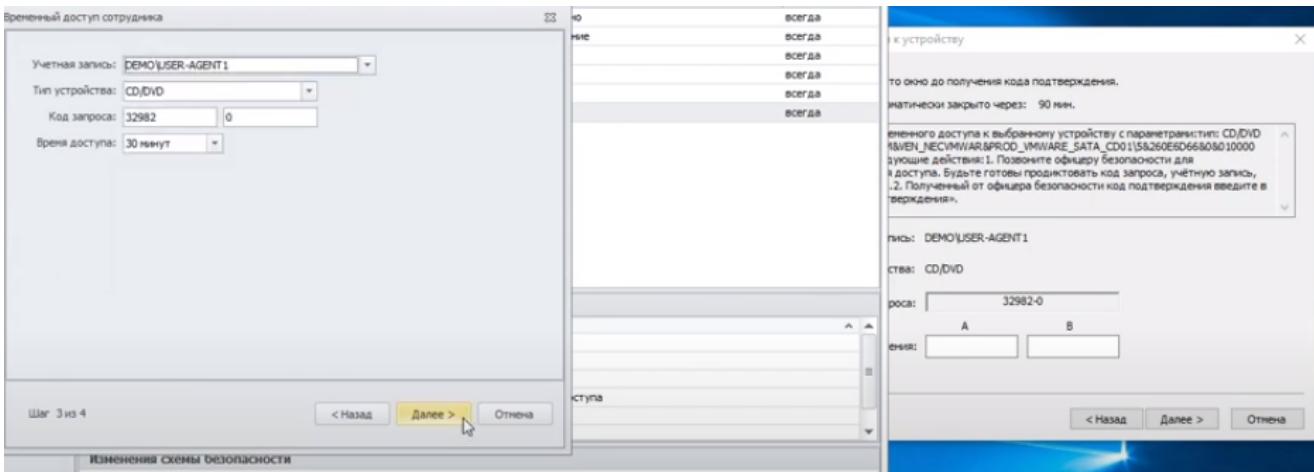
Зафиксировать этапы выдачи доступа и работоспособность скриншотами.

Следующие правила создаются в политике «Отдел2».



Screenshot of the 'Правила' (Rules) configuration screen. The title bar shows 'InfoWatch Device Monitor Management Console - officer@172.16.1.4 - Политики'. The left sidebar shows 'Навигация' (Navigation) with 'Политики' selected, and a list of rules: 'Отдел 1 (0)', 'Отдел 2 (0)', 'Политика на устройства (0)', and 'Политика теневого копирования...'. The main panel shows a rule named 'Временный доступ сотрудника'. The configuration fields include: 'Учетная запись:' (Account): 'Введите значение для поиска...', 'Тип устройства:' (Device type): 'Флоппи-дисковод' (Floppy disk drive), 'Код запроса:' (Request code), and 'Время доступа:' (Access time). The dropdown menu for 'Время доступа' shows the following options: 30 минут, 21 день, 22 дня, 23 дня, 24 дня, 25 дней, 26 дней, and 27 дней. To the right of the configuration panel, there is a table titled 'Период действия' (Validity period) with rows for each rule, all set to 'всегда' (always). At the bottom, there are buttons for '< Назад' (Back), 'Далее >' (Next), and 'Отмена' (Cancel).



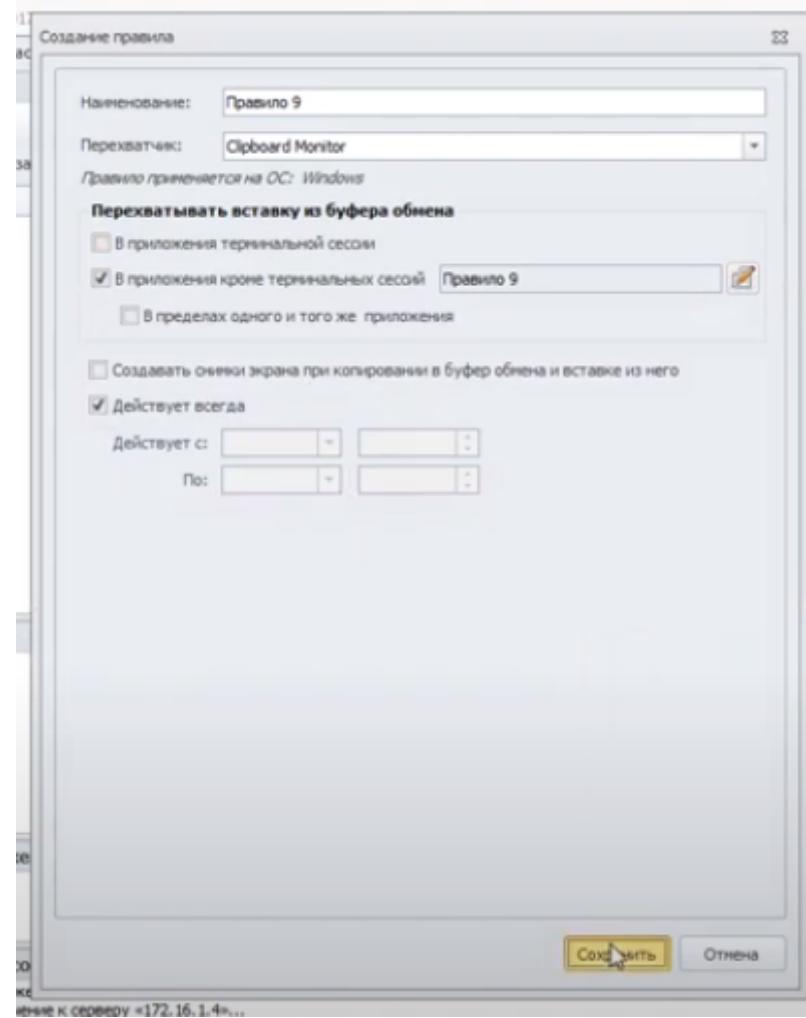


## Правило 9

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

Проверить занесение нескольких событий в WEB-консоль.

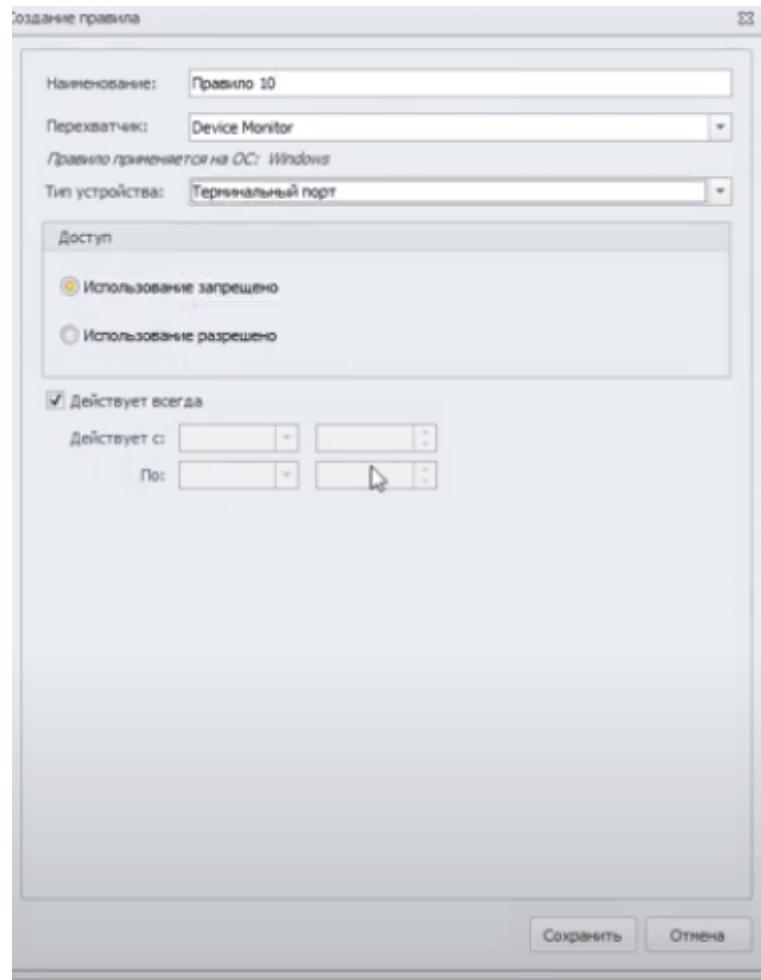
Проверить работоспособность и зафиксировать выполнение скриншотом.



## Правило 10

Необходимо запретить использовать терминальные сессии для пользователя.

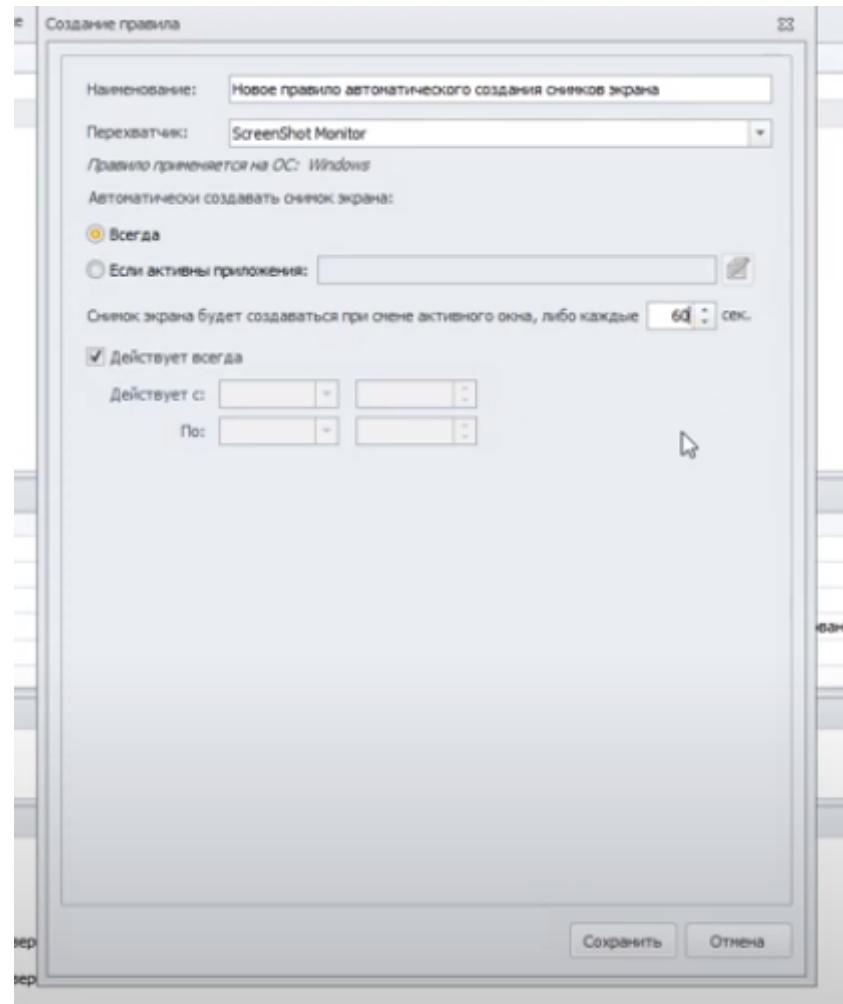
Проверить работоспособность и зафиксировать выполнение



## Правило 11

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

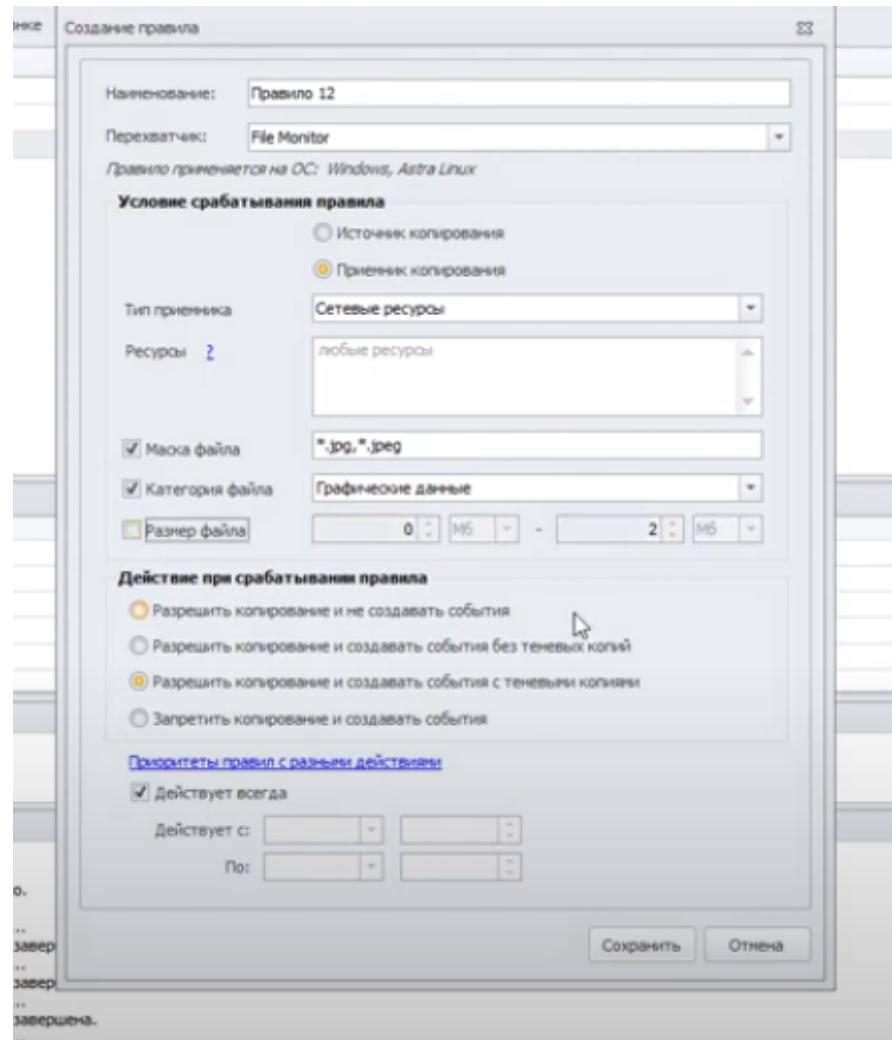
Проверить работоспособность и зафиксировать выполнение



## Правило 12

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

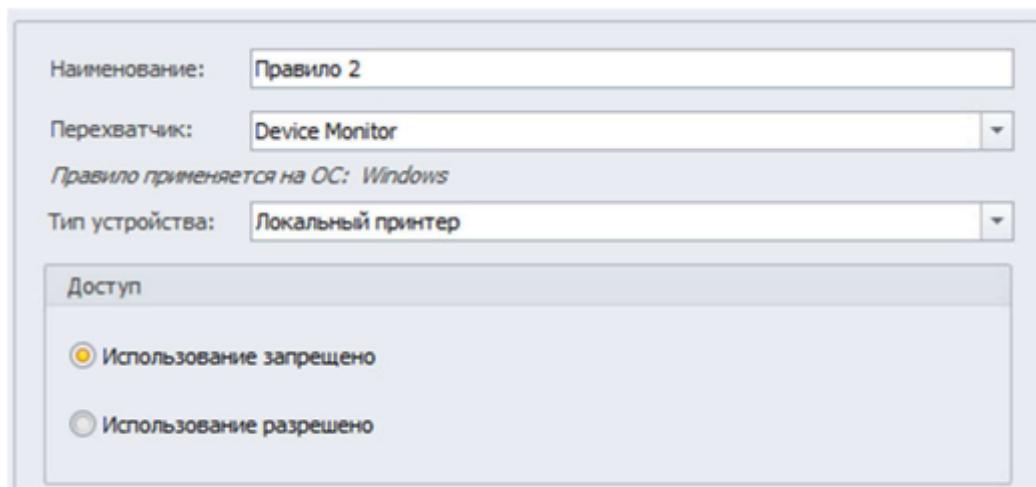
Проверить работоспособность и зафиксировать выполнение



## Правила доп

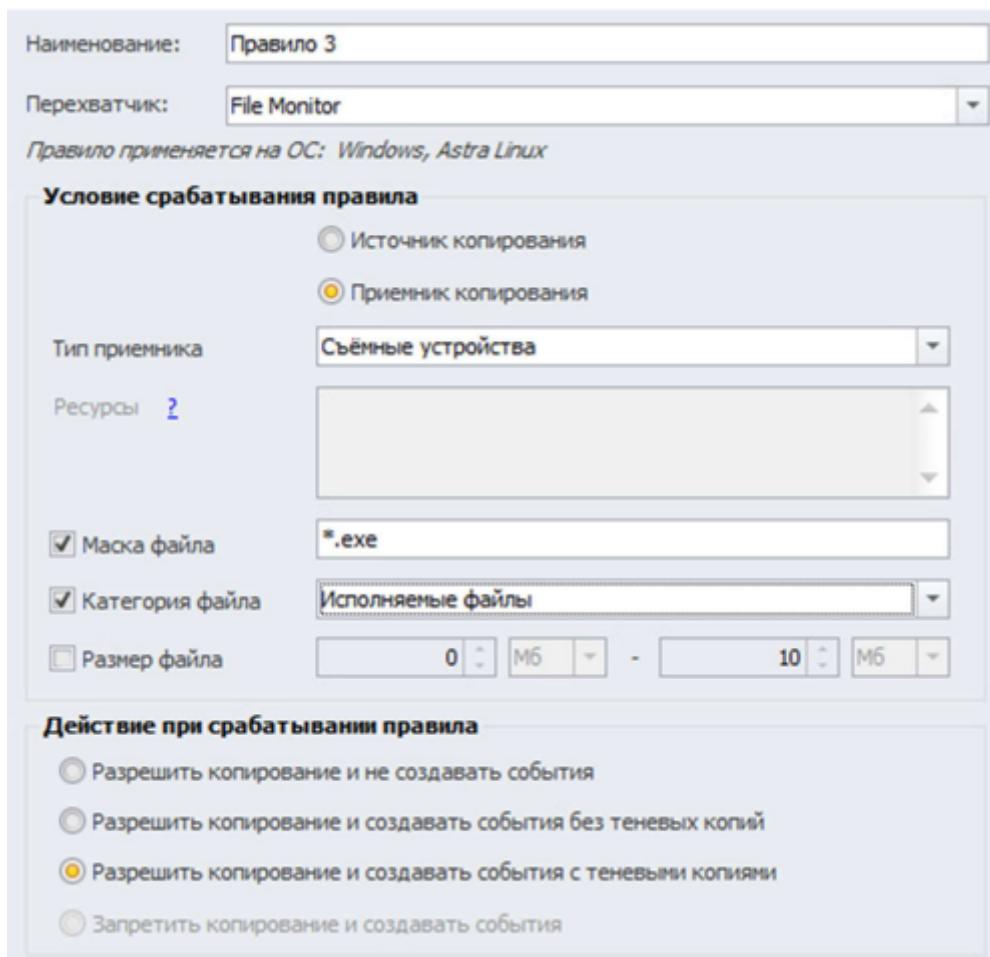
Необходимо запретить печать на локальных принтерах, но при этом оставить возможность печати на сетевых принтерах.

Зафиксировать создание политики скриншотом



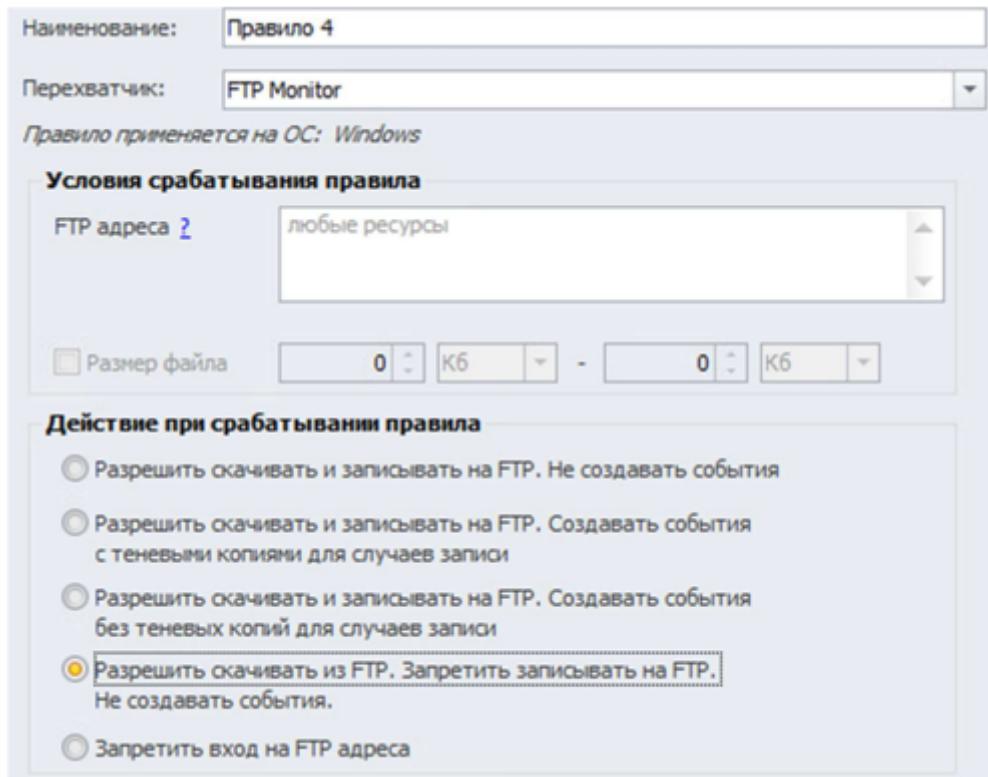
Создать политику по блокировке копирования исполняемых exe-файлов на USBнакопители. Проверить работоспособность и зафиксировать выполнение (зафиксировать результаты в виде скриншотов).

Проверить работоспособность и зафиксировать выполнение скриншотом.



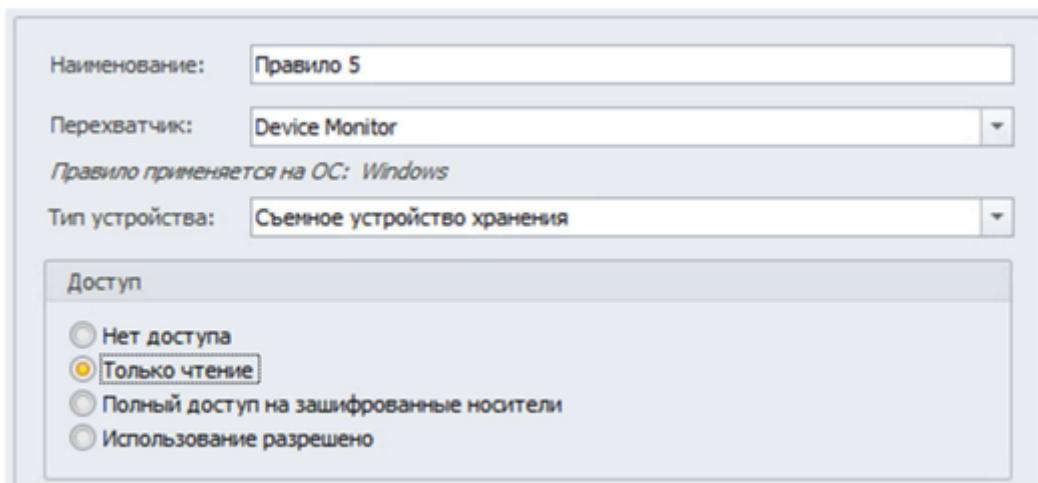
В связи с небезопасностью ftp-серверов разрешить только скачивание по протоколу ftp, загрузку файлов на сервер запретить.

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



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

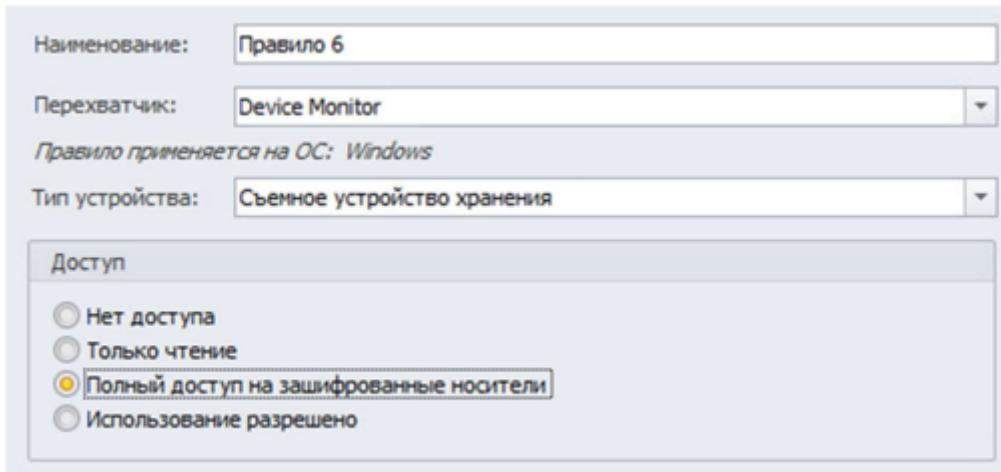
Проверить работоспособность и зафиксировать выполнение скриншотом.



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.

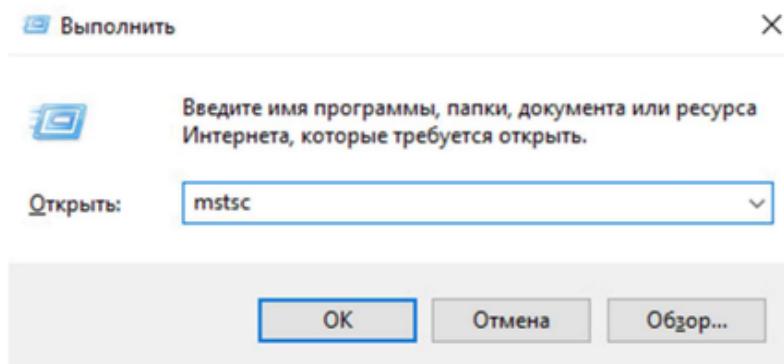
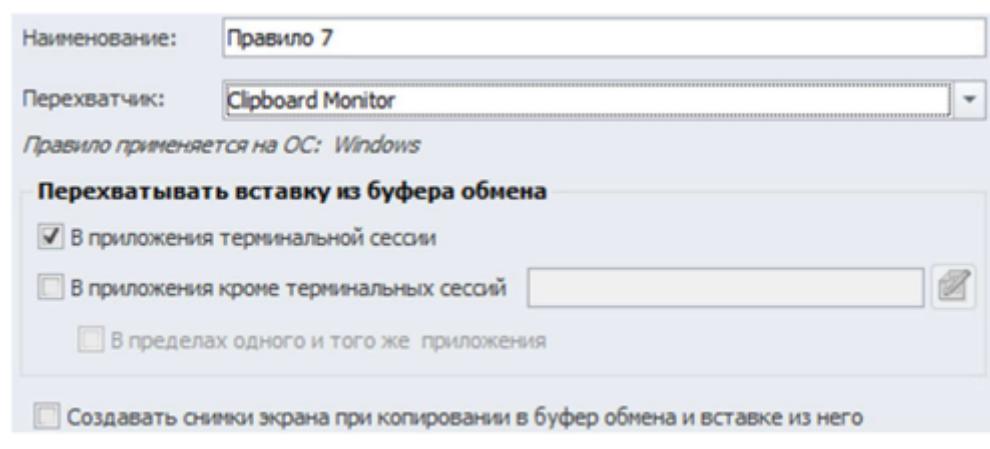
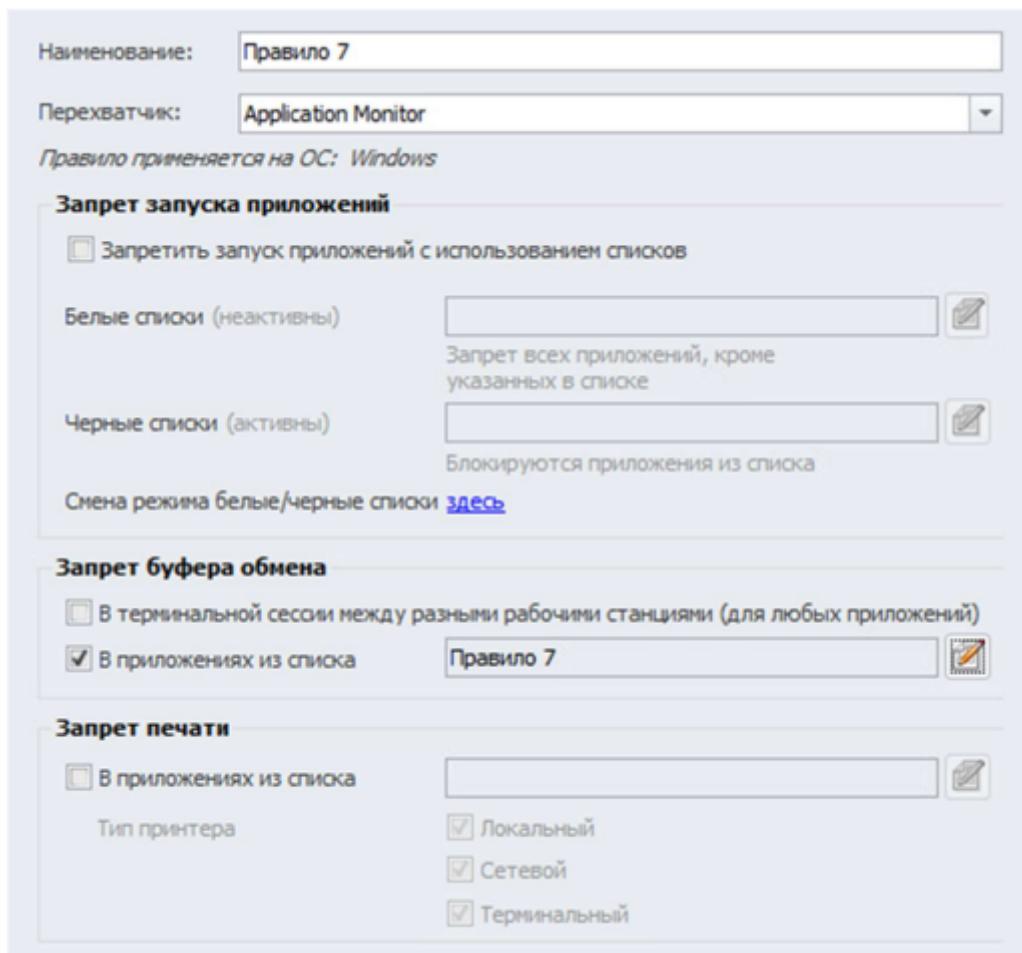


Рисунок 66 – «Открытие подключение к удаленному рабочему столу»

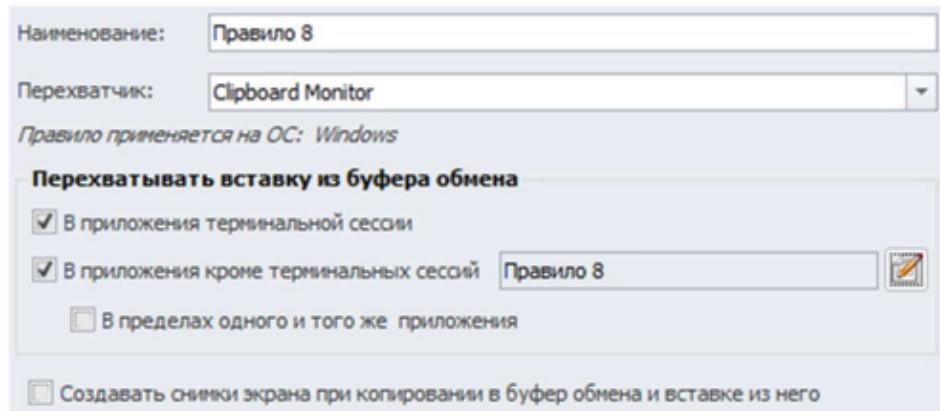
Теперь вернитесь к Device Monitor Console и создайте список приложений для правила, добавив в него «mstsc.exe». Вернитесь к политике «Отдел 2» и создайте правило в соответствии с рисунком 67. Затем, перейдите к политике «Политика на устройства» и создайте правило в соответствии с рисунком 68.

Актив  
Чтобы а  
раздел '

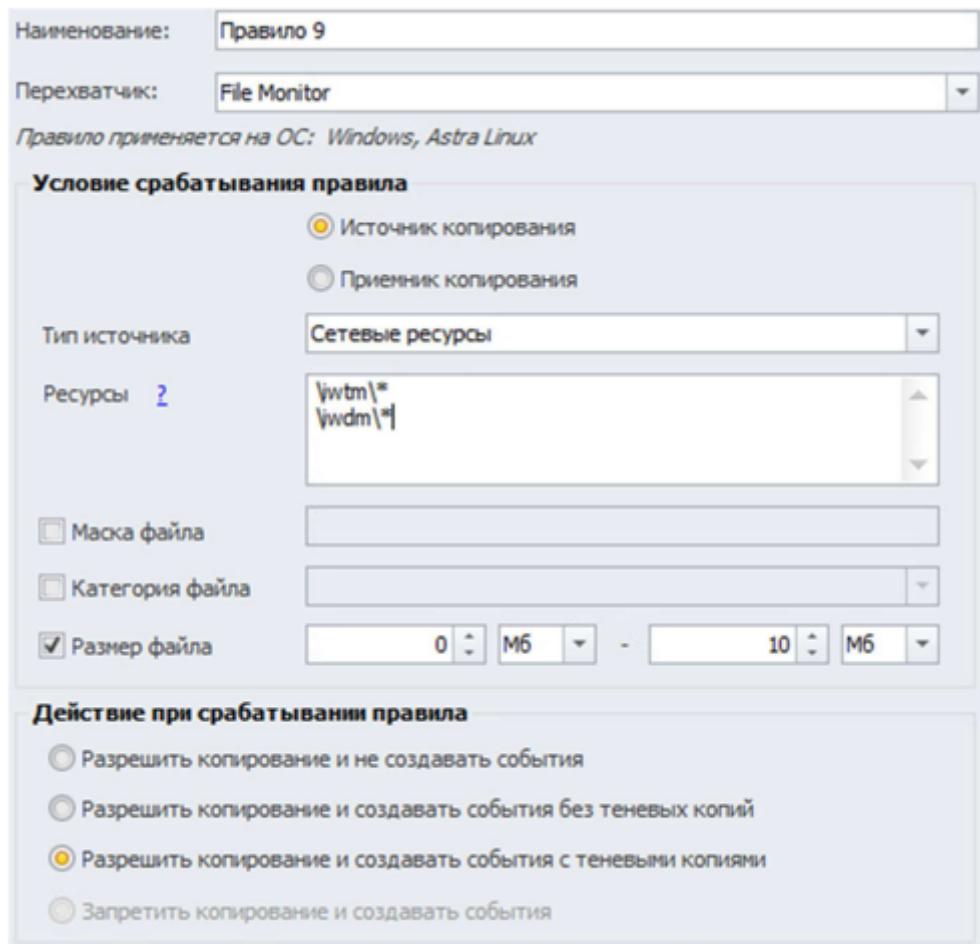


Необходимо поставить на контроль буфер обмена в текстовых процессорах (Word или Writer или Wordpad).  
Проверить работоспособность и зафиксировать выполнение занесением пары событий в IWTM на любые политики.

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 cli2).

**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**

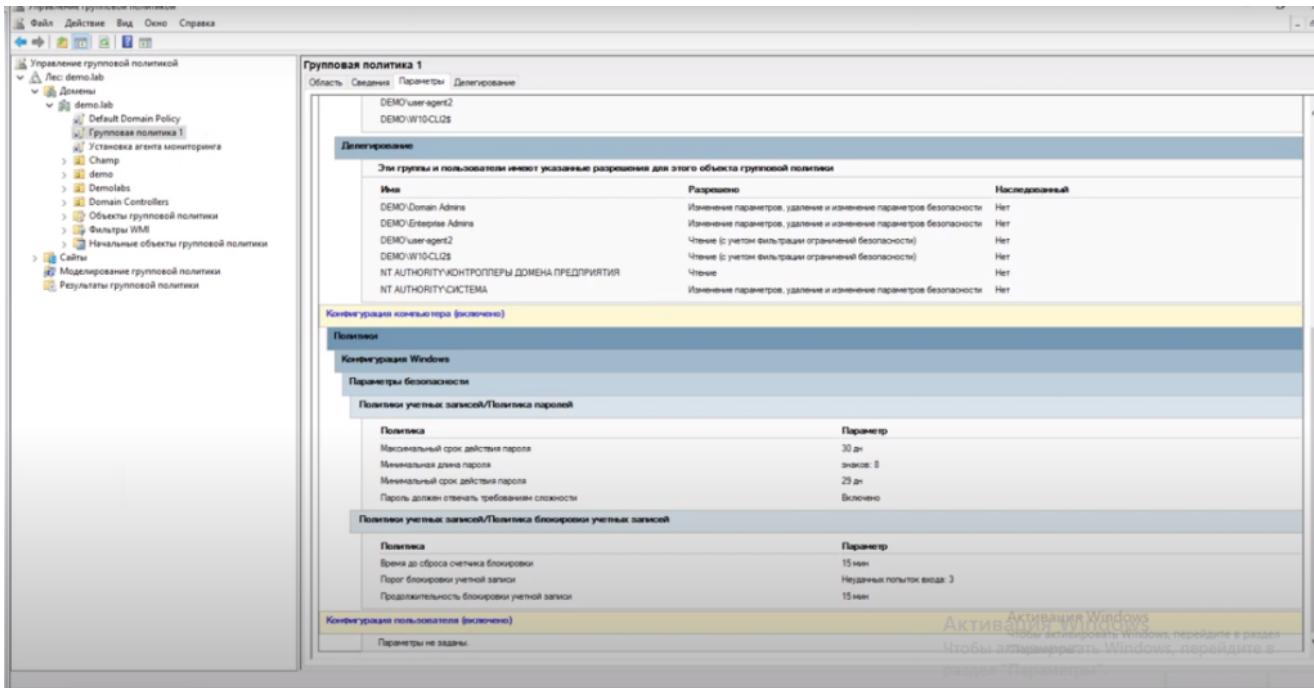
Объект GPO связан со следующим фильтром WMI:

<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»

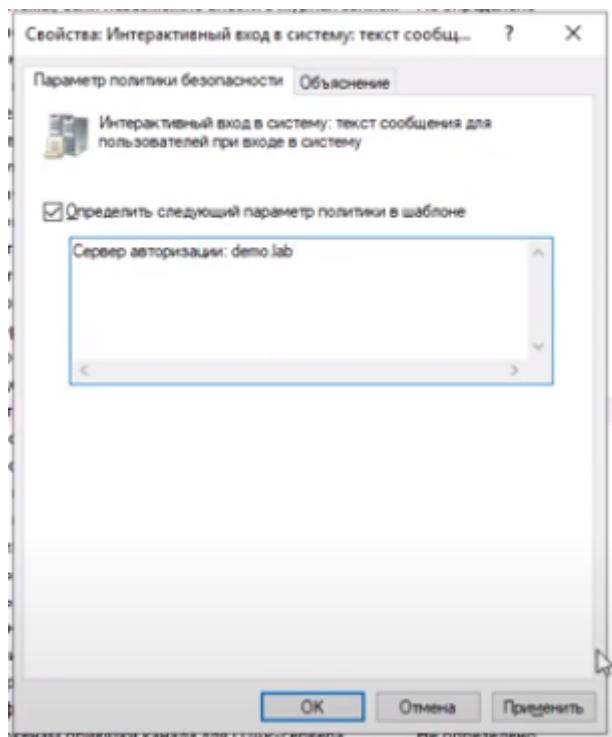
### Групповая политика 5

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

Зафиксировать настройки политики и выполнение скриншотами.

Политика

- DCOM: Ограничения компьютера на доступ в синтаксисе SDDL (Security Descriptor D... Не определено
- DCOM: Ограничения компьютера на запуск в синтаксисе SDDL (Security Descriptor De... Не определено
- Аудит: аудит доступа глобальных системных объектов Не определено
- Аудит: аудит использования привилегии на архивацию и восстановление Не определено
- Аудит: немедленное отключение системы, если невозможно внести в журнал запис... Не определено
- Аудит: принудительно переопределяет параметры категории политики аудита параллельно с текущими параметрами аудита 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 пользователей при входе в систему Не определено
- Интерактивный вход в систему: количество предыдущих подключений к кешу (в слу... Не определено
- Интерактивный вход в систему: напоминать пользователям об истечении срока действия паролей 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 коммюнити 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 отмены блокировки 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 дисков и доступ ко всем дискам и папкам Не определено
- Контроллер домена: запретить изменение пароля учетных записей компьютера Не определено
- Контроллер домена: разрешать узкоспециализированные подключения по защищенным каналам ... 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\ldapsync-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.

Политики защиты данных:

- демоэкзамен
 

Каталог объектов защиты: демоэкзамен  
Передача Копирование Хранение Работа в приложениях
- Договоры и контракты
 

Каталог объектов защиты: Договоры и контракты  
Передача 2 Копирование 1 Хранение Работа в приложениях
- Отдел кадров
 

Каталог объектов защиты: Отдел кадров  
Передача 2 Копирование 1 Хранение Работа в приложениях
- Маркетинг
 

Каталог объектов защиты: Маркетинг  
Передача 2 Копирование 1 Хранение Работа в приложениях
- Грифованная информация
 

Каталог объектов защиты: Грифованная информация  
Передача 2 Копирование 1 Хранение 1 Работа в приложениях
- Конкурсная документация
 

Каталог объектов защиты: Конкурсная документация

демоэкзамен

Название: демоэкзамен  
Период действия: Все время  
Статус:

Защищаемые данные

Выбрать  
Политика сработает при обнаружении хотя бы одного вхождения в каждый из типов данных  
Каталоги объектов защиты: демоэкзамен  
Описание: Введите описание  
Создан: 17.12.2021 05:30 Изменен: 17.12.2021 05:31

**Сохранить** **Отменить**

(выключить и удалить все к черту)

Вы редактируете конфигурацию с 13.05.2022 07:52. Применить Сохранить Оббросить Версия действующей конфигурации - № 7. Поиск событий

Каталоги объектов защиты

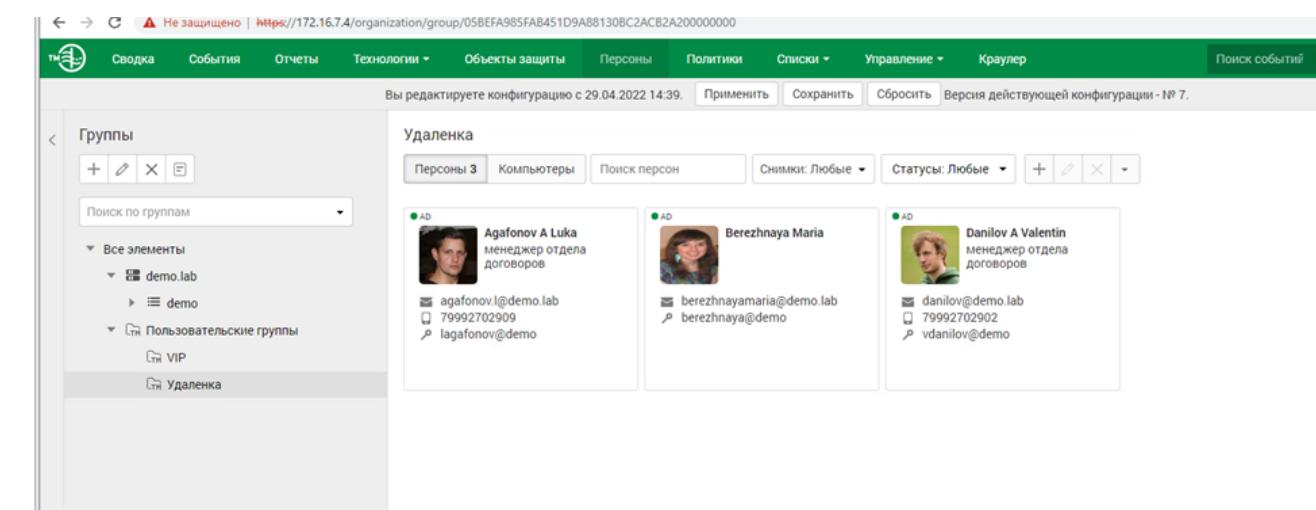
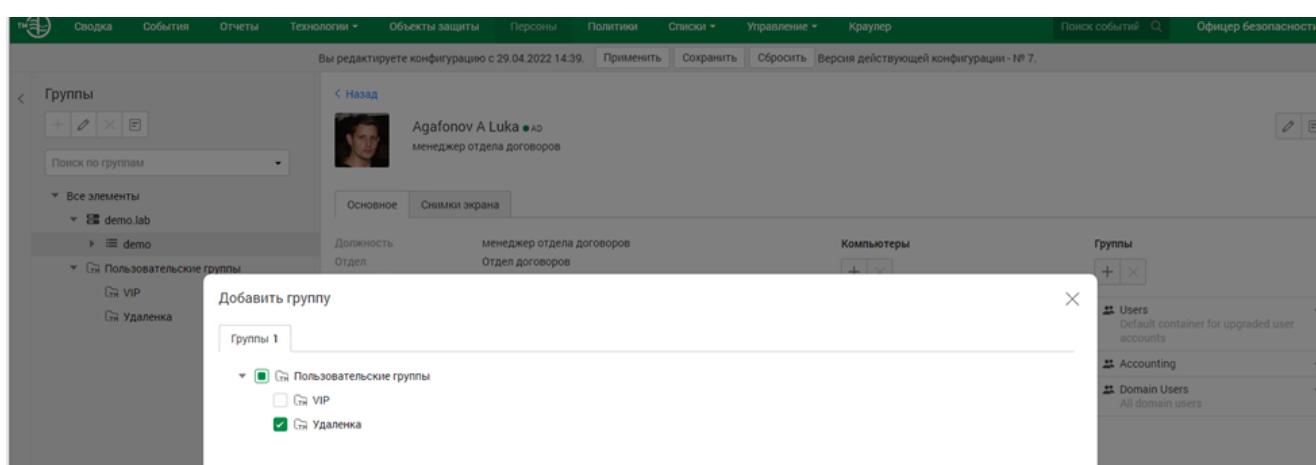
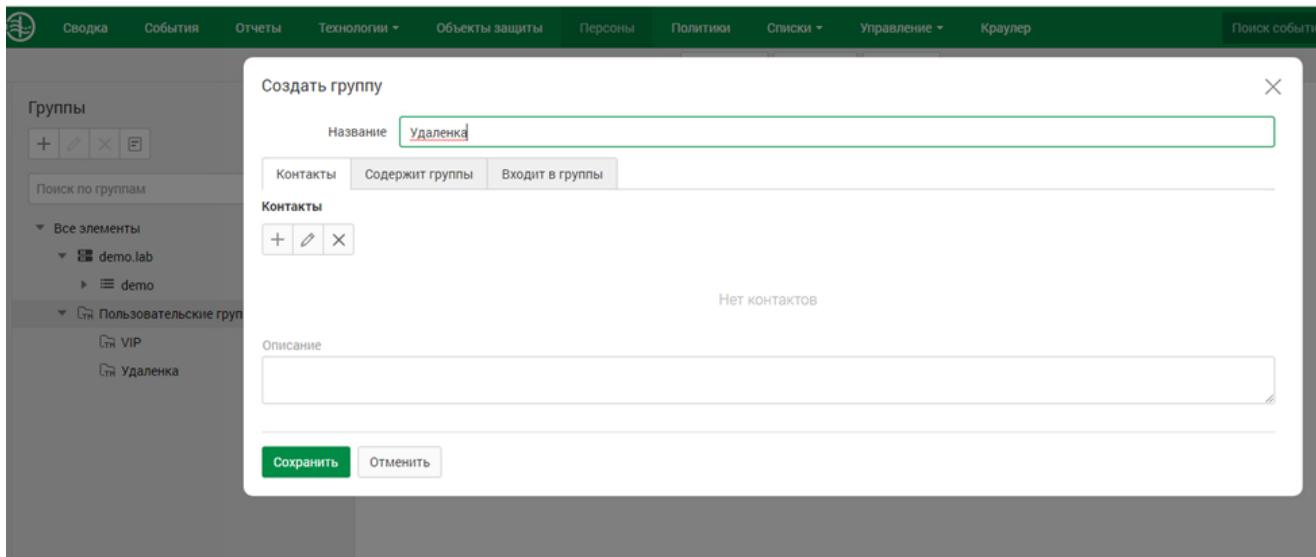
Название	Элементы технологий	Дата создания	Дата изменения	Описание
Грифы конфиденциальности	Грифы конфиденциальности	17.11.2021 05:29	17.11.2021 05:29	
Грифы секретности	Грифы секретности	17.11.2021 05:29	17.11.2021 05:29	

Грифованная информация

Активировать  
Деактивировать  Импортировать  
Экспортировать  
Создать политику защиты данных  
Создать политику защиты данных на агенте

## 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.



### 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 назвать этот список. Перейдите к созданному списку и нажмите кнопку «Добавить веб-ресурс» и начните добавьте необходимые ресурсы.

The screenshot shows the Infowatch software interface. At the top, there is a navigation bar with tabs: Сводка, События, Отчеты, Технологии, Объекты защиты, Персоны, Политики, Списки, Управление, and Краулер. The URL in the address bar is https://12.16.7.4/lists/resources. A modal window titled 'Создать список веб-ресурсов' (Create web resource list) is open. It contains fields for 'Название' (Name) set to 'Сайты партнеров' and 'Описание' (Description). Below these fields are 'Сохранить' (Save) and 'Отменить' (Cancel) buttons. In the background, a list of web resources is visible, including 'Анонимайзеры', 'Блоги', 'Веб-почта', 'Медиа', 'Мусорный трафик', 'ПО и обновления', 'Поиск работы', and 'Потенциально опасные ресурсы'. Each item has a value column and a 'Тематика для взрослых' (Adult theme) column.

## Добавить веб-ресурс

The screenshot shows the 'Add web resource' dialog box. It has two input fields: 'Значение' (Value) containing 'kb.infowatch.com' and 'Описание' (Description) which is empty. At the bottom are 'Сохранить' (Save) and 'Отменить' (Cancel) buttons.

(значения будут отличаться)

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

Сайты партнеров

+ П Поиск

Значение	Описание
dnevnik.ru\	
infotecs.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 свобода и доступна для редактирования. Последний раз конфигурацию редактировали в 29.04.2022 14:44. Версия действующе

Периметры

+ ×

Исключить из перехвата

Компания

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

## 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.

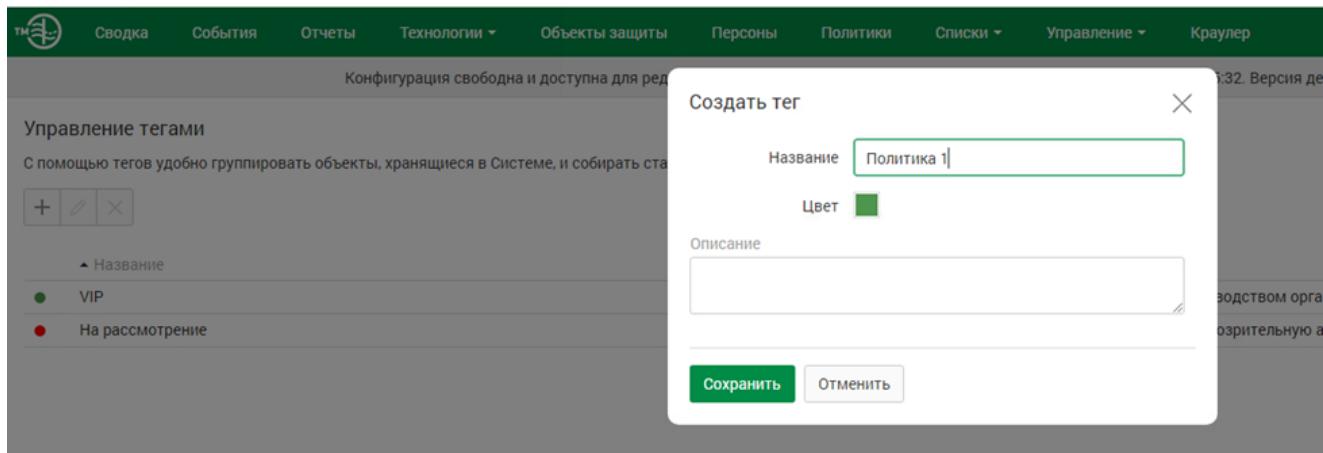
Политика защиты данных

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



Название	Дата создания	Страна	Описание
Дипломатический паспор...	17.11.2021 05:29	Российская Федера...	Дипломатический паспор...
Загранпаспорт граждани...	17.11.2021 05:29	Российская Федера...	Заграничный паспорт гра...

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

Помощь

Каталоги объектов защиты

Персональные данные

Создание объекта защиты

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

Поиск

Название Дата создания Описание

Кредитная карта 17.11.2021 05:29 Система срабатывает на изображение лицевой стороны б...

**Паспорт гражданина РФ** 17.11.2021 05:29 Система срабатывает на изображение главного разворота...

10

Создать Отменить Создать объект защиты на каждый выбранный элемент

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

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, Диплом... 29.04.2022 14:55 29.04.2022 14:55...

Резюме Резюме 17.11.2021 05:29 17.11.2021 05:29...

Сведения о государственной реги... ОГРН, ОГРНИП, Регистрационный... 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, Загранп... 17.11.2021 05:29 17.11.2021 05:29...

К < 1 2 3 > >

Сохранить Отменить

The screenshot shows the 'Politiki' (Policies) section of the software. A specific policy named 'Политика защиты данных' (Data Protection Policy) is selected. The right panel displays the configuration details for this policy:

- Название:** Политика 1
- Период действия:** Всё время
- Статус:** Включен (green switch)
- Защищаемые данные:** Выбрать (Select protected data)
- Объекты защиты:** Политика 1
- Описание:** Введите описание (Enter description)
- Создан:** 04.05.2022 14:45
- Изменен:** 04.05.2022 14:45

At the bottom right of the main window, there are 'Сохранить' (Save) and 'Отменить' (Cancel) buttons.

This screenshot shows the 'Отправители' (Senders) configuration dialog. It lists several categories of senders:

- Контакты:** Enterprise Admins, Enterprise Key Admins, Enterprise Read-only Domain Controllers, Financial, Group Policy Creator Owners (selected), HR, IT, Key Admins, Protected Users, RAS and IAS Servers.
- Группы 1:** None selected.
- Персоны:** None selected.
- Домены:** None selected.
- Периметры:** None selected.

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

This screenshot shows the 'Получатели' (Recipients) configuration dialog. It lists several recipient categories:

- Контакты:** None selected.
- Группы:** None selected.
- Персоны:** None selected.
- Домены:** None selected.
- Веб-ресурсы:** None selected.
- Периметры 1:** None selected.

Below these are search and filter fields:

- Поиск:** Помощь
- Название:** None selected.
- Исключить из перехвата:** None selected.
- Компания:** Selected.

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

**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 почтовое уведомление: Начните вводить текст
- Назначить событию вердикт: Разрешить
- Назначить событию уровень нарушения: Низкий

**Сохранить**   **Отменить**

**Правило передачи**

Отправители: W10-CLI1, W10-CLI2

Получатели: Компания

Дни действия правила: Любой день недели

Часы действия правила: 0:00 - 0:00

**Действия при срабатывании правила**

- Отправить почтовое уведомление: Начните вводить текст
- Назначить событию вердикт: Разрешить
- Назначить событию уровень нарушения: Низкий
- Назначить событию теги: Политика 1
- Назначить отправителю статус: Выберите статус

**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

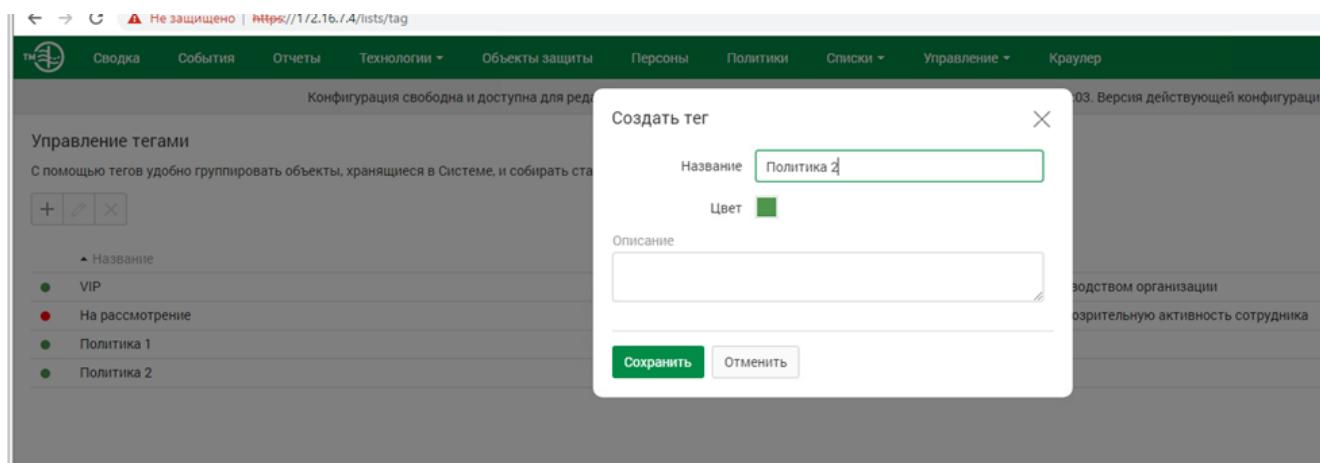
Создаем тег, после технологии – далее в объект – далее в политики (только объект)

В одну сторону

Отправитель не изменяется

Получатель не равно компания

Время и дата не изменяются Тег ранее созданный



Название	Формат файла	Название файла	Размер файла	Дата создания	Описание
Dоговор.doc	Документ Microsoft Word	Dоговор.doc	40.5 KB	29.04.2022 15:04	

Порог цитируемости текстовых данных  
50%

Порог цитируемости бинарных данных  
50%

Порог цитируемости определяет процент эталонного документа, достаточный для отнесения перехваченного объекта к данному эталонному документу

The screenshot shows the InfoWatch Traffic Monitor Enterprise interface. A modal dialog box titled 'Создать' (Create) is open. In the 'Название' (Name) field, 'Политика 2' is entered. The 'Статус' (Status) toggle switch is turned on. Below the dialog, a list of protection objects is visible, including 'Активы и бюджетированные' (Active and budgeted), 'Базы данных' (Data bases), 'Бухгалтерская отчетность' (Financial reporting), 'Грифы конфиденциальности' (Confidentiality stamps), 'Грифы секретности' (Secret stamp), 'Дирекция' (Direction), 'Договоры и контракты' (Contracts), 'Информационная безопасность' (Information security), 'Информация по кредитам' (Credit information), and 'Информация по счетам' (Account information). The date 17.11.2021 is also visible.

The screenshot shows the InfoWatch Traffic Monitor Enterprise interface. A modal dialog box titled 'Создание объекта защиты' (Create protection object) is open. It has tabs for 'Категории' (Categories), 'Текстовые объекты' (Text objects), 'Эталонные документы 1' (1 Standard documents), 'Бланки' (Templates), 'Печати' (Prints), 'Выгрузки из БД' (Exports from DB), and 'Графические объекты' (Graphic objects). The 'Эталонные документы' (Standard documents) tab is selected, showing a list with one item: 'Документ Microsoft Word' named 'Договор.doc'. The date 04.05.2023 is also visible. At the bottom of the dialog, there are 'Создать' (Create) and 'Отменить' (Cancel) buttons, and a checkbox for creating the object on selected elements.

The screenshot shows a web-based configuration interface for InfoWatch Traffic Monitor Enterprise. A modal window titled "Создание объекта защиты" (Create Protection Object) is open. In the "Название" (Name) field, "Политика 2" is entered. The "Статус" (Status) switch is turned on. Below the status are two tabs: "Элементы технологий" (Technology Elements) and "Условия обнаружения" (Detection Conditions). Under "Элементы технологий", there is a button "Выбрать элементы" (Select elements) and a list containing "Договор.doc" (Contract.doc) described as "Эталонный документ" (Sample document). There is also an "Описание" (Description) text area. At the bottom of the modal are "Создать" (Create) and "Отменить" (Cancel) buttons.

The screenshot shows the main configuration interface for protection policies. The top navigation bar includes links for Home, 192.168.21.7, demo.lab, IWDM, w10-d1, IWTM, and w10-d2. The current tab is IWDM. The URL in the address bar is https://172.16.22.2/protected/43594ED51AB64B99A87CC4541402F63800000000. The main content area displays a list of protection policies under the heading "Политики". One policy, "Политика 2", is selected and expanded, showing its details: "Политика на любые данные" (Policy for any data), "Передача" (Transfer), "Копирование" (Copy), "Хранение" (Storage), and "Работа в приложениях" (Work in applications). To the right of the policy list, a detailed view of "Политика защиты данных" (Data protection policy) is shown. It includes fields for "Название" (Name: Политика 2), "Период действия" (Period of validity: Все время) (All the time), and "Статус" (Status: On). The "Захищаемые данные" (Protected data) section has a "Выбрать" (Select) button. The "Объекты защиты" (Protected objects) section lists "Политика 2" and includes an "Описание" (Description: Введите описание) (Enter description) text area. At the bottom of the right panel are "Сохранить" (Save) and "Отменить" (Cancel) buttons. The bottom of the screen shows the Windows taskbar with icons for Start, Search, Task View, File Explorer, File History, and Google Chrome.

## 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

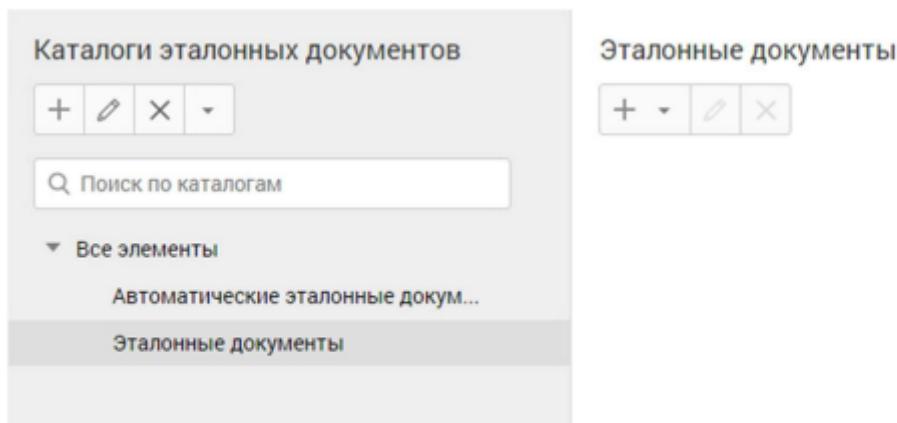


Рисунок 75 – «Эталонные документы»

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

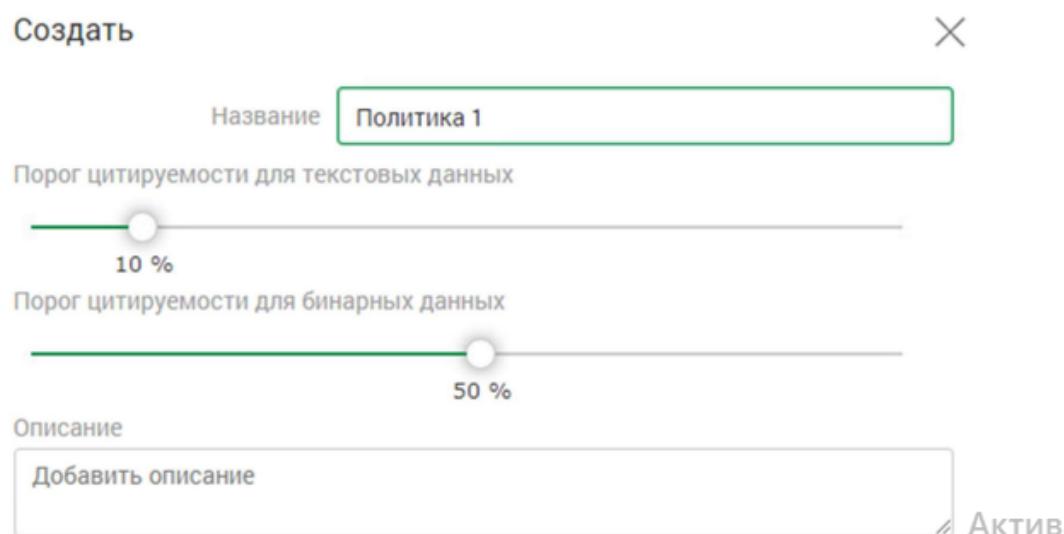


Рисунок 76 – «Создание каталога эталонных документов»

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).

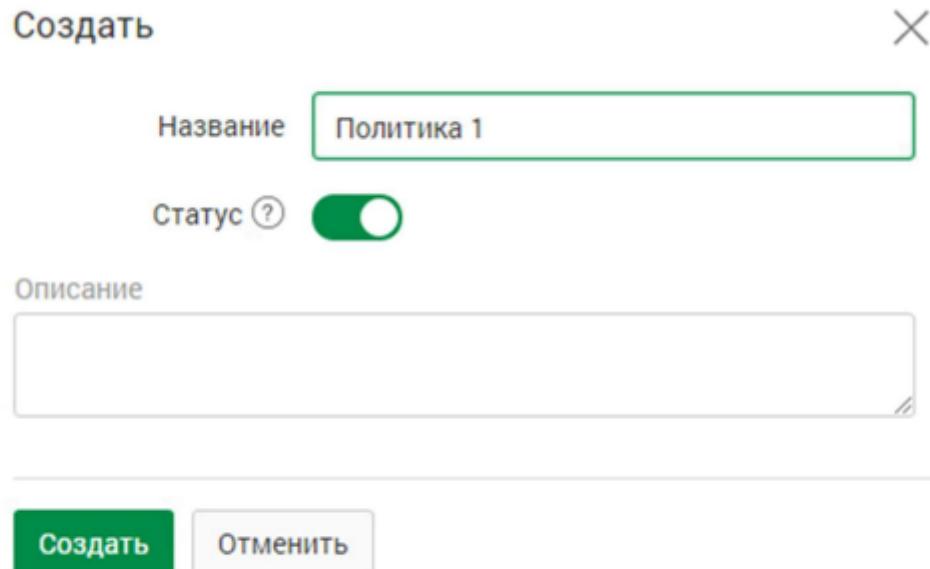
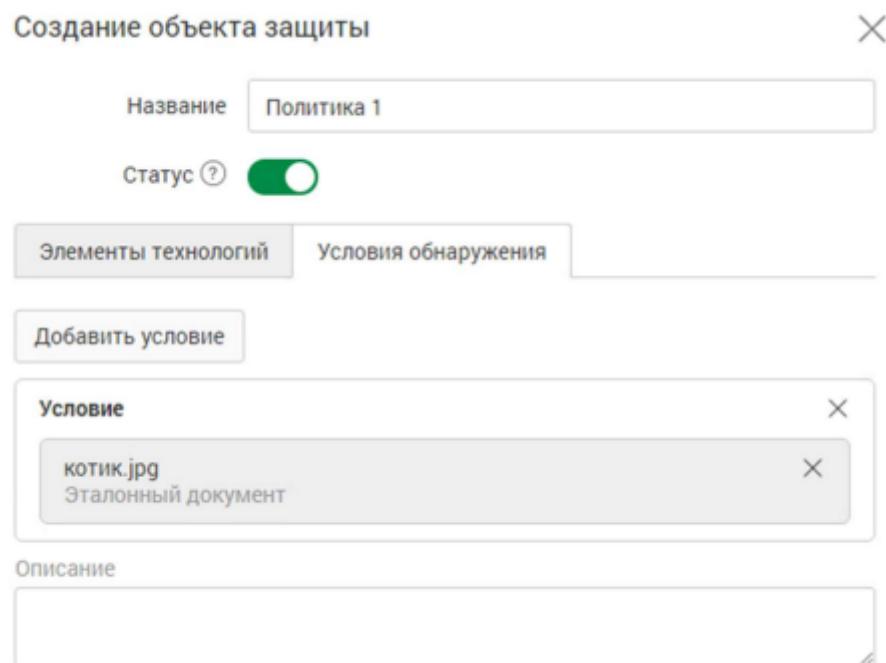


Рисунок 78 – «Создание каталога объектов защиты»

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».

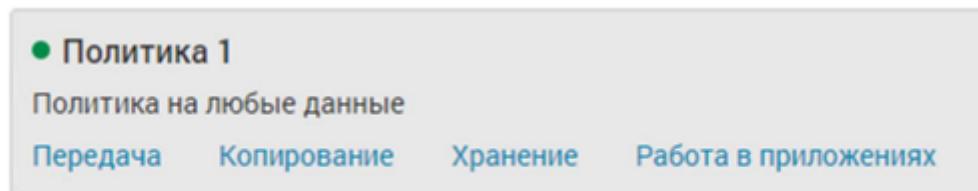


Рисунок 80 – «Политика 1»

### 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="+"/> <input type="button" value="W10-CLI1 X"/> <input type="button" value="W10-CLI2 X"/>
Отправители	<input type="button" value="= ?"/> <input type="text" value="Начните вводить текст"/> <input type="button" value="+"/>
Получатели	<input type="button" value="= ?"/> <input type="text" value="Начните вводить текст"/> <input type="button" value="+"/>
Дни действия правила	<input type="button" value="Любой день недели"/>
Часы действия правила	<input type="button" value="0:00"/> <input type="button" value="⌚"/> - <input type="button" value="0:00"/> <input type="button" value="⌚"/>

### Действия при срабатывании правила

Отправить почтовое уведомление	<input type="text" value="Начните вводить текст"/> <input type="button" value="+"/>	Ак Что раз
Назначить событию вердикт	<input type="button" value="Заблокировать"/>	
Назначить событию	<input type="button" value="Ничего"/>	

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	-	0:00

**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" value="-"/>
Назначить событию уровень нарушения	<input checked="" type="radio"/> Низкий	<input type="button" value="-"/>
Назначить событию теги	Политика 1	<input type="button" value="+"/>
Назначить отправителю статус	Выберите статус	<input type="button" value="-"/>
Удалить событие	<input type="button" value=""/>	

Акти  
Чтобы  
разде

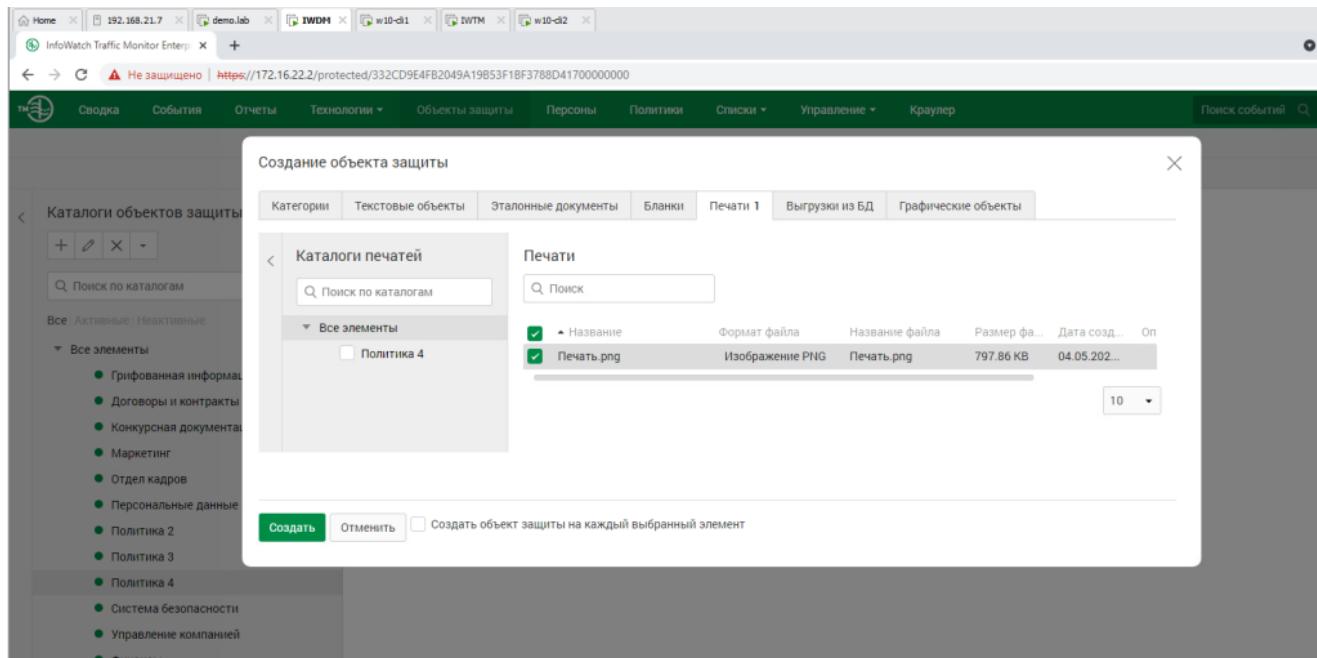
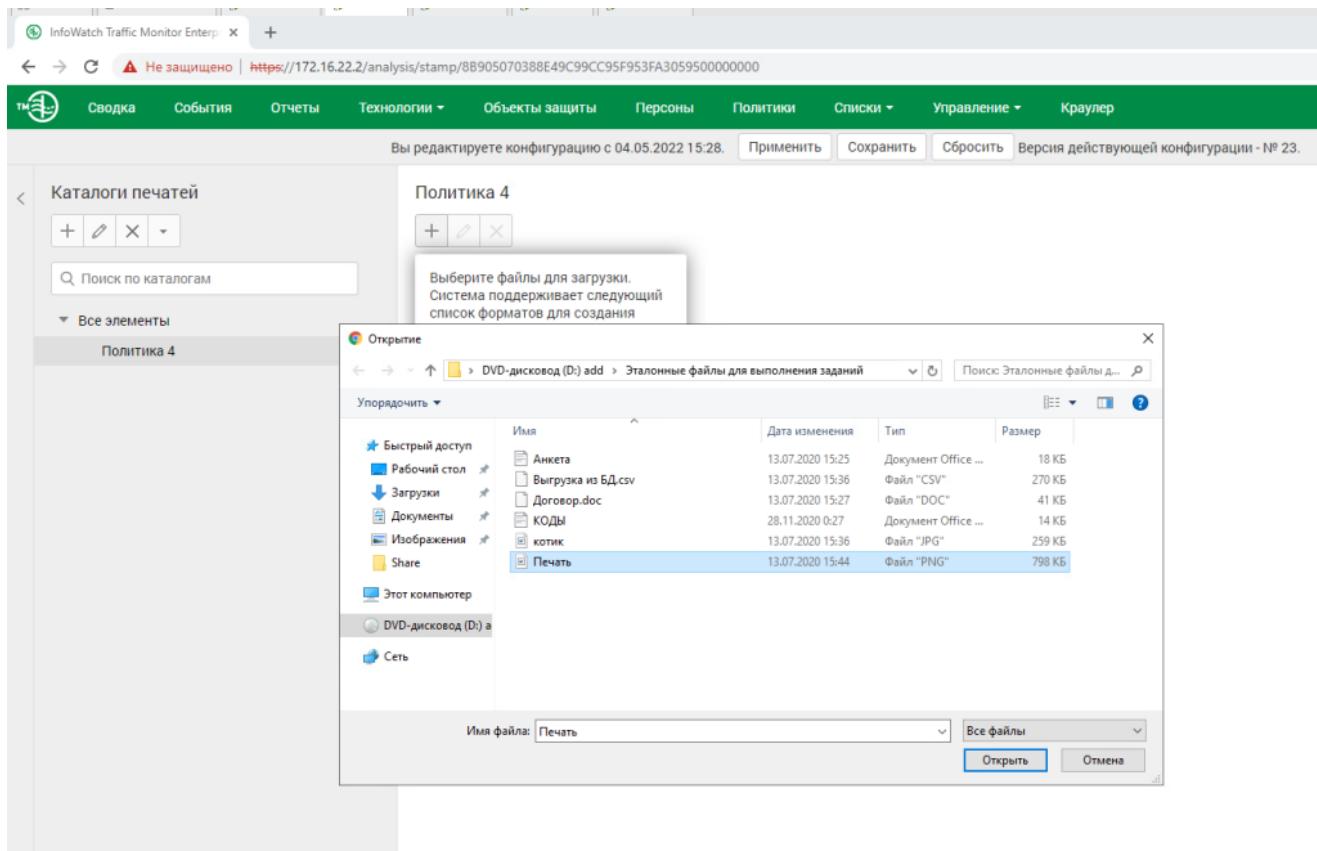
**Политика 4****Необходимо**

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



The screenshot shows the InfoWatch Traffic Monitor Enterprise web interface. The top navigation bar includes tabs for Home, 192.168.21.7, demo.lab, IWDH, w10-cl1, IWTM, and w10-cl2. Below the navigation is a browser header with the URL https://172.16.22.2/protected/332CD9E4FB2049A19B53F1BF3788D41700000000, a warning about it not being secure, and a plus sign to add new tabs.

The main menu bar contains links for Сводка, События, Отчеты, Технологии, Объекты защиты, Персоны, Политики, Списки, Управление, and Краулер.

The left sidebar displays a tree view under 'Каталоги объектов защиты' (Protection Object Catalogs) with categories like Активные и Неактивные, and sub-categories such as Все элементы, Грифованная информация, Договоры и контракты, Конкурсная документация, Маркетинг, Отдел кадров, Персональные данные, Политика 2, Политика 3, Политика 4, Система безопасности, Управление компанией, and Финансы. 'Политика 4' is currently selected.

A central modal window titled 'Создание объекта защиты' (Create Protection Object) is open. It contains fields for 'Название' (Name) set to 'Политика 4', and a 'Статус' (Status) toggle switch which is turned on. Below these are two tabs: 'Элементы технологий' (Technology Elements) and 'Условия обнаружения' (Detection Conditions). A button labeled 'Добавить условие' (Add Condition) is present. A condition box labeled 'Печать.png' and 'Печать' is shown. An 'Описание' (Description) text area is also present. At the bottom of the modal are 'Создать' (Create) and 'Отменить' (Cancel) buttons.

InfoWatch Traffic Monitor Enterprise

Не защищено | <https://172.16.22.2/policy>

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

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

Политики Добавить политику Фильтр

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 Добавить правило

Название Политика 4  
Период действия Все время  
Статус

Захищаемые 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 interface. The main window displays a list of policies (Politika 4, Politika 3, Politika 2) under the 'Политики' tab. Each policy entry includes fields for 'Объект защиты' (Protected object), 'Передача 1' (Transfer 1), and 'Копирование' (Copy). On the right side, a detailed configuration panel for 'Правило передачи' (Transfer Rule) is open. This panel allows setting up the rule direction (One-way or Both ways), type of event (Web message, ICQ, MS Lync, etc.), computers involved (DEMO-DC, DEMOLAB, IWDM, W10-CLI1), and specific users (Kornilov V. Fedosej, Accounting). It also specifies recipient fields, active days, and hours, along with an action section for triggering events. Buttons for 'Сохранить' (Save) and 'Отменить' (Cancel) are at the bottom.

## 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».

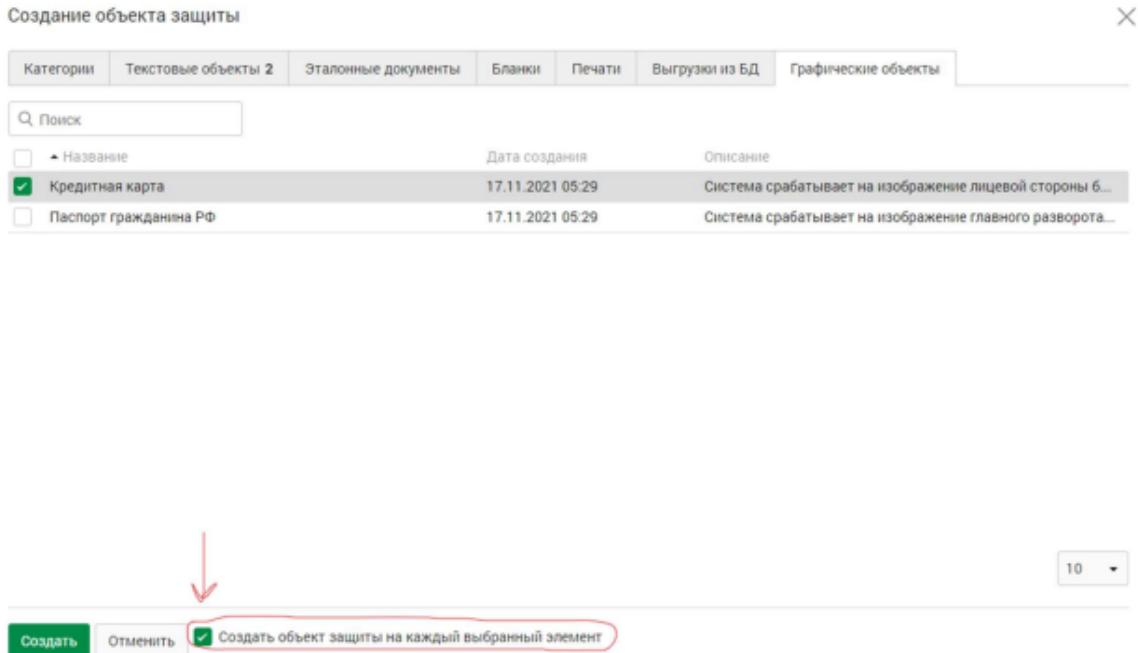


Рисунок 82 – «Чекбокс “создать объект защиты на каждый выбранный элемент”»

Активе  
Чтобы а  
раздел "

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

Выбрать

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

Активация  
Чтобы активи  
раздел "Пара

## 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="W10-CLI1 X"/> <input type="button" value="W10-CLI2 X"/> <input type="button" value="+"/>
Отправители	<input type="button" value="= ?"/> <input type="button" value="Accounting X"/> <input type="button" value="+"/>
Получатели	<input type="button" value="= ?"/> <input type="text" value="Начните вводить текст"/> <input type="button" value="+"/>
Дни действия правила	<input type="button" value="Любой день недели"/>
Часы действия правила	0:00 <input type="button" value="⌚"/> - 0:00 <input type="button" value="⌚"/>

## Действия при срабатывании правила

Отправить почтовое уведомление	<input type="text" value="Начните вводить текст"/> <input type="button" value="+"/>
Назначить событию вердикт	<input type="button" value="🚫 Заблокировать"/>

---

Получатели  =

Дни действия правила

Часы действия правила  -

**Действия при срабатывании правила**

Отправить почтовое  уведомление

Назначить событию вердикт

Назначить событию уровень нарушения

Назначить событию теги

Назначить отправителю статус

Удалить событие

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

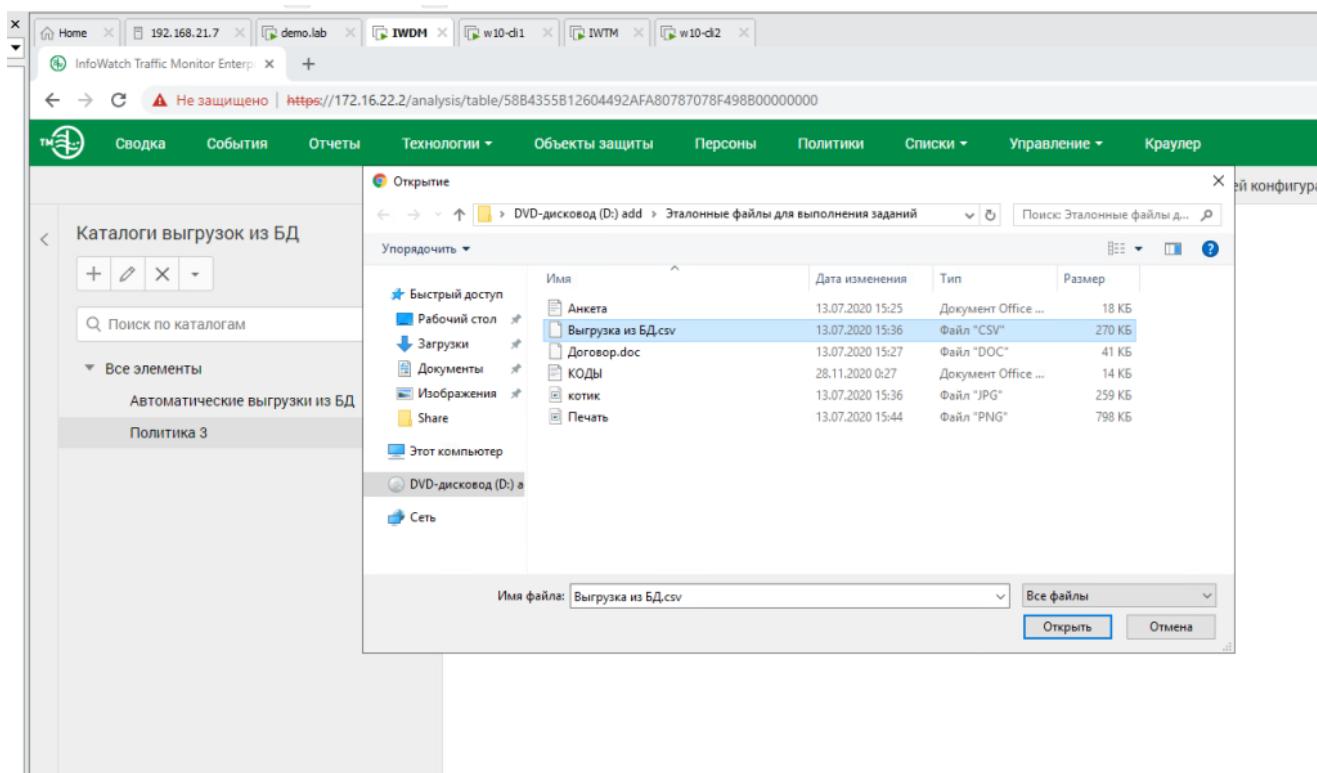
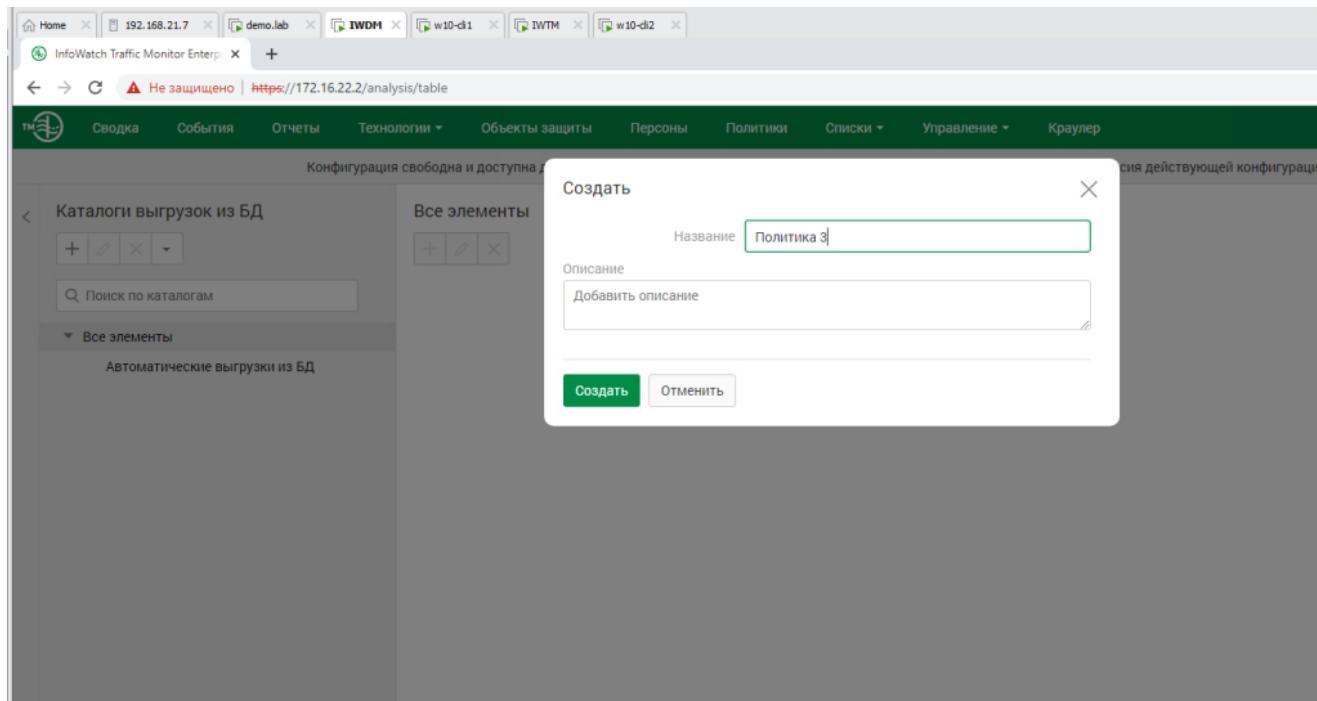
Тег: Политика 6

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



The screenshot shows the 'Редактировать' (Edit) dialog for a database export policy named 'Выгрузка из БД.csv'. The dialog includes fields for 'Название' (Name), 'Название файла' (File Name), 'Формат файла' (File Format), and 'Режим обновления' (Update Mode). It also contains a section for 'Условие обнаружения' (Detection Condition) with a table showing a single rule: 'Условие по умол...' (Condition by default) with expression '5+7+10+14+16+18' and 'Минимальное ко...' (Minimum value) set to 5. There are buttons for 'Сохранить' (Save), 'Обновить' (Update), and 'Отменить' (Cancel).

The screenshot shows the 'Создание объекта защиты' (Create Protection Object) dialog. In the 'Категории' (Categories) tab, 'Выгрузки из БД' (Exports from DB) is selected. Under 'Выгрузки из БД', the 'Выгрузка из БД.csv' item is selected. The 'Создать' (Create) button is visible at the bottom left.

The screenshot shows the 'InfoWatch Traffic Monitor Enterprise' web interface. The main menu bar includes 'Home', '192.168.21.7', 'demo.lab', 'IWDM', 'w10-d1', 'IWTM', 'w10-d2', and a 'InfoWatch Traffic Monitor Enterprise' tab which is currently active. A warning message 'Не защищено | https://172.16.22.2/protected/D304764A72AA4AFE986A5D217AC5CB9300000000' is displayed. The top navigation bar has tabs for 'Сводка', 'События', 'Отчеты', 'Технологии', 'Объекты защиты', 'Персоны', 'Политики', 'Списки', and 'Управление'. A sub-menu 'Вы редактируете конфигурацию' is open above the 'Управление' tab.

**Каталоги объектов защиты**

- + ○ Пометка
- ○ Удалить
- Поиск по каталогам
- Все | Активные | Неактивные
- ▼ Все элементы
  - Грифованная информация
  - Договоры и контракты
  - Конкурсная документация
  - Маркетинг
  - Отдел кадров
  - Персональные данные
  - Политика 2
  - Политика 3
  - Система безопасности
  - Управление компанией
  - Финансы

**Политика 3**

**Создание объекта защиты**

Название: Политика 3  
Статус: включен

Элементы технологий | Условия обнаружения

Добавить условие

**Условие**

Выгрузка из БД, csv  
Выгрузка из Бд  
Условие обнаружения  
Условие по умолчанию

Описание

**Создать** | **Отменить**

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 'Politika' configuration page. The top navigation bar includes 'Сводка', 'События', 'Отчеты', 'Технологии', 'Объекты защиты' (which is selected), 'Персоны', 'Политики', 'Списки', 'Управление', and 'Краупер'. A search bar 'Поиск событий' and a user icon 'iwtm-officer' are also present.

**Политики**

Политики защиты данных:

- 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

**Политика защиты данных**

Название: Политика 3  
Период действия: Все время  
Статус: включен

**Защищаемые данные**

Выбрать

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

**Объекты защиты**

Политика 3

Описание: Введите описание

Создан: 04.05.2022 15:01 | Изменен: 04.05.2022 15:01

**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 ИТ, который может отсылать информацию свободно.

Вердикт: разрешить

Уровень нарушения: средний

Тег: Политика 7

Политика 8

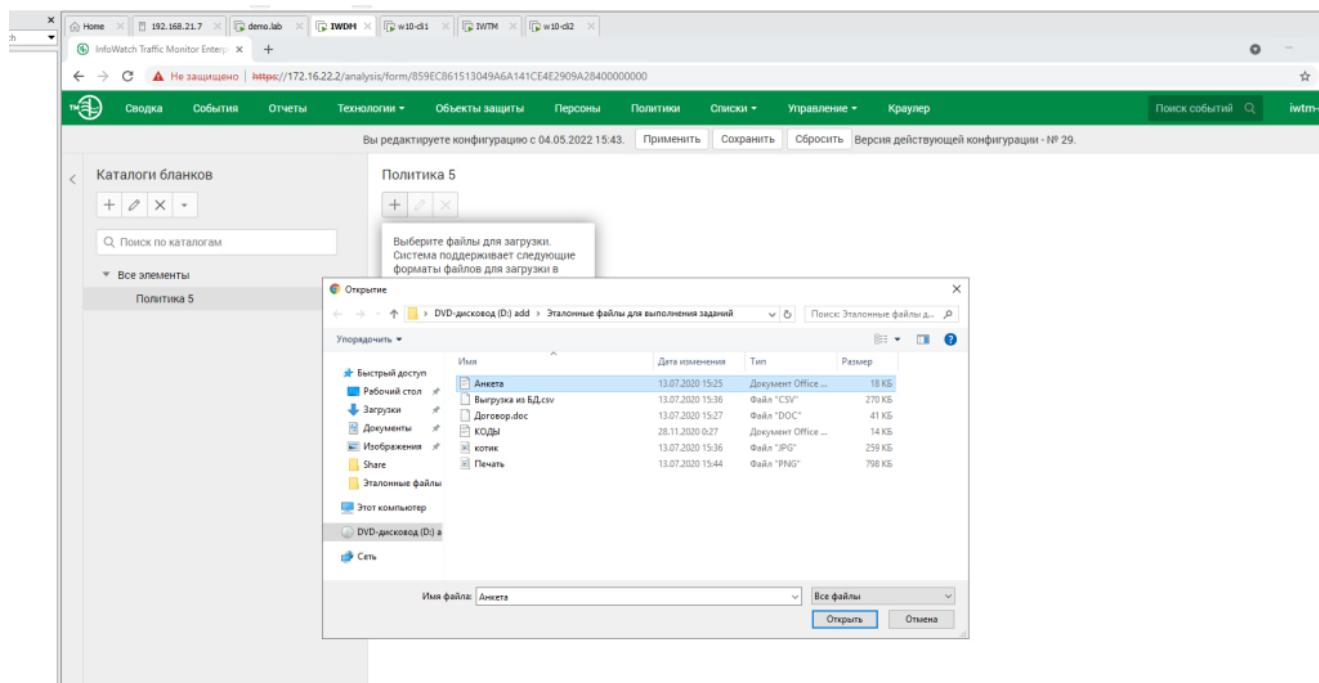
Для мониторинга движения анкет необходимо вести наблюдение за анкетами компании за пределы компании, запрещая любую внешнюю передачу документов в пустых и заполненных бланках. Для настройки используйте файл примера из AdditionalFiles.iso в datastore1.

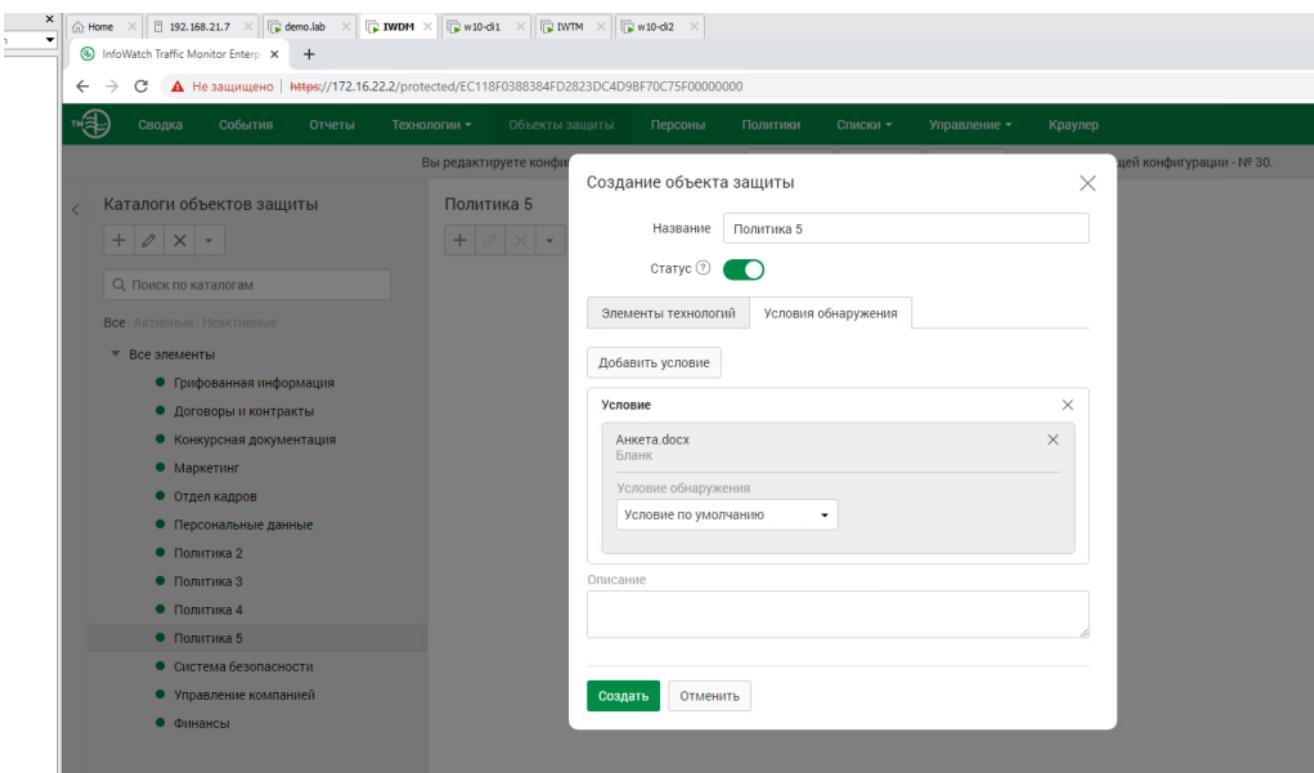
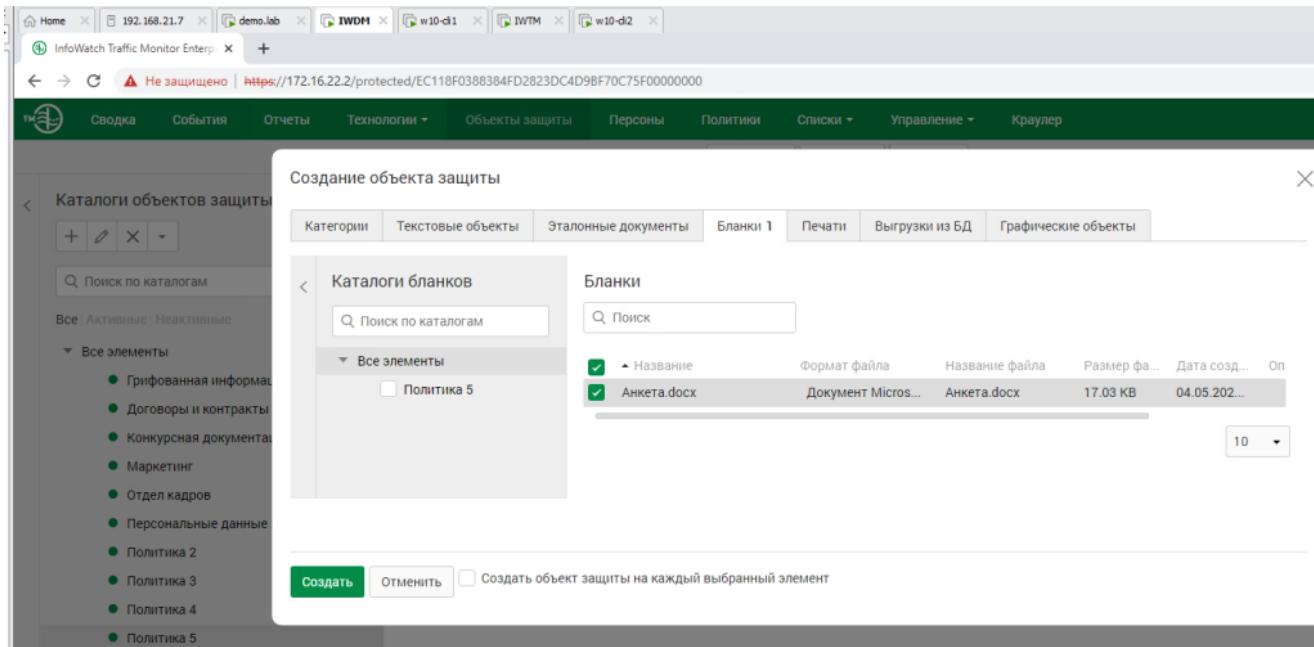
Генеральный директор и совет директоров могут обмениваться данной информацией совершенно свободно.

Вердикт: разрешить

Уровень нарушения: средний

Тег: Политика 8





## 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	Пользователи	Описание
Администратор administrator, Предустановленный	Administrator	Предустановленный администратор.
Офицер безоговорочный iwtm-officer, Предустановленный	iwtm-officer	Предустановленный офицер безоговорочный.

Создание 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

Активация Windows  
Чтобы активировать Windows, перейдите в раздел "Параметры".  
Чтобы активировать Windows, перейдите в раздел "Параметры".

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

Активация Windows  
Чтобы активировать Windows, перейдите в раздел "Приложения".

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

Управление доступом

Пользователи	
<input data-bbox="520 1140 552 1174" type="button" value="+"/>	<input data-bbox="560 1140 591 1174" type="button" value="X"/>
<input data-bbox="599 1140 631 1174" type="button" value="☰"/>	
Логин Назв... Email Роли Обла... Опис...	
<input type="checkbox"/> iwtm-o iwtm-o iwtm-o Админ Полн <input type="checkbox"/> admini Админ Админ Преду <input type="checkbox"/> officer Офице Админ Полн Преду	

Пользователи

Создание пользователя

Логин

Статус

Email

Полное имя

Роли

Области видимости

Описание

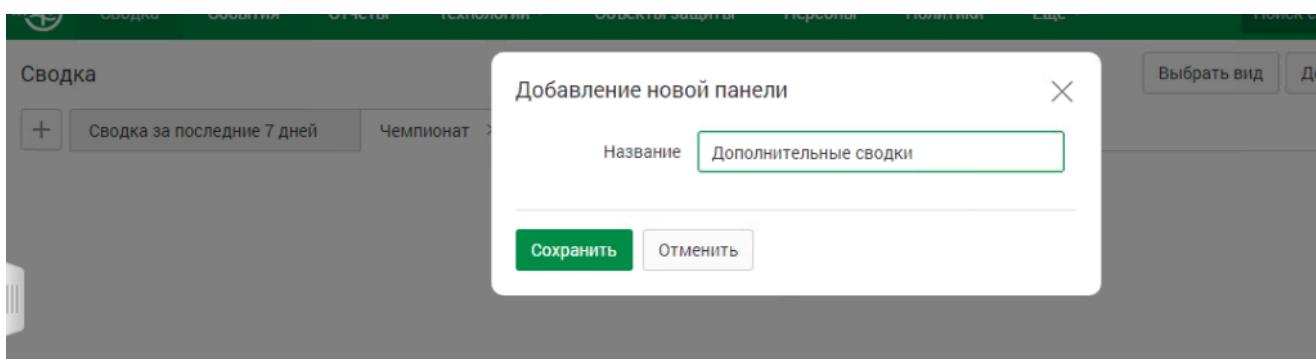
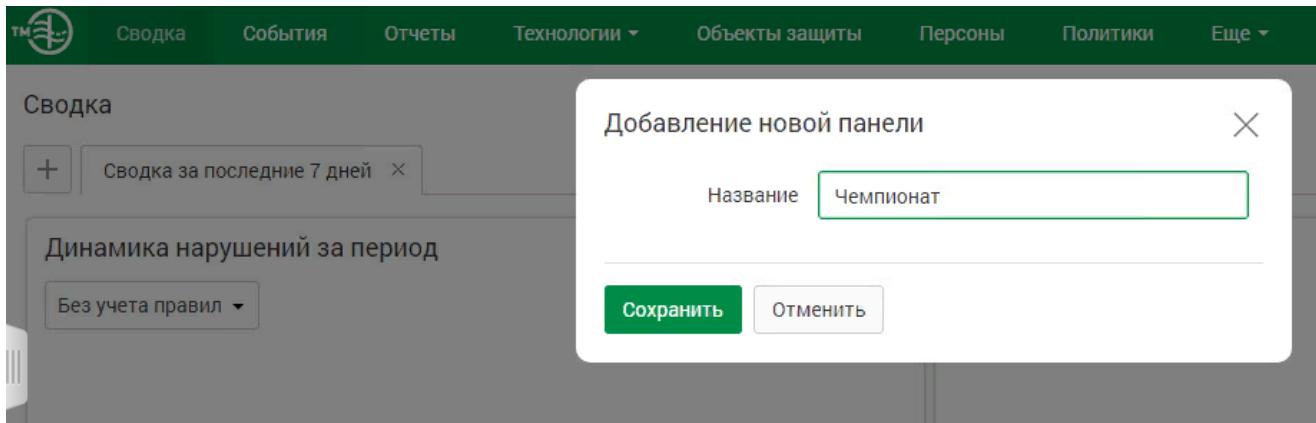
Пароль

Подтверждение пароля

Активация Windows  
Чтобы активировать Windows, перейдите в раздел "Приложения".

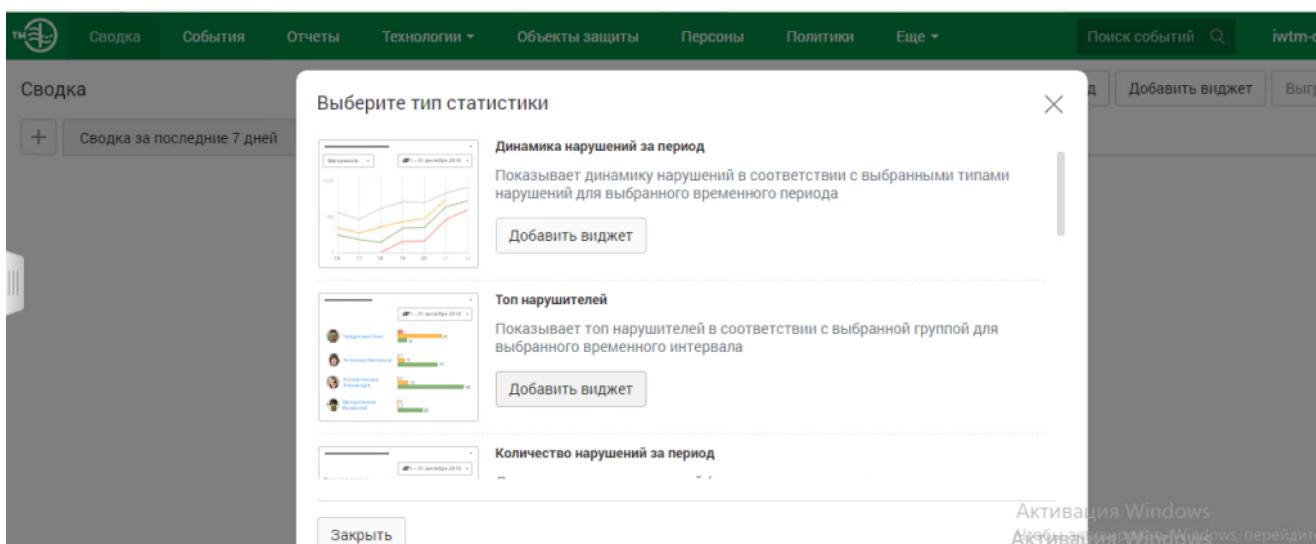
## Задание 2: Сводки

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



**Задание 3: Виджеты Создайте в сводке 4 виджета:**

1. Выборка по событиям краулера 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



## 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 поиска событий  iwtm-officer ▾

**Сводка**

+ Сводка за последние 7 дней  
Без учета правил

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

**Добавить виджет**

Закрыть

Активация Windows  
Для активации Windows, перейдите в раздел "Параметры", чтобы активировать Windows, перейдите в раздел "Параметры".



## Сводка

<a href="#">+</a>	Сводка за последние 7 дней	Чемпионат <a href="#">×</a>	Дополнительные сводки
-------------------	----------------------------	-----------------------------	-----------------------

### Общие настройки виджета

Название	По политикам
Интервал обновления:	Не обновлять <a href="#">▼</a>
Период:	Текущий месяц <a href="#">▼</a>
Политики	Начните вводить текст <a href="#">+</a>
<a href="#">Сохранить</a> <a href="#">Отменить</a>	

Сводка

Выберите тип статистики

нарушений высокого, среднего, низкого уровня за выбранный пользователем период

Добавить виджет

Подборка

Показывает события для выбранной подборки

Добавить виджет

Динамика статусов за период

Показывает динамику статусов для выбранного периода времени

Закрыть

Активация Windows  
Активация Windows  
чтобы активировать Windows, перейдите в раздел "Параметры" и выберите "Активация 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 переходим 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